FORTINET®

High Performance Network Security

FortiOS Log Reference Guide

VERSION 5.2.1

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

November 04, 2014

FortiOS 5.2.1 Log Reference Guide

01-521-257022-20141104

TABLE OF CONTENTS

Change Log

Date	Change Description
2014-11-04	Initial release.
2015-01-30	• Updated Log ID numbering section. • Added log definitions for log type and sub type IDs. • Added notes about UTM log type information in Security log section.

Introduction

This document provides information about all the log messages applicable to the FortiGate devices running FortiOS version 5.2.1. 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 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

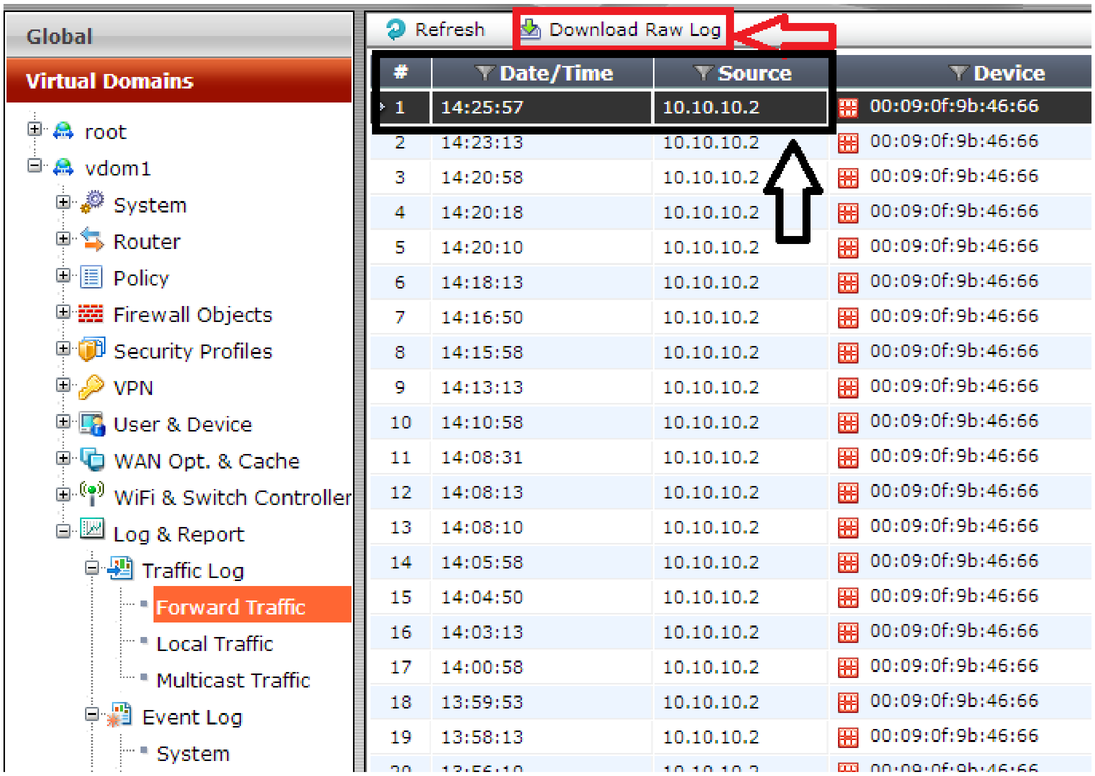
Log Field	Log Field Description	Data Type	Length	Value(s)
appact	The security action from app control	ENUM	16	• block • encrypt-kickout • monitor • pass • reject • reset

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.



#	Date/Time	Source	Device
1	14:25:57	10.10.10.2	00:09:0f:9b:46:66
2	14:23:13	10.10.10.2	00:09:0f:9b:46:66
3	14:20:58	10.10.10.2	00:09:0f:9b:46:66
4	14:20:18	10.10.10.2	00:09:0f:9b:46:66
5	14:20:10	10.10.10.2	00:09:0f:9b:46:66
6	14:18:13	10.10.10.2	00:09:0f:9b:46:66
7	14:16:50	10.10.10.2	00:09:0f:9b:46:66
8	14:15:58	10.10.10.2	00:09:0f:9b:46:66
9	14:13:13	10.10.10.2	00:09:0f:9b:46:66
10	14:10:58	10.10.10.2	00:09:0f:9b:46:66
11	14:08:31	10.10.10.2	00:09:0f:9b:46:66
12	14:08:13	10.10.10.2	00:09:0f:9b:46:66
13	14:08:10	10.10.10.2	00:09:0f:9b:46:66
14	14:05:58	10.10.10.2	00:09:0f:9b:46:66
15	14:04:50	10.10.10.2	00:09:0f:9b:46:66
16	14:03:13	10.10.10.2	00:09:0f:9b:46:66
17	14:00:58	10.10.10.2	00:09:0f:9b:46:66
18	13:59:53	10.10.10.2	00:09:0f:9b:46:66
19	13:58:13	10.10.10.2	00:09:0f:9b:46:66
20	13:56:10	10.10.10.2	00:09:0f:9b:46:66

- 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 Interface(srcintf)	The interface of the traffic's origin.	√	√	√	`srcintf="mgmt1"`
Destination IP (dstip)	The destination IP address for the web.	√	√	√	`dstip=10.6.30.1`
Destination Port(dstport)	The port number of the traffic's destination.	√	√	√	`dstport=80`
Destination Interface (dstintf)	The interface of the traffic's destination.	√	√	√	`dstintf="vdom1"`

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 subtypes.

- Forward
- Multicast
- Local
- Sniffer

In the log fields, the logs are defined as: type=traffic; subtypes = local , multicast, local, and 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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	String	16	close deny dns ip-conn start timeout
app	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	Application category	String	64	
appid	Application ID	UINT32	10	
applist	Application Control profile (name)	String	64	
apprisk	Application Risk Level	String	16	• critical • elevated • high • low • medium
collectedemail	Email address from Email Collection Captive Portal	String	66	
countapp	Number of App Ctrl logs associated with the session	UINT32	10	
countav	Number of AV logs associated with the session	UINT32	10	
countdlp	Number of the DLP logs associated with the session	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
countemail	Number of the email logs associated with the session	UINT32	10	
countips	Number of the IPS logs associated with the session	UINT32	10	
countweb	Number of the Web Filter logs associated with the session	UINT32	10	
craction	Action performed by Client Reputation	UINT32	10	
crlevel	Client Reputation level	String	10	
crscore	Client Reupation score	UINT32	10	
custom	Custom field	Custom		
date	Date	String	10	
devid	Device serial number	String	16	
devtype	Device type	String	32	
dstcountry	Country name for the destination IP	String	64	
dstintf	Destination Interface	String	32	
dstip	Destination IP Address	IP Address	39	
dstname	The destination name.	String	66	
dstport	Destination Port	UINT16	5	
dstssid	Destination SSID	String	33	

Log Field Name	Log Field Description	Data Type	Length	Value
dstuuid	UUID of the Destination IP address	String	37	
duration	Duration of the session	UINT32	10	
group	User group name	String	64	
lanin	LAN incoming traffic in bytes	UINT64	20	
lanout	LAN outgoing traffic in bytes	UINT64	20	
level	Log Level	String	11	
logid	Log ID	String	10	
mastersrcmac	The master MAC address for a host that has multiple network interfaces	String	17	
msg	Log message	String	64	
osname	Name of the device's OS	String	66	
osversion	OS version of the device	String	66	
policyid	Firewall Policy ID	UINT32	10	
poluuid	UUID of the Firewall Policy	String	37	
proto	protocol number	UINT8	3	
rcvdbyte	Received Bytes	UINT64	20	
rcvdpkt	Received Packets	UINT32	10	

Log Field Name	Log Field Description	Data Type	Length	Value
sentbyte	Sent Bytes	UINT64	20	
sentpkt	Sent Packets	UINT32	10	
service	Name of service	String	36	
sessionid	Session ID	UINT32	10	
shaperdroprcvdbyte	Received bytes dropped by shaper	UINT32	10	
shaperdropsentbyte	Sent bytes dropped by shaper	UINT32	10	
shaperperipdropbyte	Dropped bytes per IP by shaper	UINT32	10	
shaperperipname	Traffic shaper name (per IP)	String	36	
shaperrcvdname	Traffic shaper name for received traffic	String	36	
shapersentname	Traffic shaper name for sent traffic	String	36	
srccountry	Country name for Source IP	String	64	
srcintf	Source interface name	String	32	
srcip	Source IP address	IP Address	39	
srcmac	MAC address associated with the Source IP	String	17	
srcname	Source name	String	66	
srcport	Source port number	UINT16	5	

Log Field Name	Log Field Description	Data Type	Length	Value
srcssid	Source SSID	String	33	
srcuuid	UUID of the Source IP Address	String	37	
subtype	Subtype of the traffic	String	20	• local • multicast • forward • sniffer
time	Time	String	8	
trandisp	NAT translation type	String	16	• dnat • noop • snat • snat+dnat
tranip	NAT destination IP	IP Address	39	
tranport	NAT Destination Port	UINT16	5	
transip	NAT Source IP	IP Address	39	
transport	NAT Source Port	UINT16	5	
type	Log type	String	16	• traffic
unauthuser	Unauthenticated user name	String	66	
unauthusersource	The method used to detect unauthenticated user name	String	66	
user	User name	String	256	

Log Field Name	Log Field Description	Data Type	Length	Value
utmaction	Security action performed by UTM	String	32	- allow - block - n/a - reset - traffic-shape
vd	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	WAN incoming traffic in bytes	UINT32	10	
wanoptapptype	WAN Optimization Application type	String	9	- cifs - ftp - ftp-proxy - http - mapi - tcp - web-cache - web-proxy
wanout	WAN outgoing traffic in bytes	UINT32	10	

Traffic Log Messages

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

Log Message Details

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	Security action performed by App Control	enum	16	• block • encrypt-kickout • kickout • monitor • pass • reject • reset
level	Log level	String	11	
logid	Log ID	String	10	
msg	Log message	String	512	
sessionid	Session ID	uint32		
subtype	Log subtype	String	20	• app-ctrl
type	Log type	String	16	• utm
app	Application name	String	96	
appcat	Application category name	String	64	
appid	Application ID	uint32	0	
applist	Application Control profile name	String	64	
filename	File name	String	256	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
direction	Direction of the packets	enum	8	• incoming • N/A • outgoing
eventtype	App Control Event Type	String	32	
filesize	File size in bytes	uint64		
url	The URL address	String	512	
date	Date	String	10	
time	Time	String	8	
vd	Virtual domain name	String	32	
user	User name	String	256	
group	User group name	String	64	
devid	Device Serial Number	String	16	
hostname	The host name of a URL	String	256	
sentbyte	Sent Bytes	UINT64		
rcvdbyte	Received Bytes	UINT64		
dstip	Destination IP	IP Address		
srcip	Source IP	IP Address		
dstport	Destination Port	uint16		
srcport	Source Port	uint16		
proto	Protocol number	uint8		
service	Service name	String	36	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
clouduser	User login ID detected by the Deep Application Control feature	String	256	
cloudaction	Action performed by cloud application	String	32	
apprisk	Application risk level	enum		• critical • elevated • high • low • medium

Application Control Log Messages

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

Log Message Details

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	The security action performed by AV	enum	11	• analytics • blocked • monitored • pass through
agent	User agent - eg. agent="Mozilla/5.0"	String	64	
analyticscksum	The checksum of the file submitted for analytics	String	64	
analyticssubmit	The flag for analytics submission	enum	10	• false • true
botnet	IP reputation detected botnets			
checksum	The file checksum	String	16	
command	Protocol specific command, such as “POST” and “GET” for HTTP, “MODE” and “REST” for FTP	String	16	
date	Date	String	10	
devid	Device serial number	String		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
direction	Message/packets direction	enum	8	- incoming - N/A - outgoing
dstip	Destination IP Address	IP Address		
dstport	Destination Port	uint16		
dtype	Data type for virus category	String	32	
eventtype	Event type of AV	String	32	
filefilter	The filter used to identify the affected file	enum	12	- none - file pattern - file type
filename	File name	String	256	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
filetype	File type	enum	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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
from	Email address from the Email Headers (IMAP/POP3/SMTP)	String	128	
group	Group name (authentication)	String		
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	Explains the activity or event that the FortiGate unit recorded	String	512	
profile	The name of the profile that was used to detect and take action	String	64	
profiletype	The type of profile responsible for the UTM action	String	64	
proto	Protocol number	uint8		
quarskip	Quarantine skip explanation	enum	46	• File-was-not-quarantined. • No-quarantine-for-HTTP-GET-file-pattern-block. • No-quarantine-for-oversized-files • No-skip

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
rcvdbyte	Received Bytes	uint64		
recipient	Email addresses from the SMTP envelope	String	512	
ref	The URL of the FortiGuard IPS database entry for the attack	String	512	
sender	Email address from the SMTP envelope	String	128	
sentbyte	Sent Bytes	uint64		
service	Proxy service which scanned this traffic	enum	36	• ftp • ftps • http • https • im • imap • imaps • mapi • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smb • smtp • smtps • ssl
sessionid	Session ID	uint32		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
srcip	Source IP Address	IP Address		
srcport	Source Port	uint16		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• virus
switchproto	Protocol change information	String	128	
time	Time	String	8	
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	String	512	
type	The log type	String	16	• utm
url	The url address	String	512	
user	Username (authentication)	String	256	
vd	VDOM name	String	32	
virus	Virus Name	String	128	
virusid	Virus ID (unique virus identifier)	uint32		

AntiVirus Log Messages

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

Log Message Details

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

Message ID	Message	Severity
8458	MESGID_MMS_CHECKSUM_NOTIF	Notice
8704	MESGID_OVERSIZE_WARNING	Warning
8705	MESGID_OVERSIZE_NOTIF	Notice
8706	MESGID_OVERSIZE_MIME_WARNING	Warning
8707	MESGID_OVERSIZE_MIME_NOTIF	Notice
8720	MESGID_SWITCH_PROTO_WARNING	Warning
8721	MESGID_SWITCH_PROTO_NOTIF	Notice
8960	MESGID_SCAN_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
8972	MESGID_SCAN_ARCHIVE_UNHANDLED_WARNING	Warning
8973	MESGID_SCAN_ARCHIVE_UNHANDLED_NOTIF	Notice
9233	MESGID_ANALYTICS_SUBMITTED	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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	Security action performed by DLP	enum	16	• ban • ban-sender • block • exempt • log-only • quarantine-interface • quarantine-ip
level	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	Explains the activity or event that the FortiGate unit recorded	String	512	
sessionid	Session ID	uint32		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• dlp
type	Log type	String	16	• utm
filename	File name	String	256	
docsource	DLP fingerprint document source	String	515	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
epoch	Epoch used for locating file	uint32		
eventid	The serial number of the dlparchive file in the same epoch	uint32		
eventtype	DLP event type	String	32	
filetype	File type	String	16	
filtercat	DLP filter category	enum	8	
filteridx	DLP filter ID	uint32		
filtertype	DLP filter type	enum	23	• file • message • none • credit-card • encrypted • file-size • file-type • fingerprint • none • regexp • ssn • watermark
profile	DLP profile name	String	64	
sensitivity	Sensitivity for document fingerprint	String	36	
severity	Severity level of a DLP rule	enum	8	
subject	The subject title of the email message	String	128	
url	The URL address	String	512	
filtername	DLP rule name	String	128	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
direction	Direction of packets	enum	8	• incoming • N/A • outgoing
dlpextra	DLP extra information	String	256	
profiletype	Profile type	String	64	
date	The date the log event was generated on the device	String	10	
time	Time stamp of the event	String	8	
sender	Email address from the SMTP envelope	String	128	
recipient	Email addresses from the SMTP envelope	String	512	
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	String	512	
from	Email address from the Email Headers (IMAP/POP3/SMTP)	String	128	
user	User name	String	256	
vd	Virtual domain name	String	32	
group	User group name	String	64	
devid	Device Serial Number	String		
hostname	The host name of a URL	String	256	
sentbyte	Sent Bytes	UINT64		
rcvdbyte	Received bytes	UINT64		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
dstip	Destination IP	IP Address		
srcip	Source IP	IP Address		
srcport	Source Port	UINT16		
dstport	Destination Port	UINT16		
proto	Protocol number	UINT8		
service	Service name	enum	36	• ftp • ftps • http • https • im • imap • imaps • mapi • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smtp • smtps • ssl
agent	User agent - eg. agent="Mozilla/5.0"	String	64	
filesize	File size in bytes	INT64		

DLP Log Messages

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

Log Message Details

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	Security action of the email filter	enum	8	• blocked • detected • exempted
agent	User agent - eg. agent="Mozilla/5.0"	String	64	
attachment	The flag for email attachement	enum	3	• no • yes
banword	Banned word	String	128	
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	String	512	
date	Date	String	10	
devid	Device Serial Number	String		
direction	Direction of packets	enum	8	• incoming • N/A • outgoing
dstip	Destination IP	IP Address		
dstport	Destination Port	UINT16		
eventtype	Email Filter event type	String	32	
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	String	512	
group	User group name	String		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
level	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	Explains the activity or event that the FortiGate unit recorded	String	512	
profile	Email Filter profile name	String	64	
profiletype	Profile type	String	64	
proto	Protocol number	uint8		
rcvdbyte	Received Bytes	UINT64		
recipient	Email addresses from the SMTP envelope	String	512	
sender	Email addresses from the SMTP envelope	String	128	
sentbyte	Sent Bytes	UINT64		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
service	Service name	enum	36	- ftp - ftps - http - https - im - imap - imaps - mapi - mm1 - mm3 - mm4 - mm7 - nntp - pop3 - pop3s - smtp - smtps - ssl
sessionid	Session ID	UINT32		
size	Email size in Bytes?	String	16	
srcip	Source IP	IP Address		
srcport	Source Port	UINT16		
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	- email filter
time	Time	String	8	
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	String	512	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
type	Log type	String	16	- utm
user	User name	String	256	
vd	Virtual domain name	String	32	

Email Filter Log Messages

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

Log Message Details

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
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

Message ID	Message	Severity
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

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	Security action performed by WF	ENUM	11	• allowed • blocked • dlp • exempted • filtered • passthrough
agent	User agent - eg. agent="Mozilla/5.0"	String	64	
banword	Banned word	String	128	
cat	Web category ID	UINT8		
catdesc	Web category description	String	64	
contenttype	Content Type from HTTP header	String	64	
date	Date	String	10	
devid	Device Serial Number	String		
direction	Direction of the web traffic	ENUM	8	• incoming • N/A • outgoing
dstip	Destination IP	IP Address		
dstport	Destination Port	UINT16		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
error	URL rating error message	String	256	
eventtype	Web Filter event type	String	32	
filtertype	The script filter type	ENUM	10	• javascript • jscript • n/a • unknown • vbscript
from	MMS-only - From/To headers from the email	String	128	
group	User group name	String	64	
hostname	The host name of a URL	String	256	
initiator	The initiator user for override	String	64	
keyword	Keyword used for search	String	512	
level	Log 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	
method	Rating override method by URL domain name or IP address.	ENUM	6	• domain • ip
mode	Rating override mode	String	32	
msg	Explains the activity or event that the FortiGate unit recorded	String	512	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
ovrdid	URL rating override ID	UINT32		
ovrdtbl	Rating override table	String	128	
profile	Web Filter profile name	String	64	
profiletype	Profile type	String	64	
proto	Protocol number	UINT8		
quotaexceeded	Quota has been exceeded	ENUM	3	• no • yes
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	UINT64		
quotatype	Quota type	ENUM	16	• time • traffic
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based).	UINT64		
rcvdbyte	Received Bytes	UINT64		
reqtype	Request type	ENUM	8	• direct • referral
ruledata	Rule data	String	512	
ruletype	Rule type	ENUM	9	• directory • domain • rating
sentbyte	Sent Bytes	UINT64		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
service	Service name	ENUM	36	• dns • ftp • ftps • http • https • im • imap • imaps • mm1 • mm3 • mm4 • mm7 • nntp • pop3 • pop3s • smtp • smtps • ssl
sessionid	Session ID	UINT32		
srcip	Source IP	IP Address		
srcport	Source Port	UINT16		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• webfilter
time	Time	String	8	
to	MMS-only - From/To headers from the email	String	512	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
type	Log type	String	16	• utm
url	The URL address	String	512	
urlfilteridx	URL filter ID	UINT32		
urlfilterlist	URL filter list	String	64	
urltype	URL filter type	ENUM	8	• ftp • http • https • mail • phishing • telnet
user	User name	String		
vd	Virtual domain name	String		

Web Filter Log Messages

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

Log Message Details

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

Log Message Details

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

Log Message Details

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

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	Security action performed by IPS	ENUM	16	• clear_session • detected • drop_session • dropped • pass_session • reset • reset_client • reset_server
agent	User agent - eg. agent="Mozilla/5.0"	String	66	
attack	Attack Name	String		
attackcontext	the trigger patterns and the packetdata with base64 encoding	String		
attackcontextid	attack context id / total	String		
attackid	Attack ID	UINT32		
count	Repeat count for an attack event	UINT32		
date	The date the log event was generated on the device	String	10	
devid	Device Serial Number	String		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
direction	Direction of packets	ENUM	8	• incoming • N/A • outgoing
dstip	Destination IP	IP Address		
dstport	Destination Port	UINT16		
eventtype	IPS Event Type	String	32	
group	User group name	String		
icmpcode	Destination Port of the ICMP message	String	6	
icmpid	Source port of the ICMP message	String	8	
icmptype	The type of ICMP message	String	6	
incidentserialno	Incident serial number	UINT32		
level	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	Log message for the attack	String	518	
profile	Profile name for IPS	String	64	
profiletype	Profile Type	String	64	
proto	Protocol number	UINT8		
rcvdbyte	Received Bytes	UINT64		
ref	URL of the FortiGuard IPS database entry for the attack.	String	512	
sentbyte	Sent Bytes	UINT64		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
service	Service name	String	36	
sessionid	Session ID	UINT32		
severity	Severity of the attack	ENUM	8	• critical • high • info • low • medium
srcip	Source IP	IP Address		
srcport	Source Port	UINT16		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• ips
time	Time stamp of the event	String	8	
type	Log type	String	16	• utm
user	User name	String	256	
vd	Virtual domain name	String	32	

IPS Log Messages

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

Log Message Details

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

Event Log

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

Event logs 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

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

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this firewall policy	string		
connection_type	Forticlient connection type	string	6	
count	The number of dropped SIP packets	uint16		
date	The date the log event was generated on the device	string		
devid	The serial number of the device	string		
forticlient_id	forticlient uuid	string	33	
hostname	The host name or IP	string		
interface	Interface	string		
ip	IP address	ip		
level	The log priority level	string		
license_limit	number of limited licenses	string	32	
license_used	number of licenses used	uint16	5	
logdesc	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		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
msg	Explains the activity or event that the FortiGate unit recorded	string		
name	Name	string		
reason	The reason this log was generated	string		
repeat		uint16	5	

Log Details

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		For event logs, the possible values of this field depend on the sub type: • ipsec • success • failure • negotiate_error • esp_error • dpd_failure • sub type voip • start • end • timeout • blocked • succeeded • failed • authentication-required • subcategory 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		• endpoint
time	Time stamp of the event	string		
type	The log type	string		• event

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
authproto	authentication protocol	string	64	
used_for_ type	used to describe the log type	uint16	5	
user	The name of the user creating the traffic	string		
vd	Virtual domain name	string		

Endpoint Log Messages

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

Log Message Details

Message ID	Message	Severity
45056	LOG_ID_FCC_EXCEED	Notice
45057	LOG_ID_FCC_ADD	Information
45058	LOG_ID_FCC_CLOSE	Information
45059	LOG_ID_FCC_UPGRADE_SUCC	Notice
45060	LOG_ID_FCC_UPGRADE_FAIL	Error
45100	LOG_ID_EC_REG_FAIL	Warning
45101	LOG_ID_EC_REG_SUCCEED	Notice
45102	LOG_ID_EC_REG_RENEWED	Notice
45103	LOG_ID_EC_REG_BLOCK	Notice
45104	LOG_ID_EC_REG_UNBLOCK	Notice
45105	LOG_ID_EC_REG_DEREG	Notice
45106	LOG_ID_EC_REG_LIC_UPGRADED	Notice
45107	LOG_ID_EC_CONF_DISTRIBUTED	Notice
45108	LOG_ID_EC_FTCL_UNREG	Notice
45109	LOG_ID_EC_FTCL_LOGOFF	Notice
45110	LOG_ID_EC_FTCL_ENABLE_NOTSYNC	Notice

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
apn	Access Point Name	String	0	
c-bytes	Number of bytes for signaling	UINT64	20	
c-ggsn	Control plane GGSN IP address for GTP signaling	IP Address	39	
c-ggsn-teid	Control plane for GGSN TEID (Tunnel endpoint identifier) for signaling	UINT32	10	
c-gsn	Control plane GSN IP address for GTP signaling	IP Address	39	
cpaddr	Control Plane Address (either downlink or uplink)	IP Address	39	
cpdladdr	Control plane downlink IP address	IP Address	39	
cpdlisraddr	Control plane ISR downlink IP address	IP Address	39	
cpdlisrteid	Control plane ISR downlink teid	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
cpdlteid	Control plane downlink teid	UINT32	10	
c-pkts	Number of packets for signaling	UINT64	20	
cpteid	Control Plane teid (either downlink or uplink)	UINT32	10	
cpuladdr	Control plane uplink IP address	IP Address	39	
cpulteid	Control plane uplink teid	UINT32	10	
c-sgsn	Control plane SGSN IP address for GTP signalling	IP Address	39	
c-sgsn-teid	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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
deny_cause		ENUM	0	• 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 serial number of the device	String	16	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
dtlexp		ENUM	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-cteid-exists • no-tunnel-exists • none • payload-teid-is-zero • response-hteid-doesnt-match-request
duration	Tunnel duration	UINT32	0	
end-usr-address	End user address	IP Address	39	
from	Source IP address	String	0	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
headerteid	Header (Tunnel end-point identifier)	UINT32	10	
ietype	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	International mobile subscriber ID	String	0	
level	The log priority level	String	11	
linked-nsapi	Linked Network Service Access Point Identifier	UINT8	3	

Log Details

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. For more detail about what the combination of type, subtype and message ID means	String	10	
msg-type	Message type	UINT8	0	
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	String	0	
nsapi	Network Service Access Point Identifier, an identifier used in cellular data networks	UINT8	3	
rai	Routing Area Identification	String	32	
rat-type	Type of router audit tool	ENUM	7	
selection	Access point selection	ENUM	14	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
seqnum	GTP packet sequence number	UINT32	10	
snetwork	Source Network, it's a IE type in GTPv2 packet	String	64	
status	The status of the action the FortiGate unit took when the event occurred	ENUM	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	gtp
time	Timestamp for the event	String	8	
to	Destination IP address	String	0	
tunnel-idx	VPN tunnel index	UINT32	0	
type	The log type	String	16	event
u-bytes	Number of bytes used for traffic	UINT64	20	
u-ggsn	User plane GGSN IP address for GTP user traffic	IP Address	39	

Log Details

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

GTP Log Messages

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

Log Message Details

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

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
activity	HA activity message	String	128	
devintfname	HA device Interface Name	String	32	
from_vcluster	source virtual cluster number	UINT32	10	
ha_group	HA Group Number - can be 1 - 256	UINT8	3	
ha_role	The HA role in the cluster	ENUM	6	• Master • slave
ha-prio	HA Priority	UINT8	3	
hbdn_reason	heartbeat down reason	ENUM	18	• Linkfail • neighbor-info-lost
sn		String	64	
sync_status	The sync status with the master	ENUM	11	• in-sync • out-of-sync
sync_type	The sync type with the master	ENUM	14	• Configurations • external-files
to_vcluster	destination virtual cluster number	UINT32	10	
vcluster	virtual cluster id	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
vcluster_member	virtual cluster member id	UINT32	10	
vcluster_state	virtual cluster state	ENUM	7	• hello • init • standby • work
vdname	vdom name	String	16	

High Availability Log Messages

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

Log Message Details

Log ID	Log Message	Severity
35001	LOG_ID_HA_SYNC_VIRDB	Notice
35002	LOG_ID_HA_SYNC_ETDB	Notice
35003	LOG_ID_HA_SYNC_EXDB	Notice
35005	LOG_ID_HA_SYNC_IPS	Notice
35007	LOG_ID_HA_SYNC_AV	Notice
35008	LOG_ID_HA_SYNC_VCM	Notice
35009	LOG_ID_HA_SYNC_CID	Notice
35010	LOG_ID_HA_SYNC_FAIL	Error
37888	MESGID_HA_GROUP_DELETE	Notice
37889	MESGID_VC_DELETE	Notice
37890	MESGID_VC_MOVE_VDOM	Notice
37891	MESGID_VC_ADD_VDOM	Notice
37892	MESGID_VC_MOVE_MEMB_STATE	Notice
37893	MESGID_VC_DETECT_MEMB_DEAD	Critical
37894	MESGID_VC_DETECT_MEMB_JOIN	Critical
37895	MESGID_VC_ADD_HADEV	Notice
37896	MESGID_VC_DEL_HADEV	Notice
37897	MESGID_HADEV_READY	Notice

Log Message Details

Log ID	Log Message	Severity
37898	MESGID_HADEV_FAIL	Warning
37899	MESGID_HADEV_PEERINFO	Notice
37900	MESGID_HBDEV_DELETE	Notice
37901	MESGID_HBDEV_DOWN	Critical
37902	MESGID_HBDEV_UP	Information
37903	MESGID_SYNC_STATUS	Information
37904	MESGID_HA_ACTIVITY	Notice
37904	MESGID_HA_ACTIVITY	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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
date	The date the log event was generated on the device	String		
devid	The serial number of the device	String		
interface	Interface	String	32	
level	The log priority level	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		
msg	Explains the activity or event that the FortiGate unit recorded	String	256	
subtype	The subtype of the log message. The possible values of this field depend on the log type	String		• router
time	Time stamp of the event	String		
type	The log type	String		• event
vd	Virtual domain name	String		

Router Log Messages

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

Log Message Details

Message ID	Message	Severity
20300	LOG_ID_BGP_NB_STAT_CHG	Unknown
27001	LOG_ID_VRRP_STATE_CHG	Information
51000	51000	Information

System

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

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

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
act	accounting state	String	16	
action	The action the FortiGate unit should take for this firewall policy	String		
addr	address	IP Address		
assigned	assigned IP address	IP Address	39	
banned_rule	banned rule or rreason	String	36	
banned_src	banned source	String	16	• ips • dos • dlp-rule • dlp-compound • av
blocked	The number of blocked messages	UINT32	10	
bandwidth		String	42	
cfgattr	configuration attribute	String	0	
cfgobj	configuration object	String	256	
cfgpath	configuration path	String	128	
cfgtid	config transaction id	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
checksum	The number of content checksum blocked messages	UINT32	10	
cipher		String		
connection_type	Forticlient connection type	String	6	
conserve	flag for conserve mode	String	32	
converted_files	Files converted	UINT32	10	
count	The number of dropped SIP packets	UINT16		
cpu	The CPU usage, for performance	UINT8	3	
created	date created	String		
daddr	destination address 'dstip'	String	80	
daemon	Daemon name	String	32	
datarange	data range for reports	String		
date	The date the log event was generated on the device	String		
desc	description	String		
devid	The serial number of the device	String	16	
dhcp_msg	DHCP message	String	0	
dintf	device interface	String	36	
dns_ip	Domain name server IP address	IP Address	39	
dns_name	Domain name server name	String	64	
dport	The destination port number	UINT16	5	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
dstip	The destination IP address	IP Address		
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		
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry	UINT16		
entermargin	Enter margin	UINT32	10	
error	error reason for log upload to forticloud	String	256	
exitmargin	Exit margin	UINT32	10	
expected	Number of expected packets	String		
fams_pause		UINT32	10	
field	field name	String	32	
file	file name for a generated report	String	128	
filesize	report file size in bytes	UINT64		
forticlient_id	forticlient uuid	String	33	
free		String	32	
from	sender email address for notification	String	128	
gateway	gateway ip address for PPPoE status report	IP Address	39	
green		String	32	
handshake	Handshake session ID	String		
hash	character	String	32	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
hostname	The host name or IP	String	128	
id	ID / primary key for the record	String		
identidx	The identity index number	String		
infected	The number of infected messages	UINT32	10	
intercepted	The number of intercepted messages	UINT32	10	
interface	interface name or ID	String	32	
intf	user interface	String	16	
iptype	IP protocol type	String	16	
lease	lease IP address range	UINT32	10	
len	length	UINT16		
level	The log priority level	String	11	
license_ limit	License limit	String	32	
license_ used	License used	UINT16	5	
limit		UINT32	10	
local	Local IP address	IP Address	39	
log	log type	String	32	
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	
major	major priority level	String		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
max	Maximum value	String		
max-minor		String		
mem	The memory usage, for performance	UINT8	3	
min	Minimum value	String		
min-minor		String		
minor	minor priority level	String		
module	module name	String	32	
monitor-name		String	32	
monitor-type		String	32	
msg	Explains the activity or event that the FortiGate unit recorded	String	256	
msgproto	The message protocol	UINT8		
mtu	Maximum transmission unit	UINT32	10	
name	User or host name	String	128	
nat	Network address translation	IP Address	39	
new_status	latest status	String	512	
new_value	new virtual domain name	String	128	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
nf_type	The notification type	String	0	• bword • file_block • carrier_ ep_bwl • flood • dupe • alert • mms_ checksu m • virus
old_status	archived status	String	512	
old_value	original virtual domain name	String	16	
passwd	Password	String	20	
pid	Policy ID	UINT32	10	
policy	The policy that triggered this log	String		
policyid	The policy ID that triggered this log	UINT32	10	
poolname	The pool name	String	36	
port	port number	UINT8		
portbegin		UINT16	5	
portend		UINT16	5	
probeid		UINT32	10	
probeproto	The protocol	String	16	
processtime	process time for reports	String		
profile_vd	Virtual domain of the profile	String	64	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
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	0	
proto	The protocol	UINT8		
reason	The reason why the log was recorded	String		
received	Number of packets received	String		
recv-minor		String		
red		String	32	
remote	remote IP address	IP Address	39	
repeat		UINT16	5	
reporttype	report type	ENUM		
saddr	source address ip. use 'srcip'	String	80	
scanned	The number of scanned messages	UINT32	10	
sensor	sensor name	String	36	
serial	The serial number of the log message	UINT32		
serialno	serial number of the device	String	16	
server	server ip address	IP Address		
service	The service of where the activity or event occurred, whether it was on a web page using HTTP or HTTPs	String	0	
sess_duration	The duration of the session	UINT32	0	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
session_id	The session ID	UINT32	10	
setuprate		UNIT64		
slot	Slot ID	UINT8	0	
srcip	The source IP address	IP Address		
src_int	source interface - use 'srcintf'	String	64	
src_port	source port address	UINT16	5	
ssl2	ssl session	String		
status	The status of the action the FortiGate unit took when the event occurred	String		
submodule	submodule name	String	32	
subtype	The subtype of the log message. The possible values of this field depend on the log type	String		• system
suspicious	The number of suspicious messages	UINT32	10	
sysconserve	System conserve	String	32	
time	Time stamp of the event	String	8	
to	recipient email addresses for notification	String	512	
total	Total IP sessions	UINT32	10	
totalsession	Total IP sessions	UINT32	10	
trace_id	Trace ID	String	32	
type	The log type	String	16	• event
ui	User Interface	String		

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
unit		UINT32	10	
url	The URL address of where the file was acquired	String	512	
used		UINT32	10	
used_for_type	Type of service used	UINT16	5	
user	The name of the user creating the traffic	String	256	
vd	Virtual domain	String	32	
vip	Virtual IP address	String	64	
virus	virus name	String	128	

System Log Messages

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

Log Message Details

Message ID	Message	Severity
20000	20000	Debug
20001	LOG_ID_CLIENT_DISASSOCIATED	Information
20001	LOG_ID_CLIENT_DISASSOCIATED	Debug
20002	LOG_ID_DOMAIN_UNRESOLVABLE	Notice
20003	LOG_ID_MAIL_SENT_FAIL	Notice
20004	LOG_ID_POLICY_TOO_BIG	Unknown
20005	LOG_ID_PPP_LINK_UP	Information
20006	LOG_ID_PPP_LINK_DOWN	Information
20007	20007	Critical
20011	LOG_ID_CLIENT_NEW_ASSOCIATION	Information
20012	LOG_ID_CLIENT_WPA_1X	Information
20013	LOG_ID_CLIENT_WPA_SSN	Information
20015	LOG_ID_IEEE802_NEW_STATION	Information
20016	LOG_ID_MODEM_EXCEED_REDIAL_COUNT	Information
20020	LOG_ID_MODEM_HOTPLUG	Warning
20021	LOG_ID_MAIL_RESENT	Information
20025	LOG_ID_REPORTD_REPORT_SUCCESS	Notice
20026	LOG_ID_REPORTD_REPORT_FAILURE	Error

Log Message Details

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

Log Message Details

Message ID	Message	Severity
20051	LOG_ID_RAD_FAIL_OPT_IPV6_MULTICAST_HOPS	Critical
20052	LOG_ID_RAD_FAIL_OPT_IPV6_HOPLIMIT	Critical
20053	LOG_ID_RAD_FAIL_OPT_IPPROTO_ICMPV6	Critical
20054	LOG_ID_RAD_EXIT_BY_SIGNAL	Information
20055	LOG_ID_RAD_FAIL_CMDB_QUERY	Critical
20056	LOG_ID_RAD_FAIL_CMDB_FOR_EACH	Critical
20057	LOG_ID_RAD_FAIL_FIND_VIRT_INTF	Critical
20058	LOG_ID_RAD_UNLOAD_INTF	Information
20059	LOG_ID_RAD_NO_PKT_INFO	Warning
20060	LOG_ID_RAD_INV_ICMPV6_LEN	Warning
20061	LOG_ID_RAD_INV_ICMPV6_TYPE	Critical
20062	LOG_ID_RAD_INV_ICMPV6_RA_LEN	Warning
20063	LOG_ID_RAD_ICMPV6_NO_SRC_ADDR	Warning
20064	LOG_ID_RAD_INV_ICMPV6_RS_LEN	Warning
20065	LOG_ID_RAD_INV_ICMPV6_CODE	Warning
20066	LOG_ID_RAD_INV_ICMPV6_HOP	Warning
20067	LOG_ID_RAD_MISMATCH_HOP	Warning
20068	LOG_ID_RAD_MISMATCH_MGR_FLAG	Warning
20069	LOG_ID_RAD_MISMATCH_OTH_FLAG	Warning
20071	LOG_ID_RAD_MISMATCH_TIMER	Warning
20072	LOG_ID_RAD_EXTRA_DATA	Critical

Log Message Details

Message ID	Message	Severity
20073	LOG_ID_RAD_NO_OPT_DATA	Critical
20074	LOG_ID_RAD_INV_OPT_LEN	Critical
20075	LOG_ID_RAD_MISMATCH_MTU	Warning
20077	LOG_ID_RAD_MISMATCH_PREF_TIME	Warning
20078	LOG_ID_RAD_INV_OPT	Critical
20079	LOG_ID_RAD_READY	Information
20080	LOG_ID_RAD_FAIL_TO_RCV	Critical
20081	LOG_ID_RAD_INV_HOP	Critical
20082	LOG_ID_RAD_INV_PKTINFO	Critical
20083	LOG_ID_RAD_FAIL_TO_CHECK	Warning
20084	LOG_ID_RAD_FAIL_TO_SEND	Warning
20085	20085	Information
20086	20086	Unknown
20090	LOG_ID_INTF_LINK_STA_CHG	Notice
20099	LOG_ID_INTF_STA_CHG	Information
20100	20100	Critical
20101	LOG_ID_WEB_LIC_EXPIRE	Critical
20102	LOG_ID_SPAM_LIC_EXPIRE	Critical
20103	LOG_ID_AV_LIC_EXPIRE	Critical
20104	LOG_ID_IPS_LIC_EXPIRE	Warning
20105	LOG_ID_LOG_UPLOAD_SKIP	Warning

Log Message Details

Message ID	Message	Severity
20107	LOG_ID_LOG_UPLOAD_ERR	Warning
20108	LOG_ID_LOG_UPLOAD_DONE	Notice
20110	LOG_ID_HPAPI_ESPD_START	Notice
20111	LOG_ID_HPAPI_ESPD_RESET	Warning
20200	LOG_ID_FIPS_SELF_TEST	Notice
20201	LOG_ID_FIPS_SELF_ALL_TEST	Notice
20202	LOG_ID_DISK_FORMAT_ERROR	Warning
20203	LOG_ID_DAEMON_SHUTDOWN	Information
20204	LOG_ID_DAEMON_START	Information
20205	LOG_ID_DISK_FORMAT_REQ	Critical
20206	LOG_ID_DISK_SCAN_REQ	Warning
22000	LOG_ID_INV_PKT_LEN	Warning
22001	LOG_ID_UNSUPPORTED_PROT_VER	Warning
22002	LOG_ID_INV_REQ_TYPE	Warning
22003	LOG_ID_FAIL_SET_SIG_HANDLER	Warning
22004	LOG_ID_FAIL_CREATE_SOCKET	Warning
22005	LOG_ID_FAIL_CREATE_SOCKET_RETRY	Warning
22006	LOG_ID_FAIL_REG_CMDB_EVENT	Warning
22009	LOG_ID_FAIL_FIND_AV_PROFILE	Warning
22010	LOG_ID_SENDTO_FAIL	Error
22011	22011	Unknown

Log Message Details

Message ID	Message	Severity
22012	22012	Unknown
22013	22013	Alert
22014	22014	Alert
22015	LOG_ID_EXCEED_VD_RES_LIMIT	Notice
22016	22016	Notice
22020	LOG_ID_FAIL_CREATE_HA_SOCKET	Warning
22021	LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY	Warning
22100	LOG_ID_QUAR_DROP_TRAN_JOB	Warning
22101	LOG_ID_QUAR_DROP_TLL_JOB	Warning
22102	LOG_ID_LOG_DISK_FAILURE	Critical
22104	LOG_ID_POWER_RESTORE	Critical
22105	LOG_ID_POWER_FAILURE	Critical
22106	LOG_ID_POWER_OPTIONAL_NOT_DETECTED	Information
22110	LOG_ID_SPARE_BLOCK_LOW	Critical
22200	LOG_ID_AUTO_UPT_CERT	Warning
22201	LOG_ID_AUTO_GEN_CERT	Warning
22202	LOG_ID_AUTO_UPT_CERT_FAIL	Error
22203	LOG_ID_AUTO_GEN_CERT_FAIL	Error
22700	LOG_ID_IPS_FAIL_OPEN	Critical
22800	LOG_ID_SCAN_SERV_FAIL	Critical
22801	LOG_ID_SCAN_LEAVE_CONSERVE_MODE	Critical

Log Message Details

Message ID	Message	Severity
22802	LOG_ID_SYS_ENTER_CONSERVE_MODE	Critical
22803	LOG_ID_SYS_LEAVE_CONSERVE_MODE	Critical
22804	LOG_ID_LIC_STATUS_CHG	Critical
22805	LOG_ID_FAIL_TO_VALIDATE_LIC	Warning
22806	LOG_ID_DUP_LIC	Warning
22810	LOG_ID_SCAN_ENTER_CONSERVE_MODE	Critical
22900	LOG_ID_CAPUTP_SESSION	Notice
22901	LOG_ID_FAZ_CON	Notice
22902	LOG_ID_FAZ_DISCON	Notice
22903	LOG_ID_FAZ_CON_ERR	Critical
22916	LOG_ID_FDS_STATUS	Notice
22917	LOG_ID_FDS_SMS_QUOTA	Notice
22921	LOG_ID_EVENT_ROUTE_INFO_CHANGED	Critical
22922	LOG_ID_EVENT_LINK_MONITOR_STATUS	Notice
22923	LOG_ID_EVENT_VWL_LQTY_STATUS	Notice
22924	LOG_ID_EVENT_VWL_VOLUME_STATUS	Notice
26001	LOG_ID_DHCP_MSG	Information
26002	LOG_ID_DHCP_NO_SHARE_NET	Error
26003	LOG_ID_DHCP_STAT	Information
26004	LOG_ID_DHCP_MULT_SUB_NET	Error
26005	LOG_ID_DHCP_INV_ADDR_RANGE	Error

Log Message Details

Message ID	Message	Severity
29001	LOG_ID_PPPD_MSG	Unknown
29002	LOG_ID_PPPD_AUTH_SUC	Notice
29003	LOG_ID_PPPD_AUTH_FAIL	Notice
29009	LOG_ID_PPPOE_STATUS_REPORT	Notice
29011	LOG_ID_PPPD_FAIL_TO_EXEC	Error
29012	LOG_ID_PPP_OPT_ERR	Error
29012	LOG_ID_PPP_OPT_ERR	Unknown
29013	LOG_ID_PPPD_START	Error
29013	LOG_ID_PPPD_START	Notice
29013	LOG_ID_PPPD_START	Unknown
29014	LOG_ID_PPPD_EXIT	Information
29015	LOG_ID_PPP_RCV_BAD_PEER_IP	Error
29016	LOG_ID_PPP_RCV_BAD_LOCAL_IP	Error
29017	LOG_ID_PPP_OPT_NOTIF	Error
29017	LOG_ID_PPP_OPT_NOTIF	Unknown
29020	LOG_ID_WIRELESS_SET_FAIL	Error
29020	LOG_ID_WIRELESS_SET_FAIL	Notice
29020	LOG_ID_WIRELESS_SET_FAIL	Unknown
32001	LOG_ID_ADMIN_LOGIN_SUCC	Error
32001	LOG_ID_ADMIN_LOGIN_SUCC	Notice
32001	LOG_ID_ADMIN_LOGIN_SUCC	Information

Log Message Details

Message ID	Message	Severity
32001	LOG_ID_ADMIN_LOGIN_SUCC	Unknown
32002	LOG_ID_ADMIN_LOGIN_FAIL	Alert
32003	LOG_ID_ADMIN_LOGOUT	Information
32005	LOG_ID_ADMIN_OVERIDE_VDOM	Information
32006	LOG_ID_ADMIN_ENTER_VDOM	Information
32007	LOG_ID_ADMIN_LEFT_VDOM	Information
32008	LOG_ID_VIEW_LOG_FAIL	Warning
32009	LOG_ID_SYSTEM_START	Information
32010	LOG_ID_DISK_LOG_FULL	Emergency
32011	LOG_ID_LOG_ROLL	Notice
32012	LOG_ID_FIPS_LEAVE_ERR_MOD	Information
32014	LOG_ID_CS_LIC_EXPIRE	Warning
32015	LOG_ID_DISK_LOG_USAGE	Warning
32018	LOG_ID_FIPS_ENTER_ERR_MOD	Emergency
32020	LOG_ID_SSH_CORRPUT_MAC	Warning
32021	LOG_ID_ADMIN_LOGIN_DISABLE	Alert
32022	LOG_ID_VDOM_ENABLED	Notice
32023	LOG_ID_MEM_LOG_FULL	Warning
32024	LOG_ID_ADMIN_PASSWD_EXPIRE	Notice
32026	LOG_ID_STORE_CONF_FAIL	Critical
32027	LOG_ID_VIEW_LOG_SUCC	Critical

Log Message Details

Message ID	Message	Severity
32027	LOG_ID_VIEW_LOG_SUCC	Notice
32028	LOG_ID_LOG_DEL_DIR	Information
32029	LOG_ID_LOG_DEL_FILE	Warning
32030	LOG_ID_SEND_FDS_STAT	Notice
32035	LOG_ID_VDOM_DISABLED	Notice
32040	LOG_ID_REPORT_DELETED	Information
32045	LOG_ID_MGR_LIC_EXPIRE	Warning
32048	LOG_ID_SCHEDULE_EXPIRE	Warning
32049	LOG_ID_FC_EXPIRE	Warning
32051	LOG_ID_LOG_UPLOAD	Notice
32086	LOG_ID_ENTER_TRANSPARENT	Warning
32087	LOG_ID_ENTER_NAT	Warning
32095	LOG_ID_GUI_CHG_SUB_MODULE	Warning
32096	LOG_ID_GUI_DOWNLOAD_LOG	Warning
32100	LOG_ID_FORTI_TOKEN_SYNC	Warning
32101	LOG_ID_LCD_CHG_CONF	Notice
32102	LOG_ID_CHG_CONFIG	Unknown
32103	LOG_ID_NEW_FIRMWARE	Notice
32120	LOG_ID_RPT_ADD_DATASET	Notice
32122	LOG_ID_RPT_DEL_DATASET	Notice
32125	LOG_ID_RPT_ADD_CHART	Notice

Log Message Details

Message ID	Message	Severity
32126	LOG_ID_RPT_DEL_CHART	Notice
32129	LOG_ID_ADD_GUEST	Notice
32130	LOG_ID_CHG_USER	Notice
32131	LOG_ID_DEL_GUEST	Notice
32132	LOG_ID_ADD_USER	Notice
32138	LOG_ID_REBOOT	Critical
32139	LOG_ID_UPD_SIGN_DB	Critical
32140	LOG_ID_NTP_SVR_STAUS_CHG	Notice
32142	LOG_ID_BACKUP_CONF	Alert
32148	LOG_ID_GET_CRL	Notice
32149	LOG_ID_COMMAND_FAIL	Notice
32151	LOG_ID_ADD_IP6_LOCAL_POL	Notice
32152	LOG_ID_CHG_IP6_LOCAL_POL	Notice
32153	LOG_ID_DEL_IP6_LOCAL_POL	Notice
32155	LOG_ID_ACT_FTOKEN_REQ	Notice
32156	LOG_ID_ACT_FTOKEN_SUCC	Notice
32157	LOG_ID_SYNC_FTOKEN_SUCC	Notice
32158	LOG_ID_SYNC_FTOKEN_FAIL	Notice
32159	LOG_ID_ACT_FTOKEN_FAIL	Notice
32168	LOG_ID_REACH_VDOM_LIMIT	Notice
32170	LOG_ID_ALARM_MSG	Alert

Log Message Details

Message ID	Message	Severity
32171	LOG_ID_ALARM_ACK	Alert
32172	LOG_ID_ADD_IP4_LOCAL_POL	Notice
32173	LOG_ID_CHG_IP4_LOCAL_POL	Notice
32174	LOG_ID_DEL_IP4_LOCAL_POL	Notice
32188	LOG_ID_SSL_PROXY_CA_INIT_FAIL	Warning
32188	LOG_ID_SSL_PROXY_CA_INIT_FAIL	Notice
32200	LOG_ID_SHUTDOWN	Critical
32201	LOG_ID_LOAD_IMG_SUCC	Critical
32202	LOG_ID_RESTORE_IMG	Critical
32203	LOG_ID_RESTORE_CONF	Critical
32204	LOG_ID_RESTORE_FGD_SVR	Critical
32205	LOG_ID_RESTORE_VDOM_LIC	Critical
32206	LOG_ID_RESTORE_SCRIPT	Warning
32207	LOG_ID_RETRIEVE_CONF_LIST	Warning
32208	LOG_ID_IMP_PKCS12_CERT	Critical
32209	LOG_ID_RESTORE_USR_DEF_IPS	Critical
32210	LOG_ID_BACKUP_IMG	Notice
32211	LOG_ID_UPLOAD_REVISION	Notice
32212	LOG_ID_DEL_REVISION	Notice
32213	LOG_ID_RESTORE_TEMPLATE	Warning
32214	LOG_ID_RESTORE_FILE	Warning

Log Message Details

Message ID	Message	Severity
32215	LOG_ID_UPT_IMG	Critical
32217	LOG_ID_UPD_IPS	Warning
32218	LOG_ID_UPD_DLP	Warning
32219	LOG_ID_BACKUP_OUTPUT	Warning
32220	LOG_ID_BACKUP_COMMAND	Warning
32221	LOG_ID_UPD_VDOM_LIC	Warning
32222	LOG_ID_GLB_SETTING_CHG	Notice
32223	LOG_ID_BACKUP_USER_DEF_IPS	Error
32224	LOG_ID_BACKUP_LOG	Notice
32225	LOG_ID_DEL_ALL_REVISION	Notice
32226	LOG_ID_LOAD_IMG_FAIL	Critical
32240	LOG_ID_SYS_USB_MODE	Critical
32252	LOG_ID_FACTORY_RESET	Critical
32253	LOG_ID_FORMAT_RAID	Critical
32254	LOG_ID_ENABLE_RAID	Critical
32255	LOG_ID_DISABLE_RAID	Critical
32300	LOG_ID_UPLOAD_RPT_IMG	Notice
32301	LOG_ID_ADD_VDOM	Notice
32302	LOG_ID_DEL_VDOM	Notice
32340	LOG_ID_LOG_DISK_UNAVAIL	Critical
32400	LOG_ID_CONF_CHG	Alert

Log Message Details

Message ID	Message	Severity
32545	LOG_ID_SYS_RESTART	Critical
32546	LOG_ID_APPLICATION_CRASH	Warning
35001	LOG_ID_HA_SYNC_VIRDB	Notice
35002	LOG_ID_HA_SYNC_ETDB	Notice
35003	LOG_ID_HA_SYNC_EXDB	Notice
35005	LOG_ID_HA_SYNC_IPS	Notice
35007	LOG_ID_HA_SYNC_AV	Notice
35008	LOG_ID_HA_SYNC_VCM	Notice
35009	LOG_ID_HA_SYNC_CID	Notice
35010	LOG_ID_HA_SYNC_FAIL	Error
36880	LOG_ID_EVENT_SYSTEM_MAC_HOST_STORE_LIMIT	Warning
37888	MESGID_HA_GROUP_DELETE	Notice
37889	MESGID_VC_DELETE	Notice
37890	MESGID_VC_MOVE_VDOM	Notice
37891	MESGID_VC_ADD_VDOM	Notice
37892	MESGID_VC_MOVE_MEMB_STATE	Notice
37893	MESGID_VC_DETECT_MEMB_DEAD	Critical
37893	MESGID_VC_DETECT_MEMB_DEAD	Notice
37894	MESGID_VC_DETECT_MEMB_JOIN	Critical
37895	MESGID_VC_ADD_HADEV	Notice

Log Message Details

Message ID	Message	Severity
37896	MESGID_VC_DEL_HADEV	Notice
37897	MESGID_HADEV_READY	Notice
37898	MESGID_HADEV_FAIL	Warning
37899	MESGID_HADEV_PEERINFO	Notice
37900	MESGID_HBDEV_DELETE	Notice
37901	MESGID_HBDEV_DOWN	Critical
37902	MESGID_HBDEV_UP	Information
37903	MESGID_SYNC_STATUS	Information
37904	MESGID_HA_ACTIVITY	Notice
38400	LOGID_EVENT_NOTIF_SEND_SUCC	Notice
38401	LOGID_EVENT_NOTIF_SEND_FAIL	Warning
38402	LOGID_EVENT_NOTIF_DNS_FAIL	Notice
38403	LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE	Critical
38404	LOGID_EVENT_NOTIF_HOSTNAME_ERROR	Error
38405	LOGID_NOTIF_CODE_SENDTO_SMS_PHONE	Notice
38406	LOGID_NOTIF_CODE_SENDTO_SMS_TO	Notice
38407	LOGID_NOTIF_CODE_SENDTO_EMAIL	Notice
40704	LOG_ID_EVENT_SYS_PERF	Notice
41000	LOG_ID_UPD_FGT_SUCC	Notice
41001	LOG_ID_UPD_FGT_FAIL	Critical
41002	LOG_ID_UPD_SRC_VIS	Notice

Log Message Details

Message ID	Message	Severity
41003	LOG_ID_INVALID_UPD_LIC	Critical
41005	LOG_ID_UPD_VCM	Notice
43264	LOGID_MMS_STATS	Information
43776	LOGID_EVENT_NAC_QUARANTINE	Notice
43800	LOG_ID_EVENT_ELBC_BLADE_JOIN	Critical
43801	LOG_ID_EVENT_ELBC_BLADE_LEAVE	Critical
43802	LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND	Critical
43803	LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST	Critical
43804	LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE	Critical
43805	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND	Critical
43806	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST	Critical
43807	LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE	Critical
43808	LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE	Critical
43809	LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE	Critical
44544	LOGID_EVENT_CONFIG_PATH	Information
44545	LOGID_EVENT_CONFIG_OBJ	Information
44546	LOGID_EVENT_CONFIG_ATTR	Information
44547	LOGID_EVENT_CONFIG_OBJATTR	Information
45000	LOG_ID_VSD_SSL_RCV_HS	Debug
45001	LOG_ID_VSD_SSL_RCV_WRG_HS	Error

Log Message Details

Message ID	Message	Severity
45002	LOG_ID_VSD_SSL_SENT_HS	Debug
45003	LOG_ID_VSD_SSL_WRG_HS_LEN	Error
45004	LOG_ID_VSD_SSL_RCV_CCS	Debug
45005	LOG_ID_VSD_SSL_RSA_DH_FAIL	Error
45006	LOG_ID_VSD_SSL_SENT_CCS	Debug
45007	LOG_ID_VSD_SSL_BAD_HASH	Error
45009	LOG_ID_VSD_SSL_DECRY_FAIL	Error
45010	LOG_ID_VSD_SSL_SESSION_CLOSED	Debug
45011	LOG_ID_VSD_SSL_LESS_MINOR	Error
45012	LOG_ID_VSD_SSL_REACH_MAX_CON	Warning
45013	LOG_ID_VSD_SSL_NOT_SUPPORT_CS	Error
45016	LOG_ID_VSD_SSL_HS_FIN	Debug
45017	LOG_ID_VSD_SSL_HS_TOO_LONG	Error
45018	LOG_ID_VSD_SSL_MORE_MINOR	Debug
45019	LOG_ID_VSD_SSL_SENT_ALERT_ERR	Error
45020	LOG_ID_VSD_SSL_SESSION_EXPIRE	Debug
45021	LOG_ID_VSD_SSL_SENT_ALERT	Debug
45022	LOG_ID_VSD_SSL_RCV_CH	Debug
45023	LOG_ID_VSD_SSL_RCV_SH	Debug
45024	LOG_ID_VSD_SSL_SENT_SH	Debug
45025	LOG_ID_VSD_SSL_RCV_ALERT	Error

Log Message Details

Message ID	Message	Severity
45027	LOG_ID_VSD_SSL_INVALID_CONT_TYPE	Error
45029	LOG_ID_VSD_SSL_BAD_CCS_LEN	Error
45031	LOG_ID_VSD_SSL_BAD_DH	Error
45032	LOG_ID_VSD_SSL_PUB_KEY_TOO_BIG	Error
45033	LOG_ID_VSD_SSL_NOT_SUPPORT_CM	Error
45034	LOG_ID_VSD_SSL_SERVER_KEY_HASH_ALGORITHM_MISMATCH	Error
45035	LOG_ID_VSD_SSL_SERVER_KEY_SIGNATURE_ALGORITHM_MISMATCH	Error
46000	LOG_ID_VIP_REAL_SVR_ENA	Notice
46001	LOG_ID_VIP_REAL_SVR_DISA	Alert
46002	LOG_ID_VIP_REAL_SVR_UP	Notice
46003	LOG_ID_VIP_REAL_SVR_DOWN	Alert
46004	LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN	Notice
46005	LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN	Alert
46006	LOG_ID_VIP_REAL_SVR_FAIL	Debug
46400	LOG_ID_EVENT_EXT_SYS	Unknown
46401	LOG_ID_EVENT_EXT_LOCAL	Unknown
46402	LOG_ID_EVENT_EXT_REMOTE	Unknown
47201	LOG_ID_AMC_ENTER_BYPASS	Emergency
47202	LOG_ID_AMC_EXIT_BYPASS	Emergency

Log Message Details

Message ID	Message	Severity
47203	LOG_ID_ENTER_BYPASS	Emergency
47204	LOG_ID_EXIT_BYPASS	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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
acct_stat	Accounting state (RADIUS)	ENUM	16	• Accounting-Off • Accounting-On • Interim-Update • start • stop
action	The action the FortiGate unit should take for this firewall policy	String	32	
adgroup	AD Group Name	String	128	
authproto	The protocol that initiated the authentication	String	64	
carrier_ep	The FortiOS Carrier end-point identification	String	0	
count	Number of Packets	UINT32	0	
date	The date the log event was generated on the device	String	10	
devid	The serial number of the device	String	16	
dstip	Destination IP	IP Address	39	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry.	UINT32		
expiry	FortiGuard override expiry timestamp	String	64	
group	User name group	String	64	
initiator	Original login user name for Fortiguard override	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	Explains the activity or event that the FortiGate unit recorded	String	256	
oldwprof	Old Web Filter Profile	String	64	
policyid		UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
approfile	New Web Filter Profile for Fortiguard override	String	64	
proto	protocol number	UINT16	0	
reason	Explains the reason why the log message was created	String	256	
rsso_key	RADIUS SSO attribute value	String	64	
scope		String	9	
server	AD server FQDN or IP	String	64	
srcip	Source IP	IP Address	39	
status	The status of the action the FortiGate unit took when the event occurred	String		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• user
time	Time stamp of the event	String	8	
type	The log type	String	16	• event
user	user name	String	256	
vd	virtual domain name	String	32	

User Log Messages

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

Log Message Details

Message ID	Message	Severity
38010	LOG_ID_FIPS_ENCRY_FAIL	Alert
38011	LOG_ID_FIPS_DECRY_FAIL	Alert
38031	LOG_ID_FSSO_LOGON	Notice
38032	LOG_ID_FSSO_LOGOFF	Notice
38033	LOG_ID_FSSO_SVR_STATUS	Notice
38656	LOGID_EVENT_RAD_RPT_PROTO_ERROR	Notice
38657	LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND	Notice
38658	LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND	Notice
38659	LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED	Notice
38660	LOGID_EVENT_RAD_RPT_ACCT_EVENT	Notice
38661	LOGID_EVENT_RAD_RPT_OTHER	Notice
38662	LOGID_EVENT_RAD_STAT_PROTO_ERROR	Notice
38663	LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND	Notice
38665	LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED	Notice
38666	LOGID_EVENT_RAD_STAT_ACCT_EVENT	Notice
38667	LOGID_EVENT_RAD_STAT_OTHER	Notice
38668	LOGID_EVENT_RAD_STAT_EP_BLK	Notice
43011	LOG_ID_EVENT_AUTH_TIME_OUT	Notice

Message ID	Message	Severity
43012	LOG_ID_EVENT_AUTH_FSAE_AUTH_SUCCESS	Notice
43013	LOG_ID_EVENT_AUTH_FSAE_AUTH_FAIL	Notice
43016	LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS	Notice
43017	LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL	Notice
43018	LOG_ID_EVENT_AUTH_FGOVRD_FAIL	Warning
43020	LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS	Notice
43025	LOG_ID_EVENT_AUTH_PROXY_SUCCESS	Notice
43026	LOG_ID_EVENT_AUTH_PROXY_FAILED	Notice
43027	LOG_ID_EVENT_AUTH_PROXY_TIME_OUT	Notice
43028	LOG_ID_EVENT_AUTH_PROXY_AUTHORIZATION_FAILED	Notice
43029	LOG_ID_EVENT_AUTH_WARNING_SUCCESS	Notice
43030	LOG_ID_EVENT_AUTH_WARNING_TBL_FULL	Warning

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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
assign ip	Assigned IP address	IP Address		
cert-type	Certification type	ENUM	6	• CA • CRL • Local • Remote
cookies	cookies	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	direction (inbound or outbound)	String	8	
dst_host	destination host name	String	64	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
duration	The duration of the interval for item counts (such as infected, scanned, etc) in this log entry	UINT32		
error_reason	Text explanation for the error	String	48	• invalid certificate • invalid SA payload • probable pre-shared key mismatch • peer SA proposal not match local policy • peer notification • not enough key material for tunnel • encapsulation mode mismatch • no matching gateway for new request • aggressive vs main mode mismatch for new request
espauth	ESP authentication	String	17	• HMAC_SHA1 • HMAC_MD5 • HMAC_SHA256
esptransform	ESP tranfrom value	String	8	• ESP_NULL • ESP_DES • ESP_3DES • ESP_AES
exch	exchange	String	12	• NSA_INIT • AUTH • CREATE_CHILD
group	User name group	String	64	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
in_spi	Remote SPI in IPsec VPN configuration	String	16	
init	Interface	String	6	• local • remote
level	The log priority level	String	11	
locip	Local IP	IP Address	39	
locport	Local Port	UINT16	5	
logdesc	Log description	String	128	
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	Mode	String	12	• aggressive • main • quick • xauth • xauth_client

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
msg	Explains the activity or event that the FortiGate unit recorded	String	256	
nextstat	Time interval in seconds for the next statistics	UINT32	10	
out_spi	Local SPI in IPsec VPN configuration	String	16	
outintf	Out interface	String	32	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
peer_notif	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

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
phase2_name	IPsec VPN Phase 2 name	String	128	
rcvdbyte	Received Bytes	UINT64	20	
reason	The reason this log was generated	String	256	
remip	Remote IP	IP Address	39	
remport	Remote Port	UINT16	5	
result	The result of the message	String	7	• ERROR • OK • DONE • PENDING
sentbyte	bytes sent	UINT64	20	
seq	Sequence number	String	16	
spi	IPsec VPN SPI	String	16	
stage	stage	UINT8	3	
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• vpn
time	Time stamp of the event	String	8	
tunnelid	Tunnel ID	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
tunnelip	Tunnel IP	IP Address	39	
tunneltype	Tunnel type	String	64	
type	The log type	String	16	- event
vd	Virtual domain name	String	32	
version	Software version	String	64	
vpntunnel	ipsec vpn tunnel name	String	128	
xauthgroup	xauth group name	String	128	
xauthuser	xauth user	String	128	

VPN Log Messages

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

Log Message Details

Message ID	Message	Severity
37124	MESGID_NEG_I_P1_ERROR	Error
37125	MESGID_NEG_I_P2_ERROR	Error
37126	MESGID_NEG_NO_STATE_ERROR	Error
37133	MESGID_INSTALL_SA	Notice
37134	MESGID_DELETE_P1_SA	Notice
37135	MESGID_DELETE_P2_SA	Notice
37136	MESGID_DPD_FAILURE	Error
37137	MESGID_CONN_FAILURE	Error
37138	MESGID_CONN_UPDOWN	Notice
37139	MESGID_P2_UPDOWN	Notice
37140	MESGID_AUTO_IPSEC	Notice
37141	MESGID_CONN_STATS	Notice
37188	MESGID_NEG_I_P1_ERROR_IKEV2	Error
37189	MESGID_NEG_I_P2_ERROR_IKEV2	Error
37190	MESGID_NEG_NO_STATE_ERROR_IKEV2	Error
37197	MESGID_INSTALL_SA_IKEV2	Notice
37198	MESGID_DELETE_P1_SA_IKEV2	Notice
37199	MESGID_DELETE_P2_SA_IKEV2	Notice

Log Message Details

Message ID	Message	Severity
37200	MESGID_DPD_FAILURE_IKEV2	Error
37201	MESGID_CONN_FAILURE_IKEV2	Error
37202	MESGID_CONN_UPDOWN_IKEV2	Notice
37203	MESGID_P2_UPDOWN_IKEV2	Notice
37204	MESGID_CONN_STATS_IKEV2	Notice
40014	LOG_ID_PPTP_REACH_MAX_CON	Warning
40016	LOG_ID_L2TPD_SVR_DISCON	Warning
40017	LOG_ID_L2TPD_CLIENT_CON_FAIL	Warning
40019	LOG_ID_L2TPD_CLIENT_DISCON	Information
40021	LOG_ID_PPTP_NOT_CONIG	Debug
40022	LOG_ID_PPTP_NO_IP_AVAIL	Warning
40024	LOG_ID_PPTP_OUT_MEM	Warning
40034	LOG_ID_PPTP_START	Notice
40035	LOG_ID_PPTP_START_FAIL	Error
40036	LOG_ID_PPTP_EXIT	Notice
40037	LOG_ID_PPTPD_SVR_DISCON	Information
40038	LOG_ID_PPTPD_CLIENT_CON	Information
40039	LOG_ID_PPTPD_CLIENT_DISCON	Information
40114	LOG_ID_L2TPD_START	Notice
40115	LOG_ID_L2TPD_EXIT	Notice
40118	LOG_ID_L2TPD_CLIENT_CON	Information

Log Message Details

Message ID	Message	Severity
41984	LOG_ID_EVENT_SSL_VPN_CERT_LOAD	Information
41985	LOG_ID_EVENT_SSL_VPN_CERT_REMOVAL	Information
41987	LOG_ID_EVENT_SSL_VPN_CERT_UPDATE	Information
41988	LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE	Information
41989	LOG_ID_EVENT_SSL_VPN_CERT_ERR	Information
41990	LOG_ID_EVENT_SSL_VPN_CERT_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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
action	The action the FortiGate unit should take for this firewall policy	ENUM		
addr_type	Address type	String	4	
alert	Alert	String		
app-type	Application type	String		
authgrp	Authenticated group	String	36	
date	The date the log event was generated on the device	String		
desc	Description	String		
devid	The serial number of the device	String		
dstip	The destination IP address	IP Address		
dstport	The destination port number of the TCP or UDP traffic. The destination port is zero for other types of traffic	UINT8		
fqdn		String	256	
fwserver_ name	Firewall server name	String	32	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
handshake	Handshake IP address	String	32	
host	The host IP address	String	256	
ip	IP address	IP Address		
level	The log priority level	String		
local	Local IP address	IP Address		
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	Explains the activity or event that the FortiGate unit recorded	String	256	
peer	Peer IP address	String	36	
policyid	The ID number of the firewall 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 article, Firewall policy=0	String		
port	Port scanned	UINT16	5	
remote	Remote IP address	IP Address		
serial	The serial number of the log message	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
session_id	The session ID	String		
srcip	The source IP address	IP Address		
srcport	The source port of the TCP or UDP traffic. The source protocol is zero for other types of traffic	INT8		
subtype	The subtype of the log message. The possible values of this field depend on the log type	String		• wad
time	Time stamp of the event	String	8	
type	The log type	String		• event
vd	Virtual domain name	String	32	

WAD Log Messages

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

Log Message Details

Message ID	Message	Severity
40960	LOGID_EVENT_WAD_WEBPROXY_FWD_SRV_ERROR	Notice
48000	LOG_ID_WAD_SSL_RCV_HS	Debug
48001	LOG_ID_WAD_SSL_RCV_WRG_HS	Error
48002	LOG_ID_WAD_SSL_SENT_HS	Debug
48003	LOG_ID_WAD_SSL_WRG_HS_LEN	Error
48004	LOG_ID_WAD_SSL_RCV_CCS	Debug
48005	LOG_ID_WAD_SSL_RSA_DH_FAIL	Error
48006	LOG_ID_WAD_SSL_SENT_CCS	Debug
48007	LOG_ID_WAD_SSL_BAD_HASH	Error
48009	LOG_ID_WAD_SSL_DECRY_FAIL	Error
48011	LOG_ID_WAD_SSL_LESS_MINOR	Error
48013	LOG_ID_WAD_SSL_NOT_SUPPORT_CS	Error
48016	LOG_ID_WAD_SSL_HS_FIN	Debug
48017	LOG_ID_WAD_SSL_HS_TOO_LONG	Error
48019	LOG_ID_WAD_SSL_SENT_ALERT	Error
48023	LOG_ID_WAD_SSL_RCV_ALERT	Error
48027	LOG_ID_WAD_SSL_INVALID_CONT_TYPE	Error
48029	LOG_ID_WAD_SSL_BAD_CCS_LEN	Error

Message ID	Message	Severity
48031	LOG_ID_WAD_SSL_BAD_DH	Error
48032	LOG_ID_WAD_SSL_PUB_KEY_TOO_BIG	Error
48100	LOG_ID_WAD_AUTH_FAIL_CERT	Error
48101	LOG_ID_WAD_AUTH_FAIL_PSK	Error
48102	LOG_ID_WAD_AUTH_FAIL_OTH	Error
48300	LOG_ID_WRG_SVR_FGT_CONF	Critical
48301	LOG_ID_UNEXP_APP_TYPE	Critical

Wireless

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 Details

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	time in seconds - time passed since last seen	UINT32	10	
ap	The physical access point name	String	36	
apscan	The name of the AP, which scanned and detected the rogue AP	String	36	
aptype	AP Type	UINT8	3	
bssid	Service Set ID	String	17	
cfgtxpower	Config TX power	UINT32	10	
channel	Channel	UINT8	3	
configcountry	Config Country	String	4	
date	The date the log event was generated on the device	String	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
detectionmethod	Detection method	String	21	
devid	The serial number of the device	String	16	
ds	direction with distribution system	String	8	
eapolcnt	EAPOL packet count	UINT32	10	
eapoltype	EAPOL packet type	ENUM	16	
encrypt	whether the packet is encrypted or not	UINT8	3	
frametype	the type of frame used in traffic	String	32	
invalidmac	the MAC address with invalid OUI	String	17	
ip	IP address	IP Address	39	
level	The log priority level	String	11	
live	time in seconds	UINT32	10	
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 Details

Log Field Name	Log Field Description	Data Type	Length	Value
manuf	Manufacturer name	String	20	
meshmode	Mesh mode	String	19	
mgmtcnt	The number of unauthorized client flooding management frames	UINT32	10	
msg	Explains the activity or event that the FortiGate unit recorded	String	256	
noise	Traffic noise	INT8	4	
onwire	A flag to indicate if the AP is onwire or not	String	3	
opercountry	Operating Country	String	4	
opertxpower	Operating TX power	UINT32	10	
approfile	The application profile	String	36	
radioband	Radio band ID	String	64	
radioid	Radio signal ID	UINT8	3	
radioidclosest	Radio ID on the AP closest the rogue AP	UINT8	3	
radioiddetected	Radio ID on the AP which detected the rogue AP	UINT8	3	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
rate	Traffic rate	UINT8	3	
reason	The reason for which log was generated	String	256	
rssi	Received signal strength indicator	UINT8	3	
security	The wireless security	String	10	• open • wep64 • wep128 • wpa-psk • wpa-radius • wpa • wpa2 • wpa2-auto
securitymode	Security mode	String	20	
signal	Traffic signal	INT8	4	
snclosest	SN of the AP closest to the rogue AP	String	36	
sndetected	SN of the AP which detected the rogue AP	String	36	
snmeshparent	SN of the mesh parent	String	36	
ssid	Base Service Set ID	String	33	
stacount	Number of stations/clients	UINT32	10	

Log Details

Log Field Name	Log Field Description	Data Type	Length	Value
stamac	Station/Client MAC address	String	17	
status	The status of the action the FortiGate unit took when the event occurred	UINT8	3	
subtype	The subtype of the log message. The possible values of this field depend on the log type	String	20	• wireless
tamac	the MAC address of Transmitter, if none, then Receiver	String	17	
threattype	WIDS threat type	String	64	
time	Time stamp of the event	String	8	
type	The log type	String	16	• event
vap	The virtual access point name	String	36	
vd	Virtual domain name	String	32	
weakwepiv	Weak Wep Initiation Vector	String	8	

Wireless Log Messages

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

Log Message Details

Message ID	Message	Severity
43520	LOG_ID_EVENT_WIRELESS_SYS	Notice
43521	LOG_ID_EVENT_WIRELESS_ROGUE	Unknown
43522	LOG_ID_EVENT_WIRELESS_WTP	Notice
43524	LOG_ID_EVENT_WIRELESS_STA	Notice
43525	LOG_ID_EVENT_WIRELESS_ONWIRE	Unknown
43526	LOG_ID_EVENT_WIRELESS_WTPR	Notice
43527	LOG_ID_EVENT_WIRELESS_ROGUE_CFG	Notice
43528	LOG_ID_EVENT_WIRELESS_WTPR_ERROR	Unknown
43529	LOG_ID_EVENT_WIRELESS_CLB	Notice
43530	LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE	Notice
43531	LOG_ID_EVENT_WIRELESS_WIDS_BR_DEAUTH	Notice
43532	LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP	Notice
43533	LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI	Notice
43534	LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR	Notice
43535	LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV	Notice
43542	LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD	Notice
43544	LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD	Notice
43546	LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH	Notice

High Performance Network Security