FortiOS Log Reference

VERSION 5.2.2

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

May 25, 2015

FortiOS 5.2.2 Log Reference

01-522-262694-20150525

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-05-25	Updated for version 5.2.2.
2015-08-27	Added delta between version 5.2.1 and 5.2.2.

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.

How This Reference is Organized

The following sections are grouped by log type with the exception of Event and Security log types which are grouped by sub types, for example; **Security->AntiVirus** and **Event->System**, due to the large number of sub types associated with the security and event logs.

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

This chapter includes the following topic:

Managing and Understanding Logs

This document is organized by log types and sub types which provide quick access to messages related to specific logs and filters the messages into meaningful sections in the database.

It provides administrators with a comprehensive list of all the log messages that the FortiGate generates with explanations of what the messages mean and what possible actions you might take upon receiving them. The document is organized by log type and sub types. In each section, the log entry messages are listed by their log type ID numbers. See, the Log Types and Sub Types section for more information about the Log ID numbering format.

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

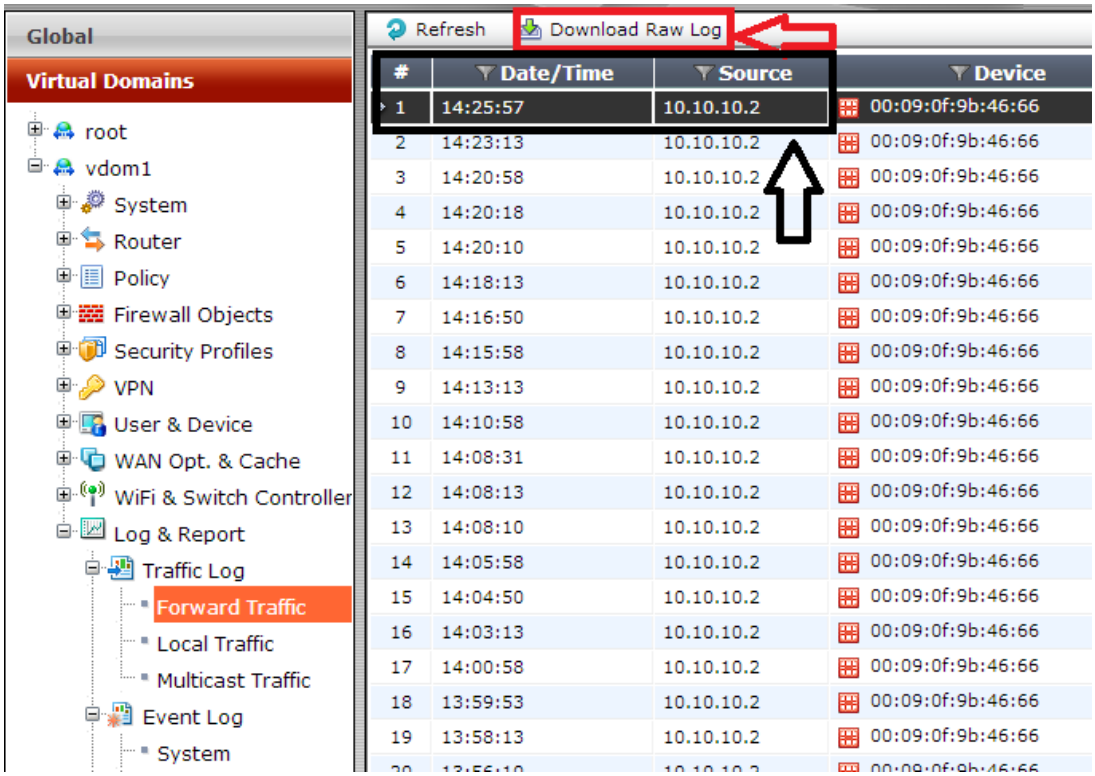
Log Field	Log Field Description	Data Type	Length	Value(s)
appact	The security action from app control	ENUM	16	• block • encrypt-kickout • monitor • pass • reject • reset

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`
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					

Example: Traffic Log (Raw Format)

Field Name (Raw format view in parentheses)	Field Description	Exists in Log Type			Example Field - Value (raw format)
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 Inter-face(srcintf)	The interface of the traffic's origin.	√	√	√	`srcintf="mgmt1"`
Destination IP (dstip)	The destination IP address for the web.	√	√	√	`dstip=10.6.30.1`
Destination Port(dstport)	The port number of the traffic's des-tination.	√	√	√	`dstport=80`
Destination Interface (dstintf)	The interface of the traffic's destination.	√	√	√	`dstintf="vdom1"`

Example: Traffic Log (Raw Format)

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

Log Type IDs	Sub Type IDs
event:1	• system:0 • vpn:1 • user:2 • router:3 • wireless:4 • wad:5 • gtp:6 • endpoint:7 • ha:8
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

Log Type IDs	Sub Type IDs
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
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

Log Type IDs	Sub Type IDs
netscan: 11	• discovery:0 • vulnerability:1
UTM	• virus:2 • webfilter:3 • ips:4 • spam:5 • contentlog:6 • voip:8 • dlp:9 • app-ctrl:10

Traffic Log

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

Traffic logs include the following log sub types.

- Forward
- Multicast
- Local
- Sniffer

The following table describes the log fields of the Traffic log.

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

Log Field Name	Log Field Description	Data Type	Length	Value
action	The 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	• close • deny • dns • ip-conn • start • timeout
app	The application name.	String	96	

Log Field Name	Log Field Description	Data Type	Length	Value
appact	The security action from app control.	String	16	• block • encrypt-kickout • monitor • pass • reject • reset
appcat	The application category.	String	64	
appid	The application ID.	UINT32	10	
applist	The application control profile (name).	String	64	
apprisk	The application risk level.	String	16	• critical • elevated • high • low • medium
collectedemail	The email address from email collection captive portal.	String	66	
countapp	The number of appplication control logs associated with the session.	UINT32	10	
countav	The number of AntiVirus logs associated with the session.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
countdlp	The number of the DLP logs associated with the session.	UINT32	10	
countemail	The number of the email logs associated with the session.	UINT32	10	
countips	The number of the IPS logs associated with the session.	UINT32	10	
countweb	The number of the Web Filter logs associated with the session.	UINT32	10	
craction	The action performed by client reputation.	UINT32	10	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
custom	The custom field.	Custom		
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
devtype	The device type.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
dstcountry	The country name for the destination IP.	String	64	
dstintf	The destination interface.	String	32	
dstip	The destination IP address.	IP Address	39	
dstname	The destination name.	String	66	
dstport	The destination port.	UINT16	5	
dstssid	The destination SSID.	String	33	
dstuuid	The UUID of the destination IP address.	String	37	
duration	The duration of the session.	UINT32	10	
group	The group name.	String	64	
lanin	The local area network incoming traffic in bytes.	UINT64	20	
lanout	The local area network outgoing traffic in bytes.	UINT64	20	
level	The log priority level.	String	11	

Log Field Name	Log Field Description	Data Type	Length	Value
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message ID.	String	10	
mastersrcmac	The master MAC address for a host that has multiple network interfaces.	String	17	
msg	The activity or event that the FortiGate unit recorded.	String	64	
osname	The name of the operating system.	String	66	
osversion	The version of the operating system.	String	66	
policyid	The firewall policy ID.	UINT32	10	
poluuid	The UUID of the firewall policy.	String	37	
proto	The protocol number.	UINT8	3	
rcvdbyte	The number of bytes received.	UINT64	20	
rcvdpkt	The number of packets received.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
sentbyte	The number of bytes sent.	UINT64	20	
sentpkt	The number of packets sent.	UINT32	10	
service	The name of service.	String	36	
sessionid	The session ID.	UINT32	10	
shaperdroprcvdbyte	The number of received bytes dropped by shaper.	UINT32	10	
shaperdropsentbyte	The number of sent bytes dropped by shaper.	UINT32	10	
shaperperipdropbyte	The number of dropped bytes per IP by shaper.	UINT32	10	
shaperperipname	The traffic shaper name (per IP).	String	36	
shaperrcvdname	The traffic shaper name for received traffic.	String	36	
shapersentname	The traffic shaper name for sent traffic.	String	36	
srccountry	The country name for source IP.	String	64	
srcintf	The source interface name.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
srcip	The source IP address.	IP Address	39	
srcmac	The MAC address associated with the Source IP.	String	17	
srcname	The source name.	String	66	
srcport	The source port number.	UINT16	5	
srcssid	The source SSID.	String	33	
srcuuid	The UUID of the source IP address.	String	37	
subtype	The subtype of the traffic.	String	20	
time	The time stamp of the event.	String	8	
trandisp	The NAT translation type.	String	16	• dnat • noop • snat • snat+dnat
tranip	The NAT destination IP.	IP Address	39	
tranport	The NAT destination port.	UINT16	5	
transip	The NAT source IP address.	IP Address	39	
transport	The NAT source port.	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
type	The log type.	String	16	
unauthuser	The unauthenticated user name.	String	66	
unauthusersource	The method used to detect unauthenticated user name.	String	66	
user	The user name.	String	256	
utmaction	The security action performed by UTM.	String	32	• allow • block • n/a • reset • traffic-shape
vd	The virtual domain name.	String	32	
vpn	The name of the VPN tunnel.	String	32	
vpntype	The type of the VPN tunnel.	String	14	• ipsec-ddns • ipsec-dynamic • ipsec-static • sslvpn
wanin	The WAN incoming traffic in bytes.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
wanoptapptype	The WAN optimization application type.	String	9	• cifs • ftp • ftp-proxy • http • mapi • tcp • web-cache • web-proxy
wanout	The 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

Security Log

The following sections provide information about the different types of logs recorded under the Security log type.

In FortiOS 5.0 and previous versions, the logs were displayed under the UTM log type. In FortiOS 5.2.0 and later versions, the UTM logs are displayed under the Security log type. All logs grouped in the security log include the log field type=utm.

Application Control

Application Control log messages record application control protocols and events.

In the log fields, these logs are defined as: type=utm; subtype=app-ctrl.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by Application Control.	String	16	• block • encrypt-kickout • kickout • monitor • pass • reject • reset
app	The application name.	String	96	
appcat	The application category name.	String	64	
appid	The application ID.	UINT32	10	
applist	The application control profile name.	String	64	
apprisk	The application risk level.	String	16	• critical • elevated • high • low • medium
cloudaction	The action performed by cloud application.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
clouduser	The user login ID detected by the Deep Application Control feature.	String	256	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
direction	The direction of the packets.	String	8	• incoming • N/A • outgoing
dstip	The destination IP address.	IP Address	39	
dstname	The destination name.	String	64	
dstport	The destination port.	UINT16	5	
eventtype	The application control event type.	String	32	
filename	The file name.	String	256	
filesize	The file size in bytes.	UINT64	10	
group	The user group name.	String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
hostname	The host name of a URL.	String	256	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String	512	
profile	The application control profile name.	String	36	
profiletype	The application control profile type.	String	36	
proto	The protocol number.	UINT8	3	
rcvdbyte	The number of bytes received.	UINT64	20	
sentbyte	The number of bytes sent.	UINT64	20	
service	The service name.	String	36	
sessionid	The session ID.	UINT32	10	
srcip	The source IP address.	IP Address	39	

Log Field Name	Log Field Description	Data Type	Length	Value
srcname	The source name.	String	64	
srcport	The source port.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
url	The URL address.	String	512	
user	The user name.	String	256	
vd	The virtual domain name.	String	32	

Application Control Log Messages

The following table describes the log message IDs and messages of the Application Control 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

AntiVirus

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

In the log fields, these logs are defined as: type=utm; subtype=virus.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by antivirus profile.	String	11	• analytics • blocked • monitored • pass through
agent	The user agent - eg. agent="Mozilla/5.0".	String	64	
analyticscksum	The checksum of the file submitted for analytics.	String	64	
analyticssubmit	The flag for analytic submission.	String	10	• false • true
checksum	The file checksum.	String	16	
command	The protocol specific command, such as “POST” and “GET” for HTTP, “MODE” and “REST” for FTP.	String	16	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
direction	The direction of packets.	String	8	• incoming • N/A • outgoing
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	
dtype	The data type for virus category.	String	32	
eventtype	The event type of antivirus.	String	32	
filefilter	The filter used to identify the affected file.	String	12	• none • file pattern • file type
filename	The file name.	String	256	

Log Field Name	Log Field Description	Data Type	Length	Value
filetype	The file type.	String	16	• arj • cab • lzh • rar • tar • zip • bzip • gzip • bzip2 • bat • msc • uue • mime • base64 • binhex • com • elf • exe • hta • html • jad • class • cod • javascript • msoffice • fsg • upx • petite • aspack • prc • sis • hlp • activemime • jpeg • gif • tiff • png • bmp • ignored • unknown

Log Field Name	Log Field Description	Data Type	Length	Value
from	The email address from the Email Headers (IMAP/POP3/SMTP).	String	128	
group	The user group name.	String	64	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message ID.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
profile	The name of the profile that was used to detect and take action.	String	64	
proto	The protocol number.	UINT8	3	
quarskip	The quarantine skip explanation.	String	46	• File-was-notquarantined • No-quarantine-for- HTTP-GET-filepattern-block • No-quarantine-foroversized-files • No-skip
recipient	The email addresses received from the SMTP envelope.	String	512	
ref	The URL of the FortiGuard IPS database entry for the attack.	String	512	

Log Field Name	Log Field Description	Data Type	Length	Value
sender	The email address sent from the SMTP envelope.	String	128	
service	The service name.	String	5	• ftp • ftps • http • https • im • imap • imaps • mapi • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smb • smtp • smtps • ssl
sessionid	The session ID.	UINT32	10	
srcip	The source IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
switchproto	The protocol change information.	String	128	
time	The time stamp of the event.	String	8	
to	The email address(es) from the Email Headers (IMAP/POP3/SMTP.	String	512	

Log Field Name	Log Field Description	Data Type	Length	Value
type	The log type.	String	16	
url	The URL address	String	512	
user	The user name.	String	256	
vd	The virual domain name.	String	32	
virus	The name of the virus.	String	128	
virusid	The virus ID.	UINT32	10	

AntiVirus Log Messages

The following table describes the log message IDs and messages of the Anti Virus 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

Message ID	Message	Severity
8704	MESGID_OVERSIZE_WARNING	Warning
8705	MESGID_OVERSIZE_NOTIF	Notice
8706	MESGID_OVERSIZE_MIME_WARNING	Warning
8707	MESGID_OVERSIZE_MIME_NOTIF	Notice
8720	MESGID_SWITCH_PROTO_WARNING	Warning
8721	MESGID_SWITCH_PROTO_NOTIF	Notice
8960	MESGID_SCAN_UNCOMPNESTLIMIT	Notice
8961	MESGID_SCAN_UNCOMPSIZELIMIT	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

Message ID	Message	Severity
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

Data Leak Protection (DLP) log messages record data leaks. These logs provide additional information to help administrators better analyze and detect data leaks.

In the log fields, these logs are defined as: type=utm; subtype=dlp.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by DLP.	String	20	• ban • ban-sender • block • exempt • log-only • quarantine-interface • quarantine-ip
agent	The user agent - eg. agent-t="Mozilla/5.0".	String	64	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
direction	The direction of packets.	String	8	• incoming • N/A • outgoing
dlpextra	The DLP extra information.	String	256	
docsource	The document source.	String	515	
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
epoch	The Epoch used for locating file.	UINT32	10	
eventid	The serial number of the dlparchive file in the same epoch.	UINT32	10	
eventtype	The DLP event type.	String	32	
filename	The file name.	String	256	
filesize	The file size in bytes.	UINT64	10	
filetype	The file type.	String	23	
filtercat	The DLP filter category.	String	8	
filteridx	The DLP filter ID.	UINT32	10	
filtername	The DLP filter name.	String	128	
filtertype	The DLP filter type.	String	23	• file • message • none • credit-card • encrypted • file-size • file-type • fingerprint • none • regexp • ssn • watermark
from	The email address from the Email Headers (IMAP/POP3/SMTP).	String	128	
group	The user group name.	String	64	
hostname	The host name of a URL.	String	256	

Log Field Name	Log Field Description	Data Type	Length	Value
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log sub-type. The last one to five digits are the message id.	String	10	
mmsdir		String	3	
msg	The activity or event that the FortiGate unit recorded.	String	512	
profile	The DLP profile name	String	64	
proto	The protocol number	UINT8	3	
rcvdbyte	The number of bytes received.	UINT64	20	
recipient	The email addresses received from the SMTP envelope.	String	512	
sender	The email address sent from the SMTP envelope.	String	128	
sensitivity	The sensitivity for document fingerprint.	String	36	
sentbyte	The number of bytes sent.	UINT64	20	

Log Field Name	Log Field Description	Data Type	Length	Value
service	The service name.	String	36	• ftp • ftps • http • https • im • imap • imaps • mapi • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smtp • smtps • ssl
sessionid	The session ID.	UINT32	10	
severity	The severity level of a DLP rule.	String	8	
srcip	The source IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subject	The subject title of the email message.	String	128	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
to	The email address(es) to the Email Headers (IMAP/POP3/SMTP).	String	512	

Log Field Name	Log Field Description	Data Type	Length	Value
type	The log type.	String	16	
url	The URL address.	String	512	
user	The user name.	String	256	
vd	The virtual domain name.	String	32	

DLP Log Messages

The following table describes the log message IDs and messages of the Data Leak Protection 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 Filter

Email filter log messages record email protocols, such as SMTP, POP3 and IMAP.

In the log fields, these logs are defined as: type=utm; subtype=emailfilter.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action of the email filter.	String	8	• blocked • detected • exempted
agent	The user agent - eg. agent="Mozilla/5.0".	String	64	
attachment	The flag for email attachment.	String	3	• No • yes
banword	The banned word.	String	128	
cc	The email address(es) from the Email Headers (IMAP/POP3/SMTP).	String		
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
direction	The direction of packets.	String	8	• incoming • N/A • outgoing
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
eventtype	The email filter event type.	String	32	
from	The Email address(es) from the Email Headers (IMAP/POP3/SMTP).	String	128	
group	The group name.	String	64	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String	512	
profile	The email filter profile name.	String	64	
proto	The protocol number.	UINT8	3	
rcvdbyte	The number of bytes received.	UINT64	20	
recipient	The email addresses received from the SMTP envelope.	String	512	
sender	The email addresses sent from the SMTP envelope.	String	128	

Log Field Name	Log Field Description	Data Type	Length	Value
sentbyte	The number of bytes sent.	UINT64	20	
service	The service name.	String	36	• ftp • ftps • http • https • im • imap • imaps • mapi • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smtp • smtps • ssl
sessionid	The session ID.	UINT32	10	
size	The email size in bytes.	String	16	
srcip	The source IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subject	The subject title of the email message.	String	256	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	

Log Field Name	Log Field Description	Data Type	Length	Value
to	The email address(es) from the Email Headers (IMAP/POP3/SMTP).	String	512	
type	The log type.	String	16	
user	The user name.	String	256	
vd	The virtual domain name.	String	12	

Email Filter Log Messages

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

Message ID	Message	Severity
20480	LOGID_ANTISPAM_EMAIL_SMTP_NOTIF	Notice
20481	LOGID_ANTISPAM_EMAIL_SMTP_ BWORD_NOTIF	Notice
20487	LOGID_ANTISPAM_ENDPOINT_MM7_ WARNING	Warning
20488	LOGID_ANTISPAM_ENDPOINT_MM7_ NOTIF	Notice
20489	LOGID_ANTISPAM_ENDPOINT_MM1_ WARNING	Warning
20490	LOGID_ANTISPAM_ENDPOINT_MM1_ NOTIF	Notice
20491	LOGID_ANTISPAM_EMAIL_IMAP_ BWORD_NOTIF	Notice
20492	LOGID_ANTISPAM_MM1_FLOOD_ WARNING	Warning
20493	LOGID_ANTISPAM_MM1_FLOOD_NOTIF	Notice
20494	LOGID_ANTISPAM_MM4_FLOOD_ WARNING	Warning
20495	LOGID_ANTISPAM_MM4_FLOOD_NOTIF	Notice
20496	LOGID_ANTISPAM_MM1_DUPE_ WARNING	Warning
20497	LOGID_ANTISPAM_MM1_DUPE_NOTIF	Notice
20498	LOGID_ANTISPAM_MM4_DUPE_ WARNING	Warning

Message ID	Message	Severity
20499	LOGID_ANTISPAM_MM4_DUPE_NOTIF	Notice
20500	LOGID_ANTISPAM_EMAIL_MSN_NOTIF	Information
20501	LOGID_ANTISPAM_EMAIL_YAHOO_NOTIF	Information
20502	LOGID_ANTISPAM_EMAIL_GOOGLE_ NOTIF	Information
20503	LOGID_EMAIL_SMTP_GENERAL_NOTIF	Information
20504	LOGID_EMAIL_POP3_GENERAL_NOTIF	Information
20505	LOGID_EMAIL_IMAP_GENERAL_NOTIF	Information
20506	LOGID_EMAIL_MAPI_GENERAL_NOTIF	Information
20507	LOGID_ANTISPAM_EMAIL_MAPI_ BWORD_NOTIF	Notice
20508	LOGID_ANTISPAM_EMAIL_MAPI_NOTIF	Notice

IPS

Intrusion logs record security logs for protocols, such as ICMP and virus attacks. The IPS logs also provide additional log details, such as the anomaly logs. The "anomaly" logs are generated from the kernel without signatures. (e.g.TCP SYN flood etc.).

In the log fields, these logs are defined as: type=utm; subtype= ips.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by IPS.	String	16	• clear_session • detected • drop_session • dropped • pass_session • reset • reset_client • reset_server
agent	The sser agent - eg. agent-t="Mozilla/5.0".	String	66	
attack	The attack name.	String	256	
attackcontext	The trigger patterns and the packetdata with base64 encoding.	String	2040	
attackcontextid	The attack context ID.	String	10	
attackid	The attack ID.	UINT32	10	
count	The repeat count for an attack event.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
craction	The action performed by client reputation level.	UINT32	10	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
direction	The direction of packets.	UINT32	10	• incoming • N/A • outgoing
dstintf	The destination interface.	String	64	
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	
eventtype	The IPS event type.	String	32	
group	The group name.	String	64	
icmpcode	The destination port of the ICMP message.	String	6	
icmpid	The source port of the ICMP message.	String	8	
icmptype	The type of ICMP message.	String	6	

Log Field Name	Log Field Description	Data Type	Length	Value
incidentserialno	The incident serial number.	UINT32	10	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message ID.	String	10	
msg	The log message for the attack.	String	518	
profile	The profile name for IPS.	String	64	
profiletype	The profile type.	String	64	
proto	The protocol number.	UINT8	3	
ref	The URL of the FortiGuard IPS database entry for the attack.	String		
service	The service name.	String	36	
sessionid	The session ID.	UINT32	10	
severity	The severity of the attack.	String	8	• critical • high • info • low • medium
srcintf	The source interface.	String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
srcip	The source IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
user	The user name.	String	256	
vd	The 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
18432	LOGID_ATTCK_ANOMALY_TCP_UDP	Alert
18433	LOGID_ATTCK_ANOMALY_ICMP	Alert
18434	LOGID_ATTCK_ANOMALY_OTHERS	Alert

Anomaly

Anomaly logs are associated with IPS log events.

In the log fields, these logs are defined as: type=utm; subtype= anomaly.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by FortiGate for the event.	String	16	
agent	The user agent - eg. agent="Mozilla/5.0".	String	66	
attack	The attack name.	String	256	
attackcontext	The trigger patterns and the packet data with base64 encoding.	String	2040	
attackcontextid	The attack context ID.	String	10	
attackid	The attack ID.	UINT32	10	
count	The repeat count for an attack event.	UINT32	10	
craction	The action performed by client reputation.	UINT32	10	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
direction	The direction of the packets.	UINT32	10	
dstintf	The destination interface.	String	64	
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	
eventtype	The event type.	String	32	
group	The user group name.	String	64	
icmpcode	The ICMP code.	String	6	
icmpid	The ICMP message ID.	String	8	
icmptype	The ICMP message type.	String	6	
incidentserialno	The incident serial number.	UINT32	10	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log sub-type. The last one to five digits are the message id.	String	10	
msg	The event or activity that the FortiGate unit recorded.	String	518	
profile	The profile name.	String	64	
profiletype	The profile type.	String	64	
proto	The protocol name.	UINT8	3	
ref		String		
service	The service name.	String	36	

Log Field Name	Log Field Description	Data Type	Length	Value
sessionid	The session ID.	UINT32	10	
severity		String	8	
srcintf	The source interface.	String	64	
srcip	The source IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	

Anomaly Log Messages

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

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

Web Filter

Web filter log messages record URL activity as well as filters, such as a blocked URL as it is found in the URL black list.

In the log fields, these logs are defined as: type=utm; subtype= webfilter.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by the web filter.	String	11	• allowed • blocked • DLP • exempted • filtered • pass through
agent	The user agent - eg. agent="Mozilla/5.0".	String	64	
banword	The banned word.	String	128	
cat	The web category ID.	UINT8	3	
catdesc	The web category description.	String	64	
contenttype	The content type from HTTP header.	String	64	
crlevel	The client reputation level.	String	10	
crscore	The client reputation score.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
direction	The direction of the web traffic.	String	8	• incoming • N/A • outgoing
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	
error	The URL rating error message.	String	256	
eventtype	The web filter event type.	String	32	
filtertype	The script filter type.	String	10	• javascript • jscript • n/a • unknown • vbscript
from	The MMS-only - From/To headers from the email.	String	128	
group	The group name.	String	64	
hostname	The host name of a URL.	String	256	
initiator	The initiator user for override.	String	64	
keyword	The keyword used for search.	String	512	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	

Log Field Name	Log Field Description	Data Type	Length	Value
method	The rating override method by URL domain name or IP address.	String	6	• Domain • ip
mode	The rating override mode.	String	32	
msg	The activity or event that the FortiGate unit recorded.	String	512	
ovrdid	The URL rating override ID.	UINT32	10	
ovrdtbl	The rating override table.	String	128	
profile	The web filter profile name.	String	64	
proto	The protocol number.	UINT8	3	
quotaexceeded	The quota has exceeded.	String	3	• no • yes
quotamax	The maximum quota allowed - in seconds if time-based - in bytes if traffic-based	UINT64	20	
quotatype	The quota type.	String	16	• time • traffic
quotaused	The quota used - in seconds if time-based - in bytes if traffic-based).	UINT64	20	
rcvdbyte	The number of bytes received.	UINT64	20	
reqtype	The request type.	String	8	• direct • referral
ruledata	The rule date.	String	512	
ruletype	The rule type.	String	9	• directory • domain • rating

Log Field Name	Log Field Description	Data Type	Length	Value
sentbyte	The number of bytes sent.	UINT64	20	
service	The service name.	String	36	• dns • ftp • ftps • http • https • im • imap • imaps • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smtp • smtps • ssl
sessionid	The session ID.	UINT32	10	
srcip	The souurce IP address.	IP Address	39	
srcport	The source port.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
to	The MMS-only - From/To headers from the email.	String	512	
type	The log type.	String	16	
url	The URL address.	String	512	
urlfilteridx	The URL filter ID.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
urlfilterlist	The URL filter list.	String	64	
urltype	The URL filter type.	String	8	• ftp • http • https • mail • phishing • telnet
user	The user name.	String	256	
vd	The virtual domain name.	String	32	

Web Filter 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

Message ID	Message	Severity
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
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

Message ID	Message	Severity
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

Event Log

The following sections provide information about the different types of logs recorded under the Event log type.

Event log include the following log subtypes:

- Endpoint Control
- GTP
- High Availability
- System
- Router
- VPN
- USer
- WAD
- Wireless

In the log field, these logs are defined as: type=event; subtypes=endpoint control, gtp, vpn, user, wad, system, router, wireless, high availability.

Endpoint Control

Following are the log details for the events generated for Endpoint control logs.

In the log fields, these logs are defined as: type=event; subtype= endpoint.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this firewall policy.	String	32	
connection_type	The FortiClient connection type.	String	6	
count	The number of dropped SIP packets.	UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The serial number of the device.	String	16	
forticlient_id	The FortiClient uuid.	String	33	
hostname	The host name.	String	128	
interface	The interface name.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
ip	The IP address.	IP Address	39	
level	The log priority level.	String	11	
license_limit	The number of limited licenses.	String	32	
license_ used	The number of licenses used.	UINT16	5	
logdesc	The log field description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message ID.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
name		String	128	
reason	The reason this log was generated.	String	256	
repeat		UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
status	The status of the action the FortiGate unit took when the event occurred.	String	23	• ipsec • success • failure • negotiate_error • esp_error • dpd_failure • subtype voip • start • end • timeout • blocked • succeeded • failed • authentication-required • sub type gtp • forwarded • prohibited • rate-limited • state-invalid • tunnel-limited • traffic-count • user-data
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	• endpoint
time	The time stamp of the event.	String	8	
type	The log type.	String	16	• event
ui	The user interface.	String	64	
used_for_type		UINT16	5	
user	The user name.	String	256	

Log Field Name	Log Field Description	Data Type	Length	Value
vd	The virtual domain name.	String	32	

Endpoint Log Messages

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

Message ID	Message	Description	Severity
45056	LOG_ID_FCC_EXCEED	FortiClient license maxed out	Notice
45057	LOG_ID_FCC_ADD	FortiClient connection added	Information
45058	LOG_ID_FCC_CLOSE	FortiClient closed	Information
45059	LOG_ID_FCC_UPGRADE_SUCC	FortiClient license is upgraded	Notice
45060	LOG_ID_FCC_UPGRADE_FAIL	FortiClient license failed to upgrade	Error
45100	LOG_ID_EC_REG_FAIL	FortiClient registration failed	Warning
45101	LOG_ID_EC_REG_SUCCEED	FortiClient registration succeeded	Notice
45102	LOG_ID_EC_REG_RENEWED	FortiClient registration renewed	Notice
45103	LOG_ID_EC_REG_BLOCK	FortiClient registration blocked	Notice
45104	LOG_ID_EC_REG_UNBLOCK	FortiClient registration unblocked	Notice
45105	LOG_ID_EC_REG_DEREG	FortiClient deregistered	Notice
45106	LOG_ID_EC_REG_LIC_UPGRADED	FortiClient registration license upgraded	Notice
45107	LOG_ID_EC_CONF_DISTRIBUTED	FortiClient configuration distributed	Notice
45108	LOG_ID_EC_FTCL_UNREG	FortiClient unregistered	Notice
45109	LOG_ID_EC_FTCL_LOGOFF	FortiClient logged off	Notice

Message ID	Message	Description	Severity
45110	LOG_ID_EC_FTCL_ENABLE_ NOTSYNC	FortiClient sync with FortiGate disabled	Notice
45111	LOG_ID_EC_REG_SYNC_FAIL	FortiClient registration sync failed	Warning

GTP

Event-GTP log messages record GTP activity. These messages are recorded only when running FortiGate Carrier firmware.

In the log fields, these logs are defined as: type=event; subtype= gtp.

Log Field Name	Log Field Description	Data Type	Length	Value
apn	The access point name.	String	128	
c-bytes	The number of bytes for signaling.	UINT64	20	
c-ggsn	The control plane GGSN IP address for GTP signaling.	IP Address	39	
c-ggsn-teid	The control plane for GGSN TEID (Tunnel endpoint identifier) for signaling.	UINT32	10	
c-gsn	The control plane GSN IP address for GTP signaling.	IP Address	39	
cpaddr	The control plane address (either downlink or uplink).	IP Address	39	
cpdladdr	The control plane downlink IP address.	IP Address	39	
cpdlisraddr	The control plane ISR downlink IP address.	IP Address	39	

Log Field Name	Log Field Description	Data Type	Length	Value
cpdlisrteid	The control plane ISR downlink teid.	UINT32	10	
cpdlteid	The control plane downlink teid.	UINT32	10	
c-pkts	The number of packets for signaling.	UINT64	20	
cpteid	The control plane teid (either downlink or uplink).	UINT32	10	
cpuladdr	The control plane uplink IP address.	IP Address	39	
cpulteid	The control plane uplink teid.	UINT32	10	
c-sgsn	The control plane SGSN IP address for GTP signaling.	IP Address	39	
c-sgsn-teid	The control plane for SGSN TEID (Tunnel endpoint identifier) for signaling.	UINT32	10	
date	The date the log event was generated on the device.	String	10	

Log Field Name	Log Field Description	Data Type	Length	Value
deny_cause		String	25	• adv-policy-filter • apn-filter • ggsn-not-authorized • gtp-in-gtp • imsi-filter • invalid-ie-length • invalid-msg-length • invalid-reserved-field invalid-state • ip-policy • miss-mandatory-ie • msg-filter • non-ip-policy • out-state-ie • out-state-msg • packet-sanity • rate-limited • reserved-ie • reserved-msg • response-without-request • sgsn-no-handover • sgsn-not-authorized • spoof • unknown-gtp-version
devid	The device serial number.	String	16	
dstport	The destination port.	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
dtlexp		String	64	• cant-have-both-ebi-and-lbi cant-have-both-hteid-and-cteid • cause-value-should-be-isr-deactivation • expired-create-bearer-response • expired-create-indirect- tunnel-response • expired-create-response • expired-create-session-response • expired-delete-beaerer-response • expired-delete-indirect- tunnel-response • expired-delete-response expired-delete-session-response • expired-echo-response expired-modified-bearer-response • expired-release-access-bearer-response • expired-update-bearer-response • expired-update-response fteid-shouldnt-exist • header-seq-num-is-missing • hteid-is-zero • ie-is-missing • imsi-shouldnt-exist • invalid-eps-bearer-id • invalid-ie-length • invalid-mcc-mnc • invalid-tid • malformed-extension-header • malformed-p-flag • malformed-piggybacked-msg • malformed-t-flag • neither-hteid-nor-cteidexists • no-tunnel-exists • none • payload-teid-is-zero • response-hteid-doesnt-matchrequest

Log Field Name	Log Field Description	Data Type	Length	Value
duration	The GTP tunnel duration.	UINT32	10	
end-usr-address	The end user address.	The IP address.	39	
from	The Email address (es) from the Email Headers (IMAP/POP3/SMTP).	String	128	
headerteid	The Header (Tunnel endpoint identifier).	UINT32	10	
ietype	The Malformed GTP IE number.	UINT8	3	
imei-sv	International Mobile Equipment Identity or IMEI is a number, usually unique, to identify GSM, WCDMA, and iDEN mobile phones, as well as some satellite phones	String	32	
imsi	The International mobile subscriber ID.	String	16	
level	The log priority level.	String	11	
linked-nsapi	The linked Network Service Access Point identifier.	UINT8	3	
logdesc	The log field description.	String		

Log Field Name	Log Field Description	Data Type	Length	Value
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message Id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
msg-type	The message type.	UINT8	3	
msisdn	The Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card).	String	16	
nsapi	The Network Service Access Point Identifier, an identifier used in cellular data networks.	UINT8	3	
profile	The profile name.	String	64	
rai	The Routing area identification.	String	32	
rat-type	The type of router audit tool.	String	7	
selection	The access point selection.	String	14	
seqnum	The GTP packet sequence number.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
snetwork	The source Network, it's a IE type in GTPv2 packet.	String	64	
srcport	The source port.	UINT16	5	
status	The status of the action the FortiGate unit took when the event occurred.	String	23	• tunnel-limited • tunnel-limited-monitor • user-data
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
to	The email address (es) to the Email Headers (IMAP/POP3/SMTP).	String	512	
tunnel-idx	The VPN tunnel index.	UINT32	10	
type	The log type.	String	16	
u-bytes	The number of bytes used for traffic.	UINT64	20	
u-ggsn	The user plane GGSN IP address for GTP user traffic.	IP Address.	39	

Log Field Name	Log Field Description	Data Type	Length	Value
u-ggsn-teid	The user plane for GGSN TEID (Tunnel endpoint identifier) for signaling.	UINT32	10	
u-gsn	The user plane GSN IP address for GTP user traffic.	IP Address	39	
uli	The user Location Information.	String	32	
u-pkts	The number of packets used for traffic.	UINT64	20	
user_data	The user traffic content inside gtp-u tunnel.	String	256	
u-sgsn	The user plane SGSN IP address for GTP signalling.	IP Address	39	
u-sgsn-teid	The user plane for SGSN TEID (Tunnel endpoint identifier) for signaling.	UINT32	10	
vd	The virtual domain name.	String	32	
version	The software version.	String	64	

GTP Log Messages

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

Message ID	Message	Description	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

High Availability

Event-HA log messages are recorded when FortiGate units are in high availability mode. These log messages describe changes in cluster unit status. The changes in status occur if a cluster unit fails or starts up, or if a link fails or is restored. Each of these messages includes the serial number of the cluster unit reporting the message. You can use the serial number to determine the status of cluster unit that has changed.

In the log fields, these logs are defined as: type=event; subtype= ha.

Log Field Name	Log Field Description	Data Type	Length	Value
activity	The high availability activity message.	String	128	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
devintfname	The high availability device interface name.	String	32	
from_vcluster	The source virtual cluster number.	UINT32	10	
ha_group	The high availability HA group number - can be 1 - 256.	UINT8	3	

Log Field Name	Log Field Description	Data Type	Length	Value
ha_role	The high availability role in the cluster.	String	6	• Master • slave
ha-prio	The high availability priority.	UINT8	3	
hbdn_reason	The heartbeat down reason.	String	18	• Link fail • neighbor-info-lost
ip	The IP address.	IP Address	39	
level	The log priority level.	String	11	
logdesc	The log description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
sn		String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
sync_status	The sync status with the master.	String	11	• in-sync • out-of-sync
sync_type	The sync type with the master.	String	14	• Configurations • external-files
time	The time stamp of the event.	String	8	
to_vcluster	The destination virtual cluster number.	UINT32	10	
type	The log type.	String	16	
vcluster	The virtual cluster ID.	UINT32	10	
vcluster_member	The virtual cluster member ID.	UINT32	10	
vcluster_state	The virtual cluster state.	String	7	• helo • init • standby • work
vd	The virtual domain	String	32	
vdname	The virtual domain name.	String	16	

High Availability Log Messages

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

Message ID	Message	Description	Severity
35001	LOG_ID_HA_SYNC_ VIRDB	HA slave sync Virus database message	Notice
35002	LOG_ID_HA_SYNC_ETDB	HA slave sync Extended database message	Notice
35003	LOG_ID_HA_SYNC_EXDB	HA slave sync Extended database message	Notice
35005	LOG_ID_HA_SYNC_IPS	HA slave sync IDS package message	Notice
35007	LOG_ID_HA_SYNC_AV	HA slave sync AntiVirus package message	Notice
35008	LOG_ID_HA_SYNC_VCM	HA slave sync VCM package message	Notice
35009	LOG_ID_HA_SYNC_CID	HA slave sync CID package message	Notice
35010	LOG_ID_HA_SYNC_FAIL	HA slave sync failed message	Error
37888	MESGID_HA_GROUP_ DELETE	HA group deleted	Notice
37889	MESGID_VC_DELETE	Virtual cluster deleted	Notice
37890	MESGID_VC_MOVE_ VDOM	Virtual cluster VDOM moved	Notice
37891	MESGID_VC_ADD_VDOM	Virtual cluster VDOM added	Notice
37892	MESGID_VC_MOVE_ MEMB_STATE	Virtual cluster member state moved	Notice

Message ID	Message	Description	Severity
37893	MESGID_VC_DETECT_ MEMB_DEAD	Virtual cluster detect member dead	Critical
37894	MESGID_VC_DETECT_ MEMB_JOIN	Virtual cluster detect member joined	Critical
37895	MESGID_VC_ADD_ HADEV	Virtual cluster added HA device interface	Notice
37896	MESGID_VC_DEL_HADEV	Virtual cluster deleted HA device interface	Notice
37897	MESGID_HADEV_READY	HA device interface is ready	Notice
37898	MESGID_HADEV_FAIL	HA device interface failed	Warning
37899	MESGID_HADEV_ PEERINFO	HA device interface peer information	Notice
37900	MESGID_HBDEV_DELETE	Heartbeat device interface deleted	Notice
37901	MESGID_HBDEV_DOWN	Heartbeat device interface is down	Critical
37902	MESGID_HBDEV_UP	Heartbeat device interface is up	Information
37903	MESGID_SYNC_STATUS	The synchronization status with the master is displayed	Information
37904	MESGID_HA_ACTIVITY	Administrator enabled current device as HA master	Notice
37904	MESGID_HA_ACTIVITY	Administrator enabled current device as HA master	Information

Router

Event-Router log messages record events that occur on the FortiGate network interfaces.

In the log fields, these logs are defined as: type=event; subtype= router.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for routing traffic.	String	32	
date	The date the log event was generated on the device	String	10	
devid	The serial number of the device.	String	16	
dhcp_ msg	The DHCP message.	String		
dns_ip	The DNS IP address.	IP Address	39	
dns_ name	The DNS name.	String	64	
dst_int	The destination interface.	String	64	
interface	The interface name.	String	32	
lease	The lease IP address range.	UINT32	10	
level	The log priority level.	String	11	
logdesc	The log description.	String		

Log Field Name	Log Field Description	Data Type	Length	Value
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log sub-type. The last one to five digits are the message id.	String	10	
mac	The MAC address.	String	17	
msg	The activity or event that the FortiGate unit recorded.	String		
service	The service name.	String	64	
src_int	The source interface.	String	64	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
vd	The virtual domain name.	String	32	

Router Log Messages

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

Message ID	Message	Description	Severity
20300	LOG_ID_BGP_NB_STAT_ CHG	BGP neighbor status changed	Unknown
27001	LOG_ID_VRRP_STATE_CHG	VRRP state changed	Information
51000	51000	MAC address neighbor table changed	Information

System

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

In the log fields, these logs are defined as: type=event; subtype= system.

Log Field Name	Log Field Description	Data Type	Length	Value
acktime	The acknowledgment time.	String	24	
act	The accounting state.	String	16	
action	The action the FortiGate unit should take for this firewall policy.	String	32	
addr	The address.	String	80	
alarmid	The alarm ID.	UINT32	10	
assigned	The assigned IP address.	IP Address	39	
bandwidth	The bandwidth of the traffic.	String	42	
banned_rule	The banned rule or reason.	String	36	
banned_src	The banned source.	String	16	• ips • dos • dlp-rule • dlp-compound • av
blocked	The number of blocked messages.	UINT32	10	
cert	The certificate.	String	36	
cfgattr	The configuration attribute.	String		

Log Field Name	Log Field Description	Data Type	Length	Value
cfgobj	The configuration object.	String	256	
cfgpath	The configuration path.	String	128	
cfgtid	The configuration transaction id.	UINT32	10	
chassisid	The chassis ID.	UINT8		
checksum	The number of content checksum blocked messages.	UINT32	10	
cipher		UINT16		
community		String	36	
conserve	The flag for conserve mode.	String	32	
count	The number of dropped SIP packets.	UINT32	10	
cpu	The CPU usage for performance.	UINT8	3	
created		String	64	
crl		String		
daddr	The destination address 'dstip'.	String	80	
daemon	The daemon name.	String	32	
datarange	The data range for reports.	String	50	
date	The date the log event was generated on the device.	String	10	
desc	The description of the event.	String	128	
devid	The serial number of the device.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
dhcp_msg	The DHCP message.	String		
dintf	The device interface.	String	36	
dir		String	8	
disk		UINT8	3	
disklograte	The disk log rate.	UINT64	20	
dns_ip	The DNS IP address.	IP Address	39	
dns_name	The DNS name.	String	64	
dport	The destination port number.	UINT16	5	
dst_int	The interface where the through traffic goes to the public or Internet. For incoming traffic to the firewall, it is “unknown”.	String	64	
dst_port	The destination port number of the TCP or UDP traffic. The destination port is zero for other types of traffic.	UINT16	5	
dstip	The destination IP address.	IP Address	39	
dstport	The destination port.	UINT16	5	
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry.	UINT32	10	
entermargin	The enter margin.	UINT32	10	
error	The error reason for log upload to FortiCloud.	String	256	
exitmargin	The exit margin.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
fams_pause		UINT32	10	
fazlograte	The FortiAnalyzer log rate.	UINT64	20	
field	The field name.	String	32	
file	The file name for a generated report.	String	256	
filesize	The report file size in bytes.	UINT32		
free		String	32	
from	The sender email address for notification.	String	128	
gateway	The gateway IP address for PPPoE status report.	IP Address	39	
green		String	32	
group	The user group name.	String	64	
groupid	The user group IID.	UINT32	10	
handshake	The handshake session ID.	String	32	
hash	A character.	String	32	
hostname	The host name.	String	128	
identidx	The identity index number.	UINT32	10	
infected	The number of infected messages.	UINT32	10	
informationsource	The information source.	String		
intercepted	The number of intercepted messages.	UINT32	10	
interface	The interface name or ID.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
intf	The interface.	String	16	
ip	The IP address.	IP Address	39	
iptype	The IP protocol type.	String	16	
lease	The lease IP address range.	UINT32	10	
len		UINT32	10	
level	The log priority level.	String	11	
limit		UINT32	10	
local	The local IP address.	IP Address	39	
log	The log type.	String	32	
logdesc	The log description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log sub-type. The last one to five digits are the message id.	String	10	
mac	The MAC address.	String	17	
major	The major priority level.	UINT8		
max	The maximum value.	UINT8		
max_minor		UINT8		
mem	The memory usage for per-formance.	UINT8	3	
min	The minimum value.	UINT8		
min_minor		UINT8		

Log Field Name	Log Field Description	Data Type	Length	Value
minor	The minor priority level.	UINT8		
mode	The mode.	String	12	
module	The module name.	String	32	
monitor-name	The monitor name.	String	32	
monitor-type	The monitor type.	String	32	
msg	The activity or event that the FortiGate unit recorded.	String		
msgproto	The message protocol.	String	16	
mtu	The maximum transmission unit.	UINT32	10	
name	The user or host name.	String	128	
nat	The network address translation.	IP Address	39	
new_status	The latest status.	String	512	
new_value	The new virtual domain name.	String	128	
newchannel		UINT8		
newchassisid		UINT8		
newslot		UINT8		

Log Field Name	Log Field Description	Data Type	Length	Value
nf_type	The notification type.	String	14	• bword • file_block • carrier_ep_bwl • flood • dupe • alert • mms_checksum • virus
old_status	The archived status.	String	512	
old_value	The original virtual domain name.	String	16	
oldchannel		UINT8		
oldchassisid		UINT8		
oldslot		UINT8		
passwd	The password.	String	20	
pid	The policy ID.	UINT32	10	
policyid	The policy ID that triggered this log.	UINT32	10	
poolname	The pool name.	String	36	
port	The port number.	UINT16	5	
portbegin		UINT16	5	
portend		UINT16	5	
probeproto		String	16	
process		String		

Log Field Name	Log Field Description	Data Type	Length	Value
processtime	The process time for reports.	UINT32		
profile	The profile name.	String	64	
profile_vd	The virtual domain of the profile.	String	64	
profilegroup	The profile group associated with the firewall policy that traffic used when the log message was recorded.	String	4	
profiletype	The type of profile associated with the firewall policy that traffic used when the log message was recorded.	String	64	
proto	The protocol used.	UINT8	3	
reason	The reason why the log was recorded.	String	256	
received	The number of packets received.	UINT8		
recv_minor		UINT8		
red		String	32	
remote	The remote IP address.	IP Address	39	
reporttype	The report type.	String	20	
saddr	The source address ip. use 'srcip'.	String	80	
scanned	The number of scanned messages.	UINT32	10	
sensor	The sensor name.	String	36	

Log Field Name	Log Field Description	Data Type	Length	Value
serial	The serial number of the log message.	UINT32	10	
serialno	The sserial number of the device.	String	16	
server	The server IP addres.	String	64	
service	The service of where the activity or event occurred, whether it was on a web page using HTTP or HTTPs.	String	64	
sess_duration	The duration of the session.	UINT32	10	
session_id	The session ID.	UINT32	10	
setuprate		UINT64	20	
slot		UINT8		
sn		String	64	
src_int	The source interface - use 'srcintf'.	String	64	
src_port	The source port address.	UINT16	5	
srcip	The source IP address.	IP Address	39	
ssl2	The ssl session.	UINT8		
state		String	64	
status	The status of the action the FortiGate unit took when the event occurred.	String	23	
submodule	The name of the submodule.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
suspicious	The number of suspicious messages.	UINT32	10	
sysconserve	The system conserve mode.	String	32	
time	The time stamp of the event.	String	8	
to	The recipient email addres for notification.	String	512	
total	The total number of IP sessions.	UINT32	10	
totalsession	The total number of sessions.	UINT32	10	
trace_id	The trace ID.	String	32	
type	The log type.	String	16	
ui	The user interface.	String	64	
unit		UINT32	10	
url	The URL address.	String	512	
used		UINT32	10	
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	
version	The software version.	String	64	
vip	The virtual IP address.	String	64	
virus	The name of virus.	String	128	

System Log Messages

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

Message ID	Message	Description	Severity
20000	20000		Debug
20001	LOG_ID_CLIENT_ DISASSOCIATED	Client is disassociated	Information
20001	LOG_ID_CLIENT_ DISASSOCIATED	Client is disassociated	Debug
20002	LOG_ID_DOMAIN_ UNRESOLVABLE	Domain name IP address of the sender is not resolvable	Notice
20003	LOG_ID_MAIL_SENT_FAIL	Alert email send status failed	Notice
20004	LOG_ID_POLICY_TOO_BIG	Policy is too big for the system	Unknown
20005	LOG_ID_PPP_LINK_UP	Modem PPP link is up	Information
20006	LOG_ID_PPP_LINK_DOWN	Modem PPP link is down	Information
20007	20007	Kernel status failed due to exhausted NAT port	Critical
20011	LOG_ID_CLIENT_NEW_ ASSOCIATION	Client is associated	Information
20012	LOG_ID_CLIENT_WPA_1X	Client supports 1X	Information
20013	LOG_ID_CLIENT_WPA_SSN	Client supports WPA authentication	Information
20015	LOG_ID_IEEE802_NEW_ STATION	WPAD: Client supports 801.1x authentication	Information
20016	LOG_ID_MODEM_EXCEED_ REDIAL_COUNT	Modem exceeded redial limit	Information

Message ID	Message	Description	Severity
20017	LOG_ID_MODEM_FAIL_TO_OPEN	Modem failed to open	Information
20020	LOG_ID_MODEM_HOTPLUG	USB modem is removed or deleted	Warning
20020	LOG_ID_MODEM_HOTPLUG	USB modem is removed or deleted	Information
20021	LOG_ID_MAIL_RESENT	Alert email resend status is successful	Information
20025	LOG_ID_REPORTD_REPORT_SUCCESS	Report generated successfully	Notice
20026	LOG_ID_REPORTD_REPORT_FAILURE	Report generation failed	Error
20027	LOG_ID_REPORT_DEL_OLD_REC	Delete report with outdated database records	Warning
20031	LOG_ID_RAD_OUT_OF_MEM	Interface is out of memory	Critical
20032	LOG_ID_RAD_NOT_FOUND	Interface is not found	Critical
20033	LOG_ID_RAD_MOBILE_IPV6	Interface is using Mobile IPv6 extensions	Information
20034	LOG_ID_RAD_IPV6_OUT_OF_RANGE	Interface "MinRtrAdvInterval" using Mobile IPv6 extension is out of range	Critical
20035	LOG_ID_RAD_MIN_OUT_OF_RANGE	Interface "MinRtrAdvInterval" is out of range	Critical
20036	LOG_ID_RAD_MAX_OUT_OF_RANGE	Interface "MaxRtrAdvInterval" using Mobile IPv6 extension is out of range	Critical
20037	LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE	Interface "MaxRtrAdvInterval" is out of range	Critical

Message ID	Message	Description	Severity
20038	LOG_ID_RAD_MTU_OUT_OF_RANGE	Interface "AdvLinkMTU" is out of range	Critical
20039	LOG_ID_RAD_MTU_TOO_SMALL	Interface "AdvLinkMTU" is small	Critical
20040	LOG_ID_RAD_TIME_TOO_SMALL	Interface "AdvReachableTime" is small	Critical
20041	LOG_ID_RAD_HOP_OUT_OF_RANGE	Interface "AdvCurHopLimit" in router advertisement packet is too big	Critical
20042	LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE	Interface "AdvCurHopLimit" in router advertisement packet is out of range	Critical
20043	LOG_ID_RAD_AGENT_OUT_OF_RANGE	Interface "HomeAgentLifetime" in router advertisement packet is out of range	Critical
20044	LOG_ID_RAD_AGENT_FLAG_NOT_SET	Interface "AdvHomeAgentFlag HomeAgentLifetime" in router advertisement packet must be set with HomeAgentInfo	Critical
20045	LOG_ID_RAD_PREFIX_TOO_LONG	Invalid prefix length	Critical
20046	LOG_ID_RAD_PREF_TIME_TOO_SMALL	Interface "AdvValidLifetime" is less than "AdvPreferredLifetime"	Critical
20047	LOG_ID_RAD_FAIL_IPV6_SOCKET	IPv6 RADVD failed to create an IPv6 socket	Critical
20048	LOG_ID_RAD_FAIL_OPT_IPV6_PKTINFO	IPv6 RADVD failed to set IPV6_PKTINFO option	Critical
20049	LOG_ID_RAD_FAIL_OPT_IPV6_CHECKSUM	IPv6 RADVD failed to set IPV6_CHECKSUM option	Critical

Message ID	Message	Description	Severity
20050	LOG_ID_RAD_FAIL_OPT_IPV6_UNICAST_HOPS	IPv6 RADVD failed to set IPV6_UNICAST_HOPS option	Critical
20051	LOG_ID_RAD_FAIL_OPT_IPV6_MULTICAST_HOPS	IPv6 RADVD failed to set IPV6_MULTICAST_HOPS option	Critical
20052	LOG_ID_RAD_FAIL_OPT_IPV6_HOPLIMIT	IPv6 RADVD failed to set IPV6_HOPLIMIT option	Critical
20053	LOG_ID_RAD_FAIL_OPT_IPPROTO_ICMPV6	IPv6 RADVD failed to set ICMPV6_FILTER option	Critical
20054	LOG_ID_RAD_EXIT_BY_SIGNAL	IPv6 RADVD exits due to a signal	Information
20055	LOG_ID_RAD_FAIL_CMDB_QUERY	IPv6 RADVD cannot create cmf_query_create() query to the interface	Critical
20056	LOG_ID_RAD_FAIL_CMDB_FOR_EACH	IPv6 RADVD internal error occurs when cmf_query_for_each() query is used	Critical
20057	LOG_ID_RAD_FAIL_FIND_VIRT_INTF	IPv6 RADVD failed to find a virtual interface with the interface index	Critical
20058	LOG_ID_RAD_UNLOAD_INTF	IPv6 RADVD reloads a specific interface	Information
20059	LOG_ID_RAD_NO_PKT_INFO	IPv6 RADVD received a packet with no pkt_info	Warning
20060	LOG_ID_RAD_INV_ICMPV6_LEN	IPv6 RADVD received an ICMPv6 packet with invalid length	Warning
20061	LOG_ID_RAD_INV_ICMPV6_TYPE	IPv6 RADVD received an unwanted type of ICMPv6 packet	Critical
20062	LOG_ID_RAD_INV_ICMPV6_RA_LEN	IPv6 RADVD received ICMPv6 RA packet with invalid length	Warning

Message ID	Message	Description	Severity
20063	LOG_ID_RAD_ICMPV6_NO_SRC_ADDR	IPv6 RADVD received ICMPv6 RA packet with non-linklocal source address	Warning
20064	LOG_ID_RAD_INV_ICMPV6_RS_LEN	IPv6 RADVD received ICMPv6 RS packet with invalid length	Warning
20065	LOG_ID_RAD_INV_ICMPV6_CODE	IPv6 RADVD received ICMPv6 RS/RA packet with invalid code	Warning
20066	LOG_ID_RAD_INV_ICMPV6_HOP	IPv6 RADVD received ICMPv6 RS/RA packet with wrong hoplimit	Warning
20067	LOG_ID_RAD_MISMATCH_HOP	Interface "AdvCurHopLimit" on local interface does not agree with a remote site	Warning
20068	LOG_ID_RAD_MISMATCH_MGR_FLAG	Interface "AdvManagedFlag" on local interface does not agree with a remote site	Warning
20069	LOG_ID_RAD_MISMATCH_OTH_FLAG	Interface "AdvOtherConfigFlag" on local interface does not agree with a remote site	Warning
20070	LOG_ID_RAD_MISMATCH_TIME	Interface "AdvReachableTime" on local interface does not agree with a remote site	Warning
20071	LOG_ID_RAD_MISMATCH_TIMER	Interface "AdvRetransTimer" on local interface does not agree with a remote site	Warning
20072	LOG_ID_RAD_EXTRA_DATA	IPv6 RADVD finds extra data in RA packet	Critical
20073	LOG_ID_RAD_NO_OPT_DATA	IPv6 RADVD finds a RA packet with no option data	Critical

Message ID	Message	Description	Severity
20074	LOG_ID_RAD_INV_OPT_LEN	Option length is greater than RA packet total length	Critical
20075	LOG_ID_RAD_MISMATCH_ MTU	Interface "AdvLinkMTU" on local interface does not agree with a remote site	Warning
20077	LOG_ID_RAD_MISMATCH_ PREF_TIME	Interface "AdvPreferredLifetime" on our interface does not agree with a remote site	Warning
20078	LOG_ID_RAD_INV_OPT	IPv6 RADVD finds an invalid option in RA packet from a remote site	Critical
20079	LOG_ID_RAD_READY	IPv6 RADVD daemon has started	Information
20080	LOG_ID_RAD_FAIL_TO_RCV	Recvmsg() in IPv6 RADVD failed	Critical
20081	LOG_ID_RAD_INV_HOP	IPv6 RADVD received a packet with a wrong IPV6_HOPLIMIT	Critical
20082	LOG_ID_RAD_INV_PKTINFO	IPv6 RADVD received a packet with a wrong IPV6_PKTINFO	Critical
20083	LOG_ID_RAD_FAIL_TO_ CHECK	IPv6 RADVD failed to check all-routers multicast group membership	Warning
20084	LOG_ID_RAD_FAIL_TO_SEND	IPv6 RADVD failed to send sendmsg ()	Warning
20085	20085	Session status	Information
20086	20086	FMC XH0 crashed	Unknown
20090	LOG_ID_INTF_LINK_STA_ CHG	Interface link status changed	Notice
20099	LOG_ID_INTF_STA_CHG	Interface status changed	Information
20100	20100		Critical

Message ID	Message	Description	Severity
20101	LOG_ID_WEB_LIC_EXPIRE	FortiGuard Web Filter license is expired	Critical
20101	LOG_ID_WEB_LIC_EXPIRE	FortiGuard Web Filter license is expired	Warning
20102	LOG_ID_SPAM_LIC_EXPIRE	FortiGuard AntiSpam license is expired	Critical
20102	LOG_ID_SPAM_LIC_EXPIRE	FortiGuard AntiSpam license is expired	Warning
20103	LOG_ID_AV_LIC_EXPIRE	FortiGuard AntiVirus license is expired	Critical
20103	LOG_ID_AV_LIC_EXPIRE	FortiGuard AntiVirus license is expired	Warning
20104	LOG_ID_IPS_LIC_EXPIRE	FortiGuard IPS license is expired	Warning
20105	LOG_ID_LOG_UPLOAD_SKIP	Log upload to FortiCloud skipped	Warning
20107	LOG_ID_LOG_UPLOAD_ERR	Log upload error	Warning
20108	LOG_ID_LOG_UPLOAD_DONE	Log upload completed	Notice
20110	LOG_ID_HPAPI_ESPD_START	Connection to ESPD has been initialized	Notice
20111	LOG_ID_HPAPI_ESPD_RESET	Connection to ESPD has been reset	Warning
20113	LOG_ID_IPSA_DOWNLOAD_FAIL	Failed to download IPSA database	Error
20114	LOG_ID_IPSA_SELFTEST_FAIL	IPSA self test failed. IPSA disabled	Error
20115	LOG_ID_IPSA_STATUSUPD_FAIL	Failed to update IPSA drive	Error

Message ID	Message	Description	Severity
20200	LOG_ID_FIPS_SELF_TEST	A FIPS CC admistrator has initiated self test	Notice
20201	LOG_ID_FIPS_SELF_ALL_ TEST	A FIPS CC admistrator has initiated all self tests.	Notice
20202	LOG_ID_DISK_FORMAT_ ERROR	Error in disk partitioning or format-ting	Warning
20203	LOG_ID_DAEMON_ SHUTDOWN	Daemon shutdown	Information
20204	LOG_ID_DAEMON_START	Daemon started	Information
20205	LOG_ID_DISK_FORMAT_REQ	Request to format disk	Critical
20206	LOG_ID_DISK_SCAN_REQ	Request to scan disk	Warning
22000	LOG_ID_INV_PKT_LEN	Packet length does not match the specified length in the request header	Warning
22001	LOG_ID_UNSUPPORTED_ PROT_VER	Unsupported protocol version	Warning
22002	LOG_ID_INV_REQ_TYPE	Request type is not supported	Warning
22003	LOG_ID_FAIL_SET_SIG_ HANDLER	Failed to set up a signal handler	Warning
22004	LOG_ID_FAIL_CREATE_ SOCKET	Failed to create a socket	Warning
22005	LOG_ID_FAIL_CREATE_ SOCKET_RETRY	Failed to create a UDP socket to receive URL request	Warning
22006	LOG_ID_FAIL_REG_CMDB_ EVENT	Failed to register for CMDB events	Warning

Message ID	Message	Description	Severity
22009	LOG_ID_FAIL_FIND_AV_PROFILE	Failed to find AntiVirus profile by ID	Warning
22009	LOG_ID_FAIL_FIND_AV_PROFILE	Failed to find AntiVirus profile by ID	Debug
22010	LOG_ID_SENDTO_FAIL	Failed to send URL filter packet	Error
22011	22011	Kernel enters conserve mode	Unknown
22012	22012	Kernel leaves conserve mode	Unknown
22013	22013	IP pool PBA block exhaust	Alert
22014	22014	IP pool PBA NATIP exhaust	Alert
22014	22014	IP pool PBA NATIP exhaust	Notice
22015	LOG_ID_EXCEED_VD_RES_LIMIT	Exceeded VDOM resource limit	Notice
22016	22016	Deallocate IP pool PBA	Notice
22020	LOG_ID_FAIL_CREATE_HA_SOCKET	Failed to create URL filter connection for HA slaves	Warning
22021	LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY	Failed to create URL filter connection to HA master	Warning
22100	LOG_ID_QUAR_DROP_TRAN_JOB	Transfer failed, files dropped by quarantine daemon	Warning
22101	LOG_ID_QUAR_DROP_TLL_JOB	Transfer failed, poor network connection	Warning
22102	LOG_ID_LOG_DISK_FAILURE	Log disk failure is imminent	Critical
22103	LOG_ID_QUAR_DAILY_LIMIT_REACHED	FortiCloud sandbox daily limit reaced	Warning
22104	LOG_ID_POWER_RESTORE	Power supply restored	Critical

Message ID	Message	Description	Severity
22104	LOG_ID_POWER_RESTORE	Power supply restored	Notice
22105	LOG_ID_POWER_FAILURE	Power supply failed	Critical
22105	LOG_ID_POWER_FAILURE	Power supply failed	Warning
22106	LOG_ID_POWER_OPTIONAL_NOT_DETECTED	Power supply not detected	Information
22106	LOG_ID_POWER_OPTIONAL_NOT_DETECTED	Power supply not detected	Warning
22107	LOG_ID_VOLT_ANOM		Warning
22108	LOG_ID_FAN_ANOM		Warning
22109	LOG_ID_TEMP_TOO_HIGH	Temperature too high	Warning
22110	LOG_ID_SPARE_BLOCK_LOW	Available spare blocks of boot device is 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	Certificate will be auto-updated	Warning
22201	LOG_ID_AUTO_GEN_CERT	Certificate will be auto-regenerated	Warning
22201	LOG_ID_AUTO_GEN_CERT	Certificate will be auto-regenerated	Information
22202	LOG_ID_AUTO_UPT_CERT_FAIL	Certificate failed to auto-update	Error
22203	LOG_ID_AUTO_GEN_CERT_FAIL	Certificate failed to auto-generate	Error
22700	LOG_ID_IPS_FAIL_OPEN	IPS session scan resumed	Critical

Message ID	Message	Description	Severity
22800	LOG_ID_SCAN_SERV_FAIL	System scan services session failed	Critical
22801	LOG_ID_SCAN_LEAVE_ CONSERVE_MODE	System scan services exited conserve mode	Critical
22802	LOG_ID_SYS_ENTER_ CONSERVE_MODE	System entered conserve mode	Critical
22803	LOG_ID_SYS_LEAVE_ CONSERVE_MODE	System exited conserve mode	Critical
22804	LOG_ID_LIC_STATUS_CHG	License has changed	Critical
22805	LOG_ID_FAIL_TO_VALIDATE_ LIC	License cannot be validated	Warning
22806	LOG_ID_DUP_LIC	Detected duplicate license	Warning
22810	LOG_ID_SCAN_ENTER_ CONSERVE_MODE	System scan services entered conserve mode	Critical
22900	LOG_ID_CAPUTP_SESSION	CAPUTP session status	Notice
22901	LOG_ID_FAZ_CON	Connected to FortiAnalyzer	Notice
22902	LOG_ID_FAZ_DISCON	Disconnected from FortiAnalyzer	Notice
22903	LOG_ID_FAZ_CON_ERR	Failed to connect to FortiAnalyzer	Critical
22916	LOG_ID_FDS_STATUS	FortiGuard Message Service status	Notice
22917	LOG_ID_FDS_SMS_QUOTA	SMS quota is reached	Notice
22921	LOG_ID_EVENT_ROUTE_ INFO_CHANGED	Routing information is changed because link monitor entry changes its configuration or status	Critical
22922	LOG_ID_EVENT_LINK_ MONITOR_STATUS	Link Monitor status	Notice

Message ID	Message	Description	Severity
22923	LOG_ID_EVENT_VWL_LQTY_STATUS	Virtual WAN Link status	Notice
22924	LOG_ID_EVENT_VWL_VOLUME_STATUS	Virtual WAN Link volume status	Notice
26001	LOG_ID_DHCP_MSG	DHCP request and response log	Information
26001	LOG_ID_DHCP_MSG	DHCP request and response log	Unknown
26002	LOG_ID_DHCP_NO_SHARE_NET	No shared network found	Error
26003	LOG_ID_DHCP_STAT	DHCP statistics status	Information
26004	LOG_ID_DHCP_MULT_SUB_NET	Address range spans multiple sub-nets	Error
26005	LOG_ID_DHCP_INV_ADDR_RANGE	Address range does not belong to the network	Error
26006	LOG_ID_DHCP_LEASE_USAGE	DHCP lease usage	Warning
29001	LOG_ID_PPPD_MSG	PPPD status message	Unknown
29002	LOG_ID_PPPD_AUTH_SUC	PPPD authentication success	Notice
29002	LOG_ID_PPPD_AUTH_SUC	PPPD authentication success	Debug
29003	LOG_ID_PPPD_AUTH_FAIL	PPPD authentication failure	Notice
29009	LOG_ID_PPPOE_STATUS_REPORT	PPPoE status report	Notice
29011	LOG_ID_PPPD_FAIL_TO_EXEC	PPPD cannot execute a program	Error
29012	LOG_ID_PPP_OPT_ERR	PPP has received incorrect options	Unknown
29013	LOG_ID_PPPD_START	PPPD is started	Notice

Message ID	Message	Description	Severity
29014	LOG_ID_PPPD_EXIT	PPPD is exiting	Information
29015	LOG_ID_PPP_RCV_BAD_PEER_IP	PPP has received incorrect peer IP address	Error
29016	LOG_ID_PPP_RCV_BAD_LOCAL_IP	PPP has received incorrect local IP address	Error
29017	LOG_ID_PPP_OPT_NOTIF	PPP has received incorrect notifications	Unknown
29020	LOG_ID_WIRELESS_SET_FAIL	Wireless set command failed	Notice
29020	LOG_ID_WIRELESS_SET_FAIL	Wireless set command failed	Unknown
29021	LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED	Failed SNMP query	Warning
32001	LOG_ID_ADMIN_LOGIN_SUCC	Administrator logged in successfully	Information
32002	LOG_ID_ADMIN_LOGIN_FAIL	Failed administrator login attempt	Alert
32003	LOG_ID_ADMIN_LOGOUT	Administrator logged out	Information
32005	LOG_ID_ADMIN_OVERIDE_VDOM	Administrator overrode VDOM successfully	Information
32006	LOG_ID_ADMIN_ENTER_VDOM	A super admin has entered this VDOM	Information
32007	LOG_ID_ADMIN_LEFT_VDOM	A super admin has left the current VDOM	Information
32008	LOG_ID_VIEW_LOG_FAIL	Failed to view log	Warning
32009	LOG_ID_SYSTEM_START	FortiGate started	Information
32010	LOG_ID_DISK_LOG_FULL	DLP archive is full	Emergency

Message ID	Message	Description	Severity
32010	LOG_ID_DISK_LOG_FULL	DLP archive is full	Information
32010	LOG_ID_DISK_LOG_FULL	DLP archive is full	Unknown
32011	LOG_ID_LOG_ROLL	Disk log rotation	Notice
32012	LOG_ID_FIPS_LEAVE_ERR_MOD	FIPS CC exiting error mode	Information
32014	LOG_ID_CS_LIC_EXPIRE	FortiGuard customer support license expiring	Warning
32015	LOG_ID_DISK_LOG_USAGE	Alert email log full	Warning
32018	LOG_ID_FIPS_ENTER_ERR_MOD	FIPS CC error mode	Emergency
32020	LOG_ID_SSH_CORRPUT_MAC	Corrupted MAC address detected	Warning
32021	LOG_ID_ADMIN_LOGIN_DISABLE	Administrator login is disabled	Alert
32022	LOG_ID_VDOM_ENABLED	VDOM enabled	Notice
32023	LOG_ID_MEM_LOG_FULL	Memory log full	Warning
32023	LOG_ID_MEM_LOG_FULL	Memory log full	Information
32024	LOG_ID_ADMIN_PASSWD_EXPIRE	Administrator password has expired	Notice
32026	LOG_ID_STORE_CONF_FAIL	Cannot store configuration due to first line error	Critical
32027	LOG_ID_VIEW_LOG_SUCC	View disk logs	Notice
32028	LOG_ID_LOG_DEL_DIR	Disk log directory deleted	Information
32029	LOG_ID_LOG_DEL_FILE	Disk log file deleted	Warning

Message ID	Message	Description	Severity
32030	LOG_ID_SEND_FDS_STAT	Sent FDS statistics status	Notice
32035	LOG_ID_VDOM_DISABLED	VDOM disabled	Notice
32040	LOG_ID_REPORT_DELETED	Report deleted	Information
32045	LOG_ID_MGR_LIC_EXPIRE	FortiGuard management service license is expiring	Warning
32048	LOG_ID_SCHEDULE_EXPIRE	One time schedule is expiring	Warning
32049	LOG_ID_FC_EXPIRE	FortiCloud license is expiring	Warning
32051	LOG_ID_LOG_UPLOAD	Start uploading disk logs from VDOM	Notice
32086	LOG_ID_ENTER_ TRANSPARENT	System has been changed to transparent mode via LCD	Warning
32087	LOG_ID_ENTER_NAT	System has been changed to NAT mode via LCD	Warning
32095	LOG_ID_GUI_CHG_SUB_ MODULE	An administrator has performed an action on the firewall via GUI	Warning
32096	LOG_ID_GUI_DOWNLOAD_ LOG	An administrator has downloaded a log file from the firewall via GUI	Warning
32100	LOG_ID_FORTI_TOKEN_ SYNC	FortiToken synchronization	Warning
32101	LOG_ID_LCD_CHG_CONF	An administrator has changed configuration from LCD	Notice
32102	LOG_ID_CHG_CONFIG	An administrator has changed the configuration	Unknown
32103	LOG_ID_NEW_FIRMWARE	A new firmware image is available on FortiGuard	Notice
32120	LOG_ID_RPT_ADD_DATASET	Report dataset added	Notice

Message ID	Message	Description	Severity
32122	LOG_ID_RPT_DEL_DATASET	Report dataset deleted	Notice
32125	LOG_ID_RPT_ADD_CHART	Report chart widget added	Notice
32126	LOG_ID_RPT_DEL_CHART	Report chart widget deleted	Notice
32129	LOG_ID_ADD_GUEST	New guest user added	Notice
32130	LOG_ID_CHG_USER	A local user's setting changed	Notice
32131	LOG_ID_DEL_GUEST	Guest user deleted	Notice
32132	LOG_ID_ADD_USER	A new local user is added	Notice
32138	LOG_ID_REBOOT	Device rebooted	Critical
32139	LOG_ID_UPD_SIGN_DB	Updated GeoIP object	Critical
32139	LOG_ID_UPD_SIGN_DB	Updated GeoIP object	Warning
32139	LOG_ID_UPD_SIGN_DB	Updated GeoIP object	Notice
32140	LOG_ID_NTP_SVR_STAUS_CHG	NTP server status has changed	Notice
32142	LOG_ID_BACKUP_CONF	Backup system configuration	Alert
32142	LOG_ID_BACKUP_CONF	Backup system configuration	Warning
32142	LOG_ID_BACKUP_CONF	Backup system configuration	Error
32142	LOG_ID_BACKUP_CONF	Backup system configuration	Notice
32148	LOG_ID_GET_CRL	User requested a CRL update	Notice
32149	LOG_ID_COMMAND_FAIL	Command failed	Notice
32151	LOG_ID_ADD_IP6_LOCAL_POL	A new IPv6 firewall local in policy is added	Notice

Message ID	Message	Description	Severity
32152	LOG_ID_CHG_IP6_LOCAL_POL	A IPv6 firewall local in policy setting has changed	Notice
32153	LOG_ID_DEL_IP6_LOCAL_POL	A IPv6 firewall local in policy is deleted	Notice
32155	LOG_ID_ACT_FTOKEN_REQ	FortiToken request to activate	Notice
32156	LOG_ID_ACT_FTOKEN_SUCC	FortiToken activation successful	Notice
32157	LOG_ID_SYNC_FTOKEN_SUCC	Successfully synchronized FortiToken	Notice
32158	LOG_ID_SYNC_FTOKEN_FAIL	Failed to synchronize FortiToken	Notice
32159	LOG_ID_ACT_FTOKEN_FAIL	FortiToken activation failed	Notice
32168	LOG_ID_REACH_VDOM_LIMIT	Failed to add a new entry - VDOM limit reached	Notice
32170	LOG_ID_ALARM_MSG	Alarm message is created	Alert
32171	LOG_ID_ALARM_ACK	Alarm is acknowledged	Alert
32172	LOG_ID_ADD_IP4_LOCAL_POL	A new IPv4 firewall local in policy is added	Notice
32173	LOG_ID_CHG_IP4_LOCAL_POL	An IPv4 firewall local in policy's setting has changed	Notice
32174	LOG_ID_DEL_IP4_LOCAL_POL	An IPv4 firewall local in policy is deleted	Notice
32188	LOG_ID_SSL_PROXY_CA_INIT_FAIL	SSL Proxy CA initialization failed	Warning
32188	LOG_ID_SSL_PROXY_CA_INIT_FAIL	SSL Proxy CA initialization failed	Notice
32200	LOG_ID_SHUTDOWN	Device shutdown	Critical

Message ID	Message	Description	Severity
32201	LOG_ID_LOAD_IMG_SUCC	Loaded image does not support FIPS CC mode	Critical
32202	LOG_ID_RESTORE_IMG	Image restored	Critical
32203	LOG_ID_RESTORE_CONF	Configuration restored	Critical
32203	LOG_ID_RESTORE_CONF	Configuration restored	Warning
32203	LOG_ID_RESTORE_CONF	Configuration restored	Notice
32204	LOG_ID_RESTORE_FGD_SVR	FortiGuard service restored	Critical
32204	LOG_ID_RESTORE_FGD_SVR	FortiGuard service restored	Notice
32205	LOG_ID_RESTORE_VDOM_LIC	VM license restored	Critical
32205	LOG_ID_RESTORE_VDOM_LIC	VM license restored	Notice
32206	LOG_ID_RESTORE_SCRIPT	Script restored	Warning
32207	LOG_ID_RETRIEVE_CONF_LIST	Failed to retrieve configuration list	Warning
32208	LOG_ID_IMP_PKCS12_CERT	Imported "PKCS12" certificate	Critical
32209	LOG_ID_RESTORE_USR_DEF_IPS	Restored the user defined IPS signatures	Critical
32209	LOG_ID_RESTORE_USR_DEF_IPS	Restored the user defined IPS signatures	Notice
32210	LOG_ID_BACKUP_IMG	Firmware image successfully backed up	Notice
32211	LOG_ID_UPLOAD_REVISION	Upload to flash disk successful	Notice
32212	LOG_ID_DEL_REVISION	Revision database deleted successfully	Notice

Message ID	Message	Description	Severity
32213	LOG_ID_RESTORE_ TEMPLATE	Template restored	Warning
32214	LOG_ID_RESTORE_FILE	System failed to restore	Warning
32215	LOG_ID_UPT_IMG	An administator loaded a wrong image	Critical
32217	LOG_ID_UPD_IPS	An administator updated the IPS package via SCP	Warning
32217	LOG_ID_UPD_IPS	An administator updated the IPS package via SCP	Notice
32218	LOG_ID_UPD_DLP	An administator failed to update the DLP fingerprint database via SCP	Warning
32219	LOG_ID_BACKUP_OUTPUT	An administator backed up the result of standardized error output via SCP	Warning
32220	LOG_ID_BACKUP_COMMAND	An administator backed up the result of batch mode commands via SCP	Warning
32221	LOG_ID_UPD_VDOM_LIC	An administator installed the VM license via SCP	Warning
32222	LOG_ID_GLB_SETTING_CHG	An administator changed a global setting	Notice
32223	LOG_ID_BACKUP_USER_ DEF_IPS	Failed to backup user defined IPS signatures	Error
32223	LOG_ID_BACKUP_USER_ DEF_IPS	Failed to backup user defined IPS signatures	Notice
32224	LOG_ID_BACKUP_LOG	Disk logs backed up	Notice

Message ID	Message	Description	Severity
32225	LOG_ID_DEL_ALL_REVISION	Revision database corruption detected. Database is reset	Notice
32226	LOG_ID_LOAD_IMG_FAIL	Failed to load image	Critical
32240	LOG_ID_SYS_USB_MODE	System is operating in USB mode	Critical
32252	LOG_ID_FACTORY_RESET	An administator reset factory settings	Critical
32253	LOG_ID_FORMAT_RAID	An administrator formatted the RAID disk	Critical
32254	LOG_ID_ENABLE_RAID	An administator enabled RAID	Critical
32255	LOG_ID_DISABLE_RAID	An administator disabled RAID	Critical
32300	LOG_ID_UPLOAD_RPT_IMG	Upload the report image file	Notice
32301	LOG_ID_ADD_VDOM	VDOM added	Notice
32302	LOG_ID_DEL_VDOM	VDOM deleted	Notice
32340	LOG_ID_LOG_DISK_UNAVAIL	Disk is unavailable	Critical
32340	LOG_ID_LOG_DISK_UNAVAIL	Disk is unavailable	Warning
32341	LOG_ID_LOG_DISK_ DEFAULT_DISABLED	Disk log status has changed	Notice
32400	LOG_ID_CONF_CHG	Configuration has changed	Alert
32545	LOG_ID_SYS_RESTART	System is rebooted due to scheduled daily restart action	Critical
32546	LOG_ID_APPLICATION_ CRASH	Application crashed	Warning
36880	LOG_ID_EVENT_SYSTEM_ MAC_HOST_STORE_LIMIT	Number of detected devices exceeds limit that can be persistently stored	Warning

Message ID	Message	Description	Severity
38400	LOGID_EVENT_NOTIF_SEND_SUCC	The system successfully sent a notification message	Notice
38401	LOGID_EVENT_NOTIF_SEND_FAIL	The system was unable to send a notification message	Warning
38402	LOGID_EVENT_NOTIF_DNS_FAIL	The system was unable to resolve an MMSC hostname	Notice
38403	LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE	Insufficient system resource notification	Critical
38404	LOGID_EVENT_NOTIF_HOSTNAME_ERROR	Unable to resolve FortiGuard hostname	Error
38405	LOGID_NOTIF_CODE_SENDTO_SMS_PHONE	Sent token activation code notification for phone	Notice
38406	LOGID_NOTIF_CODE_SENDTO_SMS_TO	Sent token activation code notification for SMS	Notice
38407	LOGID_NOTIF_CODE_SENDTO_EMAIL	Sent token activation code notification for email	Notice
40704	LOG_ID_EVENT_SYS_PERF	System performance statistics	Notice
41000	LOG_ID_UPD_FGT_SUCC	An administrator has updated the FortiGate successfully	Notice
41001	LOG_ID_UPD_FGT_FAIL	An administrator has failed to update the FortiGate	Critical
41002	LOG_ID_UPD_SRC_VIS	The source visibility signature package is updated	Notice
41003	LOG_ID_INVALID_UPD_LIC	Invalid update license	Critical
41005	LOG_ID_UPD_VCM	An administrator has updated the VCM plugin successfully	Notice

Message ID	Message	Description	Severity
43264	LOGID_MMS_STATS	MMS statistics	Information
43776	LOGID_EVENT_NAC_ QUARANTINE	NAC anomaly quarantine	Notice
43800	LOG_ID_EVENT_ELBC_ BLADE_JOIN	Blade ready to process traffic	Critical
43801	LOG_ID_EVENT_ELBC_ BLADE_LEAVE	Blade is not ready to process traffic	Critical
43802	LOG_ID_EVENT_ELBC_ MASTER_BLADE_FOUND	Master blade found	Critical
43803	LOG_ID_EVENT_ELBC_ MASTER_BLADE_LOST	Master blade lost	Critical
43804	LOG_ID_EVENT_ELBC_ MASTER_BLADE_CHANGE	Master blade changed	Critical
43805	LOG_ID_EVENT_ELBC_ ACTIVE_CHANNEL_FOUND	ELBC channel is active	Critical
43806	LOG_ID_EVENT_ELBC_ ACTIVE_CHANNEL_LOST	ELBC channel is inactive	Critical
43807	LOG_ID_EVENT_ELBC_ ACTIVE_CHANNEL_CHANGE	ELBC channel failover	Critical
43808	LOG_ID_EVENT_ELBC_ CHASSIS_ACTIVE	ELBC chassis is active	Critical
43809	LOG_ID_EVENT_ELBC_ CHASSIS_INACTIVE	ELBC chassis is inactive	Critical
44544	LOGID_EVENT_CONFIG_ PATH	Configured path	Information
44545	LOGID_EVENT_CONFIG_OBJ	Configured object	Information

Message ID	Message	Description	Severity
44546	LOGID_EVENT_CONFIG_ ATTR	Configured attribute	Information
44547	LOGID_EVENT_CONFIG_ OBJATTR	Object attribute configured	Information
45000	LOG_ID_VSD_SSL_RCV_HS	SSL handshake received	Debug
45001	LOG_ID_VSD_SSL_RCV_ WRG_HS	SSL received incorrect handshake message	Error
45002	LOG_ID_VSD_SSL_SENT_HS	SSL handshake sent	Debug
45003	LOG_ID_VSD_SSL_WRG_HS_ LEN	SSL handshake has invalid length	Error
45004	LOG_ID_VSD_SSL_RCV_CCS	SSL ChangeCipherSpec received	Debug
45005	LOG_ID_VSD_SSL_RSA_DH_ FAIL	Verification of Diffie-Hellman parameters failed	Error
45006	LOG_ID_VSD_SSL_SENT_CCS	SSL ChangeCipherSpec sent	Debug
45007	LOG_ID_VSD_SSL_BAD_HASH	Hash in SSL Finished does not match calculated hash	Error
45009	LOG_ID_VSD_SSL_DECRY_ FAIL	SSL decryption failed	Error
45010	LOG_ID_VSD_SSL_SESSION_ CLOSED	SSL session closed	Debug
45011	LOG_ID_VSD_SSL_LESS_ MINOR	SSL minor version is less than configured minimum value	Error
45012	LOG_ID_VSD_SSL_REACH_ MAX_CON	SSL maximum connection limit reached	Warning
45013	LOG_ID_VSD_SSL_NOT_ SUPPORT_CS	SSL CipherSuites not supported	Error

Message ID	Message	Description	Severity
45016	LOG_ID_VSD_SSL_HS_FIN	SSL handshake complete	Debug
45017	LOG_ID_VSD_SSL_HS_TOO_LONG	SSL handshake is too long	Error
45018	LOG_ID_VSD_SSL_MORE_MINOR	SSL minor version larger than configured maximum value	Debug
45019	LOG_ID_VSD_SSL_SENT_ALERT_ERR	SSL alert error sent	Error
45020	LOG_ID_VSD_SSL_SESSION_EXPIRE	SSL session state expired	Debug
45021	LOG_ID_VSD_SSL_SENT_ALERT	SSL alert sent	Debug
45022	LOG_ID_VSD_SSL_RCV_CH	SSL Client Hello received	Debug
45023	LOG_ID_VSD_SSL_RCV_SH	SSL Server Hello received	Debug
45024	LOG_ID_VSD_SSL_SENT_SH	SSL Server Hello sent	Debug
45025	LOG_ID_VSD_SSL_RCV_ALERT	SSL alert received	Error
45025	LOG_ID_VSD_SSL_RCV_ALERT	SSL alert received	Debug
45027	LOG_ID_VSD_SSL_INVALID_CONT_TYPE	Invalid SSL Content Type	Error
45029	LOG_ID_VSD_SSL_BAD_CCS_LEN	SSL ChangeCipherSpec has incorrect length	Error
45031	LOG_ID_VSD_SSL_BAD_DH	SSL Diffie-Hellman has incorrect value	Error
45032	LOG_ID_VSD_SSL_PUB_KEY_TOO_BIG	SSL certificate public key is too big for SSL offloading	Error

Message ID	Message	Description	Severity
45033	LOG_ID_VSD_SSL_NOT_ SUPPORT_CM	SSL Compression Methods are not supported	Error
45034	LOG_ID_VSD_SSL_SERVER_ KEY_HASH_ALGORITHM_ MISMATCH	Server Key Exchange hash algorithm mismatch	Error
45035	LOG_ID_VSD_SSL_SERVER_ KEY_SIGNATURE_ ALGORITHM_MISMATCH	Server Key Exchange signature algorithm mismatch	Error
46000	LOG_ID_VIP_REAL_SVR_ENA	VIP real server has been enabled	Notice
46001	LOG_ID_VIP_REAL_SVR_DISA	VIP real server has been disabled	Alert
46002	LOG_ID_VIP_REAL_SVR_UP	VIP real server is active	Notice
46003	LOG_ID_VIP_REAL_SVR_ DOWN	VIP real server is down	Alert
46004	LOG_ID_VIP_REAL_SVR_ ENT_HOLDDOWN	VIP real server has started hold-down period	Notice
46005	LOG_ID_VIP_REAL_SVR_ FAIL_HOLDDOWN	VIP real server has failed during hold-down period	Alert
46006	LOG_ID_VIP_REAL_SVR_FAIL	Health monitor has detected VIP real server health problem	Debug
46400	LOG_ID_EVENT_EXT_SYS	FortiExtender system activity	Unknown
46401	LOG_ID_EVENT_EXT_LOCAL	FortiExtender AC activity	Unknown
46402	LOG_ID_EVENT_EXT_ REMOTE	Remote FortiExtender activity	Unknown
47201	LOG_ID_AMC_ENTER_ BYPASS	AMC card entered bypass mode	Emergency
47202	LOG_ID_AMC_EXIT_BYPASS	AMC card exited bypass mode	Emergency

Message ID	Message	Description	Severity
47203	LOG_ID_ENTER_BYPASS	Bypass ports pair entered bypass mode	Emergency
47204	LOG_ID_EXIT_BYPASS	Bypass ports pair exited bypass mode	Emergency

User

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

In the log fields, these logs are defined as: type=event; subtype= user.

Log Field Name	Log Field Description	Data Type	Length	Value
acct_stat	The accounting state (RADIUS).	String	14	• Accounting-Off • Accounting-On • Interim-Update • start • stop
action	The action the FortiGate unit should take for this policy.	String	32	
adgroup	The active directory group name.	String	128	
authproto	The protocol that initiated the authentication.	String	64	
carrier_ep	The FortiOS Carrier end-point identification.	String	64	
category	The log category.	UINT32	10	
count		UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
dstip	The destination IP address.	IP Address	39	
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry.	UINT32	10	
expiry	The FortiGuard override expiry timestamp.	String	64	
group	The user name group.	String	64	
initiator	The original login user name for Fortiguard override.	String	64	
level	The log priority level.	String	11	
logdesc	The log description.	String		

Log Field Name	Log Field Description	Data Type	Length	Value
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
oldwprof	The old Web Filter profile.	String	64	
policyid	The policy ID that triggered this log.	UINT32	10	
poolname	The pool name.	String	36	
portbegin		UINT16	5	
portend		UINT16	5	
proto	The protocol name.	UINT8	3	
reason	The reason why the log was recorded.	String	256	
rsso_key		String	64	
scope		String	16	
server		String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
srcip	The source IP address.	IP Address	39	
status	The status of the action the FortiGate unit took when the event occurred.	String	23	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
ui	The user interface.	String	64	
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	

User Log Messages

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

Message ID	Message	Description	Severity
38010	LOG_ID_FIPS_ENCRY_FAIL	FIPS CC encryption failed	Alert
38011	LOG_ID_FIPS_DECRY_FAIL	FIPS CC decryption failed	Alert
38031	LOG_ID_FSSO_LOGON	FSSO logon authentication status	Notice
38032	LOG_ID_FSSO_LOGOFF	FSSO logoff authentication status	Notice
38033	LOG_ID_FSSO_SVR_STATUS	FSSO Active Directory server authentication status	Notice
38656	LOGID_EVENT_RAD_RPT_ PROTO_ERROR	RADIUS protocol/profile error missing packet	Notice
38657	LOGID_EVENT_RAD_RPT_ PROF_NOT_FOUND	RADIUS protocol/profile not found	Notice
38658	LOGID_EVENT_RAD_RPT_CTX_ NOT_FOUND	RADIUS protocol/profile CTX not found	Notice
38659	LOGID_EVENT_RAD_RPT_ ACCT_STOP_MISSED	RADIUS protocol/profile account stopped	Notice
38660	LOGID_EVENT_RAD_RPT_ ACCT_EVENT	RADIUS protocol/profile error missing stop packet	Notice
38661	LOGID_EVENT_RAD_RPT_ OTHER	RADIUS protocol/profile error, missing stop packet, accounting or other report	Notice
38662	LOGID_EVENT_RAD_STAT_ PROTO_ERROR	RADIUS protocol errors	Notice
38663	LOGID_EVENT_RAD_STAT_ PROF_NOT_FOUND	RADIUS start or interim-update packet received with missing or invalid profile specified	Notice

Message ID	Message	Description	Severity
38665	LOGID_EVENT_RAD_STAT_ ACCT_STOP_MISSED	RADIUS stop packet was missed	Notice
38666	LOGID_EVENT_RAD_STAT_ ACCT_EVENT	RADIUS accounting event	Notice
38667	LOGID_EVENT_RAD_STAT_ OTHER	RADIUS other accounting event	Notice
38668	LOGID_EVENT_RAD_STAT_EP_ BLK	RADIUS endpoint block event	Notice
43011	LOG_ID_EVENT_AUTH_TIME_ OUT	Authentication timed out	Notice
43012	LOG_ID_EVENT_AUTH_FSAE_ AUTH_SUCCESS	FSSO authentication successful	Notice
43013	LOG_ID_EVENT_AUTH_FSAE_ AUTH_FAIL	FSSO authentication failed	Notice
43014	LOG_ID_EVENT_AUTH_FSAE_ LOGON	FSSO logon authentication status	Notice
43015	LOG_ID_EVENT_AUTH_FSAE_ LOGOFF	FSSO logoff authentication status	Notice
43016	LOG_ID_EVENT_AUTH_NTLM_ AUTH_SUCCESS	NTLM authentication successful	Notice
43017	LOG_ID_EVENT_AUTH_NTLM_ AUTH_FAIL	NTLM authentication failed	Notice
43018	LOG_ID_EVENT_AUTH_ FGOVRD_FAIL	FortiGuard override failed	Warning
43020	LOG_ID_EVENT_AUTH_ FGOVRD_SUCCESS	FortiGuard override successful	Notice

Message ID	Message	Description	Severity
43025	LOG_ID_EVENT_AUTH_PROXY_SUCCESS	WADauthentication HTTP proxy successful	Notice
43026	LOG_ID_EVENT_AUTH_PROXY_FAILED	WAD authentication FTP proxy failed	Notice
43027	LOG_ID_EVENT_AUTH_PROXY_TIME_OUT	WAD authentication proxy timed out	Notice
43028	LOG_ID_EVENT_AUTH_PROXY_AUTHORIZATION_FAILED	WAD authentication HTTP proxy authorization failed	Notice
43029	LOG_ID_EVENT_AUTH_WARNING_SUCCESS	FortiGuard authentication override successful	Notice
43030	LOG_ID_EVENT_AUTH_WARNING_TBL_FULL	FortiGuard authentication override failed	Warning
43040	LOG_ID_EVENT_AUTH_LOGOUT	FortiGuard authentication status	Notice

VPN

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

In the log fields, these logs are defined as: type=event; subtype= vpn.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this firewall policy.	String	32	
assignip	The assigned IP address.	IP Address	39	
cert-type	The certification type.	String	6	• CA • CRL • Local • Remote
cookies	The cookies stored during the log event.	String	64	
date	The date the log event was generated on the device.	String	10	
devid	The serial number of the device.	String	16	
dir	The direction (inbound or outbound) of packets.	String	8	

Log Field Name	Log Field Description	Data Type	Length	Value
dst_host	The destination host name.	String	64	
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry.	UINT32	10	
error_num	The error number.	UINT	32	
espauth	The ESP authentication.	String	17	• HMAC_SHA1 • HMAC_MD5 • HMAC_SHA256
esptransform	The ESP tranfrom value.	String	8	• ESP_NULL • ESP_DES • ESP_3DES • ESP_AES
exch	The exchange name.	String	12	• NSA_INIT • AUTH • CREATE_CHILD
group	The user name group.	String	64	
in_spi	The remote SPI in IPsec VPN configuration.	String	16	
init	The interface name.	String	6	• local • remote
level	The log priority level.	String	11	

Log Field Name	Log Field Description	Data Type	Length	Value
locip	The local IP address.	IP Address	39	
locport	The local port.	UINT16	5	
logdesc	The log description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
method	The HTTP method.	String	64	• IP • Domain
mode	The mode.	String	12	• aggressive • main • quick • xauth • xauth_client
msg	The activity or event that the FortiGate unit recorded.	String		
name		String	128	
nextstat	The time interval in seconds for the next statistics.	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
out_spi	The local SPI in IPsec VPN configuration.	String	16	
outintf	The out interface.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
peer_notif	The peer notification.	String	25	• NOT-APPLICABLE • INVALID-PAYLOAD-TYPE • DOI-NOT-SUPPORTED • SITUATION-NOT-SUPPORTED • INVALID-COOKIE • INVALID-MAJOR-VERSION • INVALID-MINOR-VERSION • INVALID-EXCHANGE-TYPE • INVALID-FLAGS • INVALID-MESSAGE-ID • INVALID-PROTOCOL-ID • INVALID-SPI • INVALID-TRANSFORM-ID • ATTRIBUTES-NOT-SUPPORTED • NO-PROPOSAL-CHOSEN • BAD-PROPOSAL-SYNTAX • PAYLOAD-MALFORMED • INVALID-KEY-INFORMATION • INVALID-ID-INFORMATION • INVALID-CERT-ENCODING • INVALID-CERTIFICATE • BAD-CERT-REQUEST-SYNTAX • INVALID-CERT-AUTHORITY • INVALID-HASH-INFORMATION • AUTHENTICATION-FAILED • INVALID-SIGNATURE • ADDRESS-NOTIFICATION • NOTIFY-SA-LIFETIME • CERTIFICATE-UNAVAILABLE • UNSUPPORTED-EXCHANGE-TYPE • UNEQUAL-PAYLOAD-LENGTHS • CONNECTED • RESPONDER-LIFETIME • REPLAY-STATUS • INITIAL-CONTACT • R-U-THERE

Log Field Name	Log Field Description	Data Type	Length	Value
phase2_name	The IPsec VPN Phase 2 name.	String	128	
rcvdbyte	The number of bytes received.	UINT64	20	
reason	The reason this log was generated.	String	256	
remip	The remote IP address.	IP Address	39	
remport	The remote port.	UINT16	5	
result	The result of the message.	String	31	• ERROR • OK • DONE • PENDING
role		String	9	
sentbyte	The number of bytes sent.	UINT64	20	
seq	The sequence number.	String	16	
spi	The IPsec VPN SPI.	String	16	
stage		UINT8	3	
status		String	23	

Log Field Name	Log Field Description	Data Type	Length	Value
subtype	The subtype of thelog message. Thepossible val-ues ofthis field dependon the log type.	String	20	
time	The time stamp of the event.	String	8	
tunnelid	The tunnel ID.	UINT32	10	
tunnelip	The tunnel IP address.	IP Address	39	
tunneltype	The tunnel type.	String	64	
type	The log type.	String	16	
ui	The user interface.	String	64	
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	
vpntunnel	The IPSec VPN tunnel name.	String	128	
xauthgroup	The xauth group name.	String	128	
xauthuser	The xauth user.	String	128	

VPN Log Messages

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

Message ID	Message	Description	Value
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	IPsec phase 1 error	Error
37125	MESGID_NEG_I_P2_ERROR	IPsec phase 2 error	Error
37126	MESGID_NEG_NO_STATE_ ERROR	IPsec 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	Installed IPsec SA	Notice

Message ID	Message	Description	Value
37134	MESGID_DELETE_P1_SA	Deleted IPsec phase 1 SA	Notice
37135	MESGID_DELETE_P2_SA	Deleted IPsec phase 2 SA	Notice
37136	MESGID_DPD_FAILURE	IPsec DPD failed	Error
37137	MESGID_CONN_FAILURE	IPsec connection failed	Error
37138	MESGID_CONN_UPDOWN	IPsec connection status changed	Notice
37139	MESGID_P2_UPDOWN	IPsec phase 2 status changed	Notice
37140	MESGID_AUTO_IPSEC	Auto IPsec status	Notice
37141	MESGID_CONN_STATS	IPsec tunnel statistics	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	IPsec phase 1 error	Error
37189	MESGID_NEG_I_P2_ERROR_ IKEV2	IPsec phase 2 error	Error
37190	MESGID_NEG_NO_STATE_ ERROR_IKEV2	IPsec no state error	Error
37191	MESGID_NEG_PROGRESS_P1_ NOTIF_IKEV2		Unknown

Message ID	Message	Description	Value
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	Installed IPsec SA	Notice
37198	MESGID_DELETE_P1_SA_IKEV2	Deleted IPsec phase 1 SA	Notice
37199	MESGID_DELETE_P2_SA_IKEV2	Deleted IPsec phase 2 SA	Notice
37200	MESGID_DPD_FAILURE_IKEV2	IPsec DPD failed	Error
37201	MESGID_CONN_FAILURE_IKEV2	IPsec connection failed	Error
37202	MESGID_CONN_UPDOWN_IKEV2	IPsec connection status changed	Notice
37203	MESGID_P2_UPDOWN_IKEV2	IPsec phase 2 status changed	Notice
37204	MESGID_CONN_STATS_IKEV2	IPsec tunnel statistics	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

Message ID	Message	Description	Value
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
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

Message ID	Message	Description	Value
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	PPTP tunnel up	Unknown
40002	LOG_ID_PPTP_TUNNEL_DOWN	PPTP tunnel down	Unknown
40003	LOG_ID_PPTP_TUNNEL_STAT	PPTP tunnel status	Unknown
40014	LOG_ID_PPTP_REACH_MAX_ CON	Client connection failed: PPTP connection limit reached	Warning
40016	LOG_ID_L2TPD_SVR_DISCON	L2TPD service is disconnected	Warning
40017	LOG_ID_L2TPD_CLIENT_CON_ FAIL	L2TP client connection failed	Warning
40019	LOG_ID_L2TPD_CLIENT_DISCON	L2TP client is disconnected	Information
40021	LOG_ID_PPTP_NOT_CONIG	PPTP is not configured in this VDOM	Debug
40022	LOG_ID_PPTP_NO_IP_AVAIL	No IP addresses left to assign in this VDOM	Warning
40024	LOG_ID_PPTP_OUT_MEM	Not enough memory	Warning
40034	LOG_ID_PPTP_START	PPTPD started successfully	Notice

Message ID	Message	Description	Value
40035	LOG_ID_PPTP_START_FAIL	PPTPD failed to start	Error
40036	LOG_ID_PPTP_EXIT	PPTPD exited successfully	Notice
40037	LOG_ID_PPTPD_SVR_DISCON	PPTPD service is disconnected	Information
40038	LOG_ID_PPTPD_CLIENT_CON	PPTPD client is connected	Information
40039	LOG_ID_PPTPD_CLIENT_DISCON	PPTPD client is disconnected	Information
40101	LOG_ID_L2TP_TUNNEL_UP	L2TP tunnel is up	Unknown
40102	LOG_ID_L2TP_TUNNEL_DOWN	L2TP tunnel is down	Unknown
40103	LOG_ID_L2TP_TUNNEL_STAT	L2TP tunnel status	Unknown
40114	LOG_ID_L2TPD_START	L2TPD started	Notice
40115	LOG_ID_L2TPD_EXIT	L2TPD exited	Notice
40118	LOG_ID_L2TPD_CLIENT_CON	L2TP client is connected	Information
41984	LOG_ID_EVENT_SSL_VPN_ CERT_LOAD	Certificate loaded successfully	Information
41985	LOG_ID_EVENT_SSL_VPN_ CERT_REMOVAL	Certificate is removed	Information
41987	LOG_ID_EVENT_SSL_VPN_ CERT_UPDATE	Certificate is updated	Information
41988	LOG_ID_EVENT_SSL_VPN_ SETTING_UPDATE	SSL setting changed	Information
41989	LOG_ID_EVENT_SSL_VPN_ CERT_ERR	Certificate error	Information
41990	LOG_ID_EVENT_SSL_VPN_ CERT_UPDATE_FAILED	Certificate update failed	Information

WAD

Event-Wad log messages record WAN optimization events, such as a user adding an WAN optimization rule as well as web proxy events.

In the log fields, these logs are defined as: type=event; subtype= wad.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this fire-wall policy.	String	32	
addr_type	The address type.	String	4	
alert	The alert name.	String	256	
app-type	The application type.	String	64	
authgrp	The authenticated group.	String	36	
date	The date the log event was generated on the device.	String	10	
desc	The description.	String	128	
devid	The serial number of the device.	String	16	
dstip	The destination IP address.	IP Address	39	
dstport	The destination port number of the TCP or UDP traffic. The destination port is zero for other types of traffic.	UINT16	5	
fqdn		String	256	

Log Field Name	Log Field Description	Data Type	Length	Value
fwserver_ name	The firewall server name.	String	32	
handshake	The handshake IP address.	String	32	
host	The host IP address.	String	256	
ip	The IP address.	IP Address	39	
level	The log priority level.	String	11	
local	The local IP address.	IP Address	39	
logdesc	The log description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log sub-type. The last one to five digits are the message id.	String	10	
msg	The activity or event that the FortiGate unit recorded.	String		
peer	The peer IP address.	String	36	
policyid	The ID number of the fire-wall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero. For more information, see the Knowledge Base art-icle, Firewall policy=0.	UINT32	10	
port	The port scanned.	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
reason	The reason the log event was generated.	String	256	
remote	The remote IP address.	IP Address	39	
serial	The serial number of the log message.	UINT32	10	
session_id	The session ID.	UINT32	10	
srcip	The source IP address.	IP Address	39	
srcport	The source port of the TCP or UDP traffic. The source protocol is zero for other types of traffic.	UINT16	5	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	
vd	The virtual domain name.	String	32	

WAD Log Messages

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

Message ID	Message	Description	Severity
40960	LOGID_EVENT_WAD_WEBPROXY_FWD_SRV_ERROR	Web proxy forward server error	Notice
48000	LOG_ID_WAD_SSL_RCV_HS	SSL handshake received	Debug
48001	LOG_ID_WAD_SSL_RCV_WRG_HS	SSL handshake has invalid length	Error
48002	LOG_ID_WAD_SSL_SENT_HS	SSL handshake sent	Debug
48003	LOG_ID_WAD_SSL_WRG_HS_LEN	SSL handshake message has an invalid length	Error
48004	LOG_ID_WAD_SSL_RCV_CCS	SSL ChangeCipherSpec received	Debug
48005	LOG_ID_WAD_SSL_RSA_DH_FAIL	RSA verification of Diffie-Hellman parameters failed	Error
48006	LOG_ID_WAD_SSL_SENT_CCS	SSL ChangeCipherSpec sent	Debug
48007	LOG_ID_WAD_SSL_BAD_HASH	Hash in SSL finished does not match calculated hash	Error
48009	LOG_ID_WAD_SSL_DECRY_FAIL	SSL decryption failed	Error
48011	LOG_ID_WAD_SSL_LESS_MINOR	SSL minor version is less than configured minimum value	Error
48013	LOG_ID_WAD_SSL_NOT_SUPPORT_CS	SSL Cipher Suites offered are not supported	Error

Message ID	Message	Description	Severity
48016	LOG_ID_WAD_SSL_HS_FIN	SSL handshake completed	Debug
48017	LOG_ID_WAD_SSL_HS_TOO_LONG	SSL handshake too long	Error
48019	LOG_ID_WAD_SSL_SENT_ALERT	SSL alert sent	Error
			Debug
48023	LOG_ID_WAD_SSL_RCV_ALERT	SSL alert received	Error
			Debug
48027	LOG_ID_WAD_SSL_INVALID_CONT_TYPE	Invalid SSL content type	Error
48029	LOG_ID_WAD_SSL_BAD_CCS_LEN	SSL ChangeCipherSpec has an invalid length	Error
48031	LOG_ID_WAD_SSL_BAD_DH	SSL Diffie-Hellman has an incorrect value	Error
48032	LOG_ID_WAD_SSL_PUB_KEY_TOO_BIG	Certificate's public key too long	Error
48100	LOG_ID_WAD_AUTH_FAIL_CERT	WANOpt peer certificate authentication failed	Error
48101	LOG_ID_WAD_AUTH_FAIL_PSK	WANOpt peer PSK authentication failed	Error
48102	LOG_ID_WAD_AUTH_FAIL_OTH	WANOpt peer authentication failed	Error
48300	LOG_ID_WRG_SVR_FGT_CONF	WANOpt server side FortiGate is not properly configured	Critical
48301	LOG_ID_UNEXP_APP_TYPE	Unexpected WANOpt application type	Critical

Wireless

Event-Wireless log messages record wireless events that occur with FortiGate units that have WiFi capabilities.

In the log fields, these logs are defined as: type=event; subtype= wireless.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this firewall policy.	String	32	
age	The time in seconds - time passed since last seen.	UINT32	10	
ap	The physical access point name.	String	36	
apscan	The name of the access point, which scanned and detected the rogue access point.	String	36	
apstatus	The status of the access point.	UINT8	3	
aptype	The access point type.	UINT8	3	

Log Field Name	Log Field Description	Data Type	Length	Value
bssid	The service set ID.	String	17	
cfgtxpower	The Config TX power.	UINT32	10	
channel	The channel number.	UINT8	3	
configcountry	The Config Country name.	String	4	
date	The date the log event was generated on the device.	String	10	
detectionmethod	The detection method.	String	21	
devid	The serial number of the device.	String	16	
ds	The direction with distribution system.	String	8	
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry.	UINT32	10	
eapolcnt	The EAPOL packet count.	UINT32	10	
eapoltype	The EAPOL packet type.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
encrypt	Whether the packet is encrypted or not.	UINT8	3	
frametype	The type of frame used in traffic.	String	32	
group	The user group name.	String	64	
invalidmac	The MAC address with invalid OUI.	String	17	
ip	The IP address.	IP Address	39	
level	The log priority level.	String	11	
live	The time in seconds.	UINT32	10	
logdesc	The log description.	String		
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
mac	The MAC address.	String	17	
manuf	The manufacturer name.	String	20	

Log Field Name	Log Field Description	Data Type	Length	Value
meshmode	The mesh mode.	String	19	
mgmtcnt	The number of unauthorized client flooding management frames.	UINT32	10	
msg	The activity or event that the FortiGate unit recorded.	String		
noise	The traffic noise.	INT8	4	
onwire	A flag to indicate if the AP is onwire or not.	String	3	
opercountry	The operating country.	String	4	
opertxpower	The operating TX power.	UINT32	10	
profile	The application profile .	String	64	
radioband	The radio band ID.	String	64	
radioid	The radio signal ID.	UINT8	3	
radioidclosest	The radio ID on the AP closest the rogue AP.	UINT8	3	

Log Field Name	Log Field Description	Data Type	Length	Value
radioiddetected	The radio ID on the AP which detected the rogue AP.	UINT8	3	
rate	The traffic rate.	UINT8	3	
reason	The reason for which log was generated.	String	256	
rssi	The received signal strength indicator.	UINT8	3	
security	The wireless security.	String	10	• open • wep64 • wep128 • wpa-psk • wpa-radius • wpa • wpa2 • wpa2-auto
securitymode	The security mode.	String	20	
seq		String	16	
signal	The traffic signal.	INT8	4	
sn		String	64	
snclosest	The SN of the accesspoint closest to the rogue access point.	String	36	

Log Field Name	Log Field Description	Data Type	Length	Value
sndetected	The SN of the access point which detected the rogue access point.	String	36	
snmeshparent	The SN of the mesh parent.	String	36	
srcip	The source IP address.	IP Address	39	
ssid	The base service set ID.	String	33	
stacount	The number of stations/clients.	UINT32	10	
stamac	The station/client MAC address.	String	17	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
tamac	The MAC address of Transmitter, if none, then receiver.	String	17	
threattype	The WIDS threat type.	String	64	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
user	The name of the user creating the traffic.	String	256	
vap	The virtual access point name.	String	36	
vd	The virtual domain name.	String	32	
weakwepiv	The Weak Wep Initiation Vector.	String	8	

Wireless Log Messages

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

Message ID	Message	Description	Severity
43520	LOG_ID_EVENT_ WIRELESS_SYS	Wireless system activity	Notice
43521	LOG_ID_EVENT_ WIRELESS_ROGUE	Wireless rogue AP activity	Unknown
43522	LOG_ID_EVENT_ WIRELESS_WTP	Physical AP activity	Notice
43524	LOG_ID_EVENT_ WIRELESS_STA	Wireless client activity	Notice
43525	LOG_ID_EVENT_ WIRELESS_ONWIRE	Wireless rogue AP activity	Unknown
43526	LOG_ID_EVENT_ WIRELESS_WTPR	Physical AP radio activity	Notice
			Unknown
43527	LOG_ID_EVENT_ WIRELESS_ROGUE_CFG	Wireless rogue AP status configured	Notice
43528	LOG_ID_EVENT_ WIRELESS_WTPR_ERROR	Physical AP radio activity	Unknown
43529	LOG_ID_EVENT_ WIRELESS_CLB	Wireless client load balancing	Notice
43530	LOG_ID_EVENT_ WIRELESS_WIDS_WL_ BRIDGE	Wireless bridge intrusion detected	Notice
43531	LOG_ID_EVENT_ WIRELESS_WIDS_BR_ DEAUTH	Wireless broadcasting deauthentication detected	Notice

Message ID	Message	Description	Severity
43532	LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP	Wireless Null SSID Probe Response detected	Notice
43533	LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI	Wireless Invalid MAC OUI detected	Notice
43534	LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR	Wireless Long Duration Attack detected	Notice
43535	LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV	Wireless Weak WEP IV detected	Notice
43542	LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD	Wireless EAPOL Packet Flooding detected	Notice
43544	LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD	Wireless Management Flooding detected	Notice
43546	LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH	Wireless Spoofed deauthentication detected	Notice
43548	LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP	Wireless ASLEAP Attack detected	Notice
43550	LOG_ID_EVENT_WIRELESS_STA_LOCATE	Wireless station presence detection	Notice

Other Logs

VOIP

VOIP log messages record VOIP activities that include the SIP and SCCP protocols.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for the event.	String	15	
call_id		String	64	
column		UINT32	10	
count		UINT32	10	
date	The date the log event was generated on the device.	String	10	
devid	The device serial number.	String	16	
dir		String	8	
dst_int	The destination interface.	String	16	
dst_port	The destination port.	UINT16	5	
dstip	The destination IP address.	IP Address	39	
duration		UINT32	10	
endpoint		String	128	
epoch		UINT32	10	
event_id	The event ID.	UINT32	10	
eventtype	The event type.	String	32	

Log Field Name	Log Field Description	Data Type	Length	Value
from		String	128	
group	The user group name.	String	64	
kind		String	10	
level	The log priority level.	String	11	
line		String	64	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
malform_data		UINT32	10	
malform_desc		String	47	
message_type	The type of message that the FortiGate unit recorded.	String	16	
phone		String	64	
policy_id	The policy ID.	UINT32	10	
profile	The profile name.	String	64	
profile_group	The profile group.	String	64	
profile_type	The profile type.	String	64	
proto	The protocol name.	UINT8	3	
reason	The reason why the log was recorded.	String	128	
request_name		String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
session_id	The session ID.	UINT32	10	
src_int	The source interface.	String	16	
src_port	The source port.	UINT16	5	
srcip	The source IP address.	IP Address	39	
status	The status of the action the FortiGate unit took when the event occurred.	String	23	
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
to		String	512	
type	The log type.	String	16	
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	
voip_proto	The VOIP protocol.	String	4	

VOIP Log Messages

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

Message ID	Message	Severity
44032	LOGID_EVENT_VOIP_SIP	Information
44033	LOGID_EVENT_VOIP_SIP_BLOCK	Notice
44034	LOGID_EVENT_VOIP_SIP_FUZZING	Information
44035	LOGID_EVENT_VOIP_SCCP_ REGISTER	Information
44037	LOGID_EVENT_VOIP_SCCP_CALL_ BLOCK	Information
44038	LOGID_EVENT_VOIP_SCCP_CALL_ INFO	Information

NetScan

Netscan logs record network scanning activities preformed by the FortiGate unit.

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this event.	String	17	• host-detection • os-scan • port-detection • scan • service-detection • vuln-count • vuln-detection
agent		String	64	
assetid	The asset ID.	UINT32	10	
assetname	Th asset name.	String	64	
date	The date the log event was generated on the device.	String	10	
devid	The device serial ID.	String	16	
direction	The direction of the packets.	UINT32	10	
dstintf	The destination interface.	String	32	
dstip	The destination IP address.	IP Address	39	
dstname	The destination name.	String	64	
dstport	The destination port.	UINT16	5	
end		UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
engine		String	32	
eventtype	The event type.	String	32	
group	Theuser group name.	String	64	
level	The log priority level.	String	11	
logid	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last one to five digits are the message id.	String	10	
method		String	4	• ARP • ICMP • TCP • UDP
msg	The activity or event that the FortiGate unit recorded.	String		
os	The software version.	String		
osfamily		String	64	
osgen		String	64	
osvendor	The operating system vendor.	String	64	
plugin		String	32	
policyid	The policy ID.	UINT32	10	
profile	The profile name.	String	64	

Log Field Name	Log Field Description	Data Type	Length	Value
profilegroup	The profile group.	String	4	
proto	The protocol name.	String	3	• tcp • udp
serial	The serial number of the log message.	UINT32	10	
service	The service name.	String	64	
severity		String	8	• critical • high • info • low • medium
srcintf	The source interface.	String	32	
srcip	The source IP address.	IP Address	39	
srcname	The source name.	String	64	
srcport	The source port.	UINT16	5	
start		UINT32	10	
status	The status of the action the FortiGate unit took when the event occurred.	String	8	• complete • pause • resume • start • stop
subtype	The subtype of the log message. The possible values of this field depend on the log type.	String	20	
time	The time stamp of the event.	String	8	
type	The log type.	String	16	

Log Field Name	Log Field Description	Data Type	Length	Value
user	The name of the user creating the traffic.	String	256	
vd	The virtual domain name.	String	32	
vuln	The vulnerability name.	String	128	
vulncat	The vulnerability category.	String	32	
vulncnt	The vulnerabiility count.	UINT32	10	
vulnid	The vulnerability ID.	UINT32	10	
vulnref		String		
vulnscore	The vulnerability score.	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
4100	LOG_ID_NETSCAN_SERVICE_DETECT	Notice
4101	LOG_ID_NETSCAN_VULN_MESSAGE	Notice
4102	LOG_ID_NETSCAN_DISCOVERY_MESSAGE	Notice
4104	LOG_ID_NETSCAN_HOST_DETECT	Notice
4105	LOG_ID_NETSCAN_PORT_DETECT	Notice

Appendix A: Log field diff - 5.2.1 and 5.2.2

Refer to the *FortiOS Log Reference Guide Version 5.2.1* for a complete list of log field details related to version 5.2.1. This section covers changes applicable to the 5.2.2 version only. It is recommended that you keep both the 5.2.1 and 5.2.2 *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 5.2.2 but exists in version 5.2.1. Similarly, the term **Added** indicates that a log filed was added in version 5.2.2 but does not exist in version 5.2.1.

The following table lists the log fields that were added newly or removed from the Traffic log type in FortiOS version 5.2.2.

Traffic

Log Field Name	Changes in Version 5.2.2
crlevel	Added
hostname	Removed

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 5.2.2.

Antivirus

Log Field Name	Changes in Version 5.2.2
crlevel	Added
crscore	Added
profiletype	Removed
rcvdbyte	Removed
sentbyte	Removed

Application

Log Field Name	Changes in Version 5.2.2
crlevel	Added
crscore	Added
dstname	Added
profile	Added
profiletype	Added
srcname	Added

Anomaly

Log Field Name	Changes in Version 5.2.2
action	Added
agent	Added
attack	Added
attackcontext	Added
attackcontextid	Added
attackid	Added
count	Added
craction	Added
crlevel	Added
crscore	Added
date	Added
devid	Added

Log Field Name	Changes in Version 5.2.2
direction	Added
dstintf	Added
dstip	Added
dstport	Added
eventtype	Added
group	Added
icmpcode	Added
icmpid	Added
icmptype	Added
incidentserialno	Added
level	Added
logid	Added
msg	Added
profile	Added
profiletype	Added
proto	Added
ref	Added
service	Added
sessionid	Added
severity	Added
srcintf	Added

Log Field Name	Changes in Version 5.2.2
srcip	Added
srcport	Added
subtype	Added
time	Added
type	Added
user	Added
vd	Added

DLP

Log Field Name	Changes in Version 5.2.2
mmsdir	Added
profiletype	Removed

Email

Log Field Name	Changes in Version 5.2.2
profiletype	Removed

IPS

Log Field Name	Changes in Version 5.2.2
craction	Added
crlevel	Added
crscore	Added
dstinf	Added

Log Field Name	Changes in Version 5.2.2
rcvdbyte	Removed
sentbyte	Removed
srcintf	Added

WebFilter

Log Field Name	Changes in Version 5.2.2
crlevel	Added
crscore	Added
profiletype	Removed

Event

The following tables provide a list of log fields that were added newly or removed between from the event log subtypes in FortiOS version 5.2.2.

Endpoint

Log Field Name	Changes in Version 5.2.2
dst	Removed
dstip	Added
src	Removed
srcip	Added

GTP

Log Field Name	Changes in Version 5.2.2
dstport	Added

Log Field Name	Changes in Version 5.2.2
logdesc	Added
msg	Added
profile	Added

High Availability

Log Field Name	Changes in Version 5.2.2
date	Added
devid	Added
ip	Added
level	Added
logdesc	Added
logidd	Added
msg	Added
subtype	Added
time	Added
type	Added
vd	Added

Router

Log Field Name	Changes in Version 5.2.2
action	Added
dhcp_msg	Added
dns_ip	Added

Log Field Name	Changes in Version 5.2.2
dns_name	Added
dst_int	Added
lease	Added
logdesc	Added
mac	Added
service	Added
src_int	Added

System

Log Field Name	Changes in Version 5.2.2
community	Added
dir	Added
disklograte	Added
dst	Removed
dstport	Added
expected	Removed
fazlograte	Added
group	Added
id	Removed
ip	Added
logdesc	Added
mac	Added

Log Field Name	Changes in Version 5.2.2
max_minor	Added
max-minor	Removed
mode	Added
policy	Removed
probeid	Removed
recv-minor	Removed
recv_minor	Added
profile	Added
sn	Added
src	Removed
src-vis	Removed
srcport	Added
state	Added
vcm	Removed
version	Added

User

Log Field Name	Changes in Version 5.2.2
category	Added
logdesc	Added
poolname	Added
portbegin	Added

Log Field Name	Changes in Version 5.2.2
portend	Added
profile	Removed
ui	Added

VPN

Log Field Name	Changes in Version 5.2.2
action	Added
error_num	Added
error_reason	Removed
name	Added
role	Added
status	Added
ui	Added
user	Added
version	Removed

WAD

Log Field Name	Changes in Version 5.2.2
dst	Removed
dstip	Added
logdesc	Added
reason	Added
src	Removed

Log Field Name	Changes in Version 5.2.2
srcip	Added

Wireless

Log Field Name	Changes in Version 5.2.2
group	Added
logdesc	Added
mac	Added
seq	Added
sn	Added
srcip	Added
status	Removed
user	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 5.2.2.

NetScan

Log Field Name	Changes in Version 5.2.2
custom	Removed

VOIP

Log Field Name	Changes in Version 5.2.2
dst	Removed

Log Field Name	Changes in Version 5.2.2
dstip	Added
src	Removed
srcip	Added