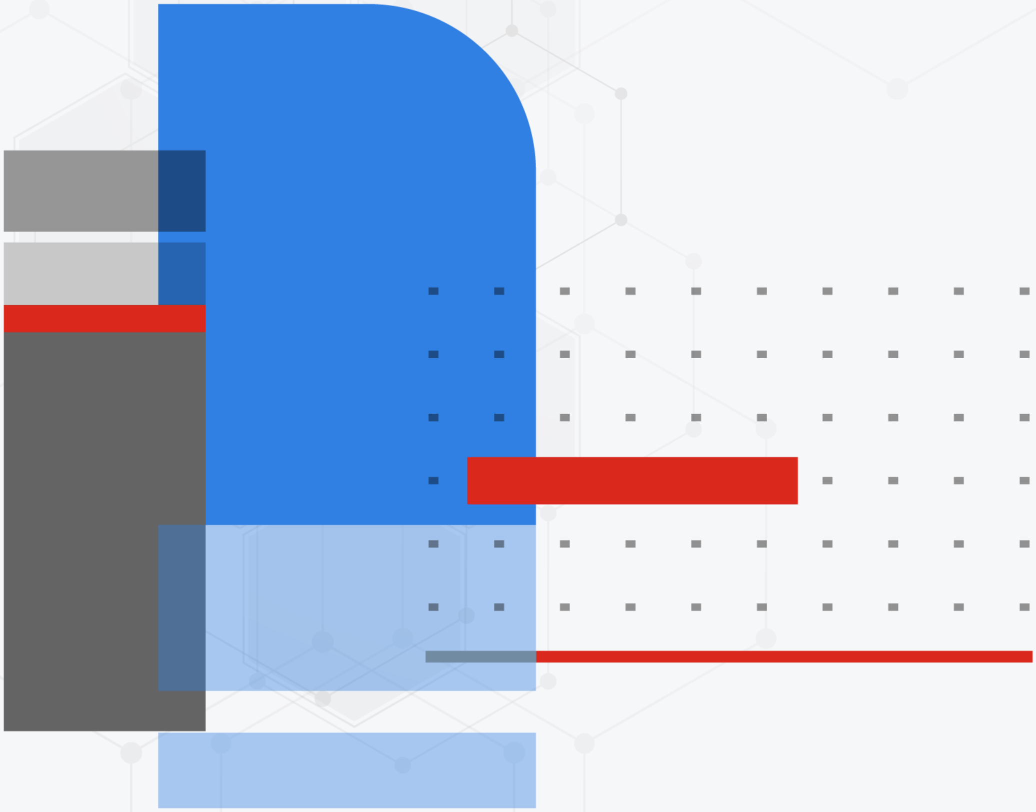
FORTINET

Log Reference

FortiOS 7.4.9



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

September 25, 2025
FortiOS 7.4.9 Log Reference
01-749-905022-20250925

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-09-25	Initial release.

Introduction

This document provides information about all the log messages applicable to the FortiGate devices running FortiOS version 7.4.9 or higher. The logs are intended for administrators to use as reference for more information about a specific log entry and message generated by FortiOS.

This document also provides information about log fields when FortiOS sends log messages to remote syslog servers in Common Event Format (CEF). See CEF support on page 68. It also describes how to enable extended logging. See UTM extended logging on page 79.

Performance statistics are not logged to disk. Performance statistics can be received by a syslog server or by FortiAnalyzer.

Before you begin

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

- Information in this document applies to all FortiGate units that are currently running FortiOS 7.4.9 or higher.
- Ensure that you have enabled logging for the FortiOS unit.
- Each log message is displayed in the *Log & Report* pane of the GUI. You can also download the RAW format from the *Log & Report* pane.
- Each log message is documented similar to how it appears in the RAW format.

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

What's new

This section identifies major changes in the Log Reference from version 7.4.0 and later. For more information about new features, please see the FortiOS 7.4 New Features Guide.

FortiOS 7.4.9

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
22118	LOG_ID_HW_MONITOR_EMERGENCY	Log ID Added
22119	LOG_ID_HW_MONITOR_WARNING	Log ID Added
22120	LOG_ID_HW_MONITOR_NOTIF	Log ID Added

FortiOS 7.4.8

Log field values

The following log field values are changed:

event logs:

Field	Change
modem	Field removed
simslot	Field removed

FortiOS 7.4.7

There are no major log changes between FortiOS 7.4.6 and 7.4.7.

FortiOS 7.4.6

Log field values

The following log field values are changed:

event logs:

Field	Change
connector	Field Added

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
22907	LOG_ID_INPUT_DETECTION	Log ID Added
22908	LOG_ID_OUTPUT_DETECTION	Log ID Added

FortiOS 7.4.5

Log field values

No log field values are changed.

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
22905	LOG_ID_LOGDEV_STATUS_CHANGE	Log ID Added
22906	LOG_ID_SECURITY_LEVEL_CHANGE	Log ID Added
46527	LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_SIM_STATE	Log ID Added
53050	LOG_ID_FTC_AUTH_FAILED	Log ID Added
53402	LOG_ID_FGFM_RECOVERY	Log ID Added
53407	LOG_ID_FABRIC_VPN_PSK_SECRET_UPG_SET	Log ID Added

ssh logs:

Log ID	Message	Change
61014	LOG_ID_SSH_UNSUPPORT_PROTO_BLOCK	Log ID Added
61015	LOG_ID_SSH_UNSUPPORT_PROTO_PASS	Log ID Added

FortiOS 7.4.4

Log field values

The following log field values are changed:

casb logs:

Field	Change
operation	Field Added
policytype	Field Added

event logs:

Field	Change
requesttype	Field Added

traffic logs:

Field	Change
srcremote	Field Added

virus logs:

Field	Change
contentencoding	Field Added

webfilter logs:

Field	Change
contentencoding	Field Removed

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
22024	LOG_ID_IPPOOLPBA_INTERIM	Log ID Added
22070	LOG_ID_FORTIGSLB_COMMUNICATION_ERROR	Log ID Added
22071	LOG_ID_FORTIGSLB_CLOUD_CONFIG_UPDATED	Log ID Added
22224	LOG_ID_EXT_RESOURCE_OVERFLOW	Log ID Added
22750	LOG_ID_METERED_BILLING_ACCEPTED	Log ID Added
22751	LOG_ID_METERED_BILLING_FAIL	Log ID Added
22752	LOG_ID_METERED_BILLING_VALID	Log ID Added
22753	LOG_ID_METERED_BILLING_INVALID	Log ID Added
32618	LOG_ID_FGT_SWITCH_EXPORT_POOL_UNDO	Log ID Added
32619	LOG_ID_FGT_SWITCH_EXPORT_VDOM_UNDO	Log ID Added
32620	LOG_ID_FGT_SWITCH_GROUP_ADD_MEMBER	Log ID Added
32621	LOG_ID_FGT_SWITCH_GROUP_DEL_MEMBER	Log ID Added
32622	LOG_ID_FGT_SWITCH_FORTILINK_CONNECTED	Log ID Added
32623	LOG_ID_FGT_SWITCH_LOCATION_CHANGE	Log ID Added
32624	LOG_ID_FGT_SWITCH_NEW_PEER_DETECT	Log ID Added
43720	LOG_ID_EVENT_WIRELESS_FIPS	Log ID Added
43721	LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_EXT_MPSK_RESULT	Log ID Added
43778	LOG_ID_EVENT_NAC_QUARANTINE_EXPIRY	Log ID Added
53010	LOG_ID_INTERNAL_FDS_FTC	Log ID Added

virus logs:

Log ID	Message	Change
9241	LOG_ID_UNKNOWN_CE_BLOCK	Log ID Added
9242	LOG_ID_UNKNOWN_CE_BYPASS	Log ID Added

webfilter logs:

Log ID	Message	Change
13696	LOG_ID_UNKNOWN_CE_BLOCK	Log ID Removed
13697	LOG_ID_UNKNOWN_CE_BYPASS	Log ID Removed

FortiOS 7.4.3

There are no major log changes between FortiOS 7.4.2 and 7.4.3.

FortiOS 7.4.2

Log field values

The following log field values are changed:

casb logs:

Field	Change
dstuuid	Field Added
srcuuid	Field Added

dlp logs:

Field	Change
filteridx	Field Removed
filtername	Field Removed
ruleid	Field Added
rulename	Field Added

event logs:

Field	Change
switchaclid	Field Added
switchautoip	Field Added
switchinterface	Field Added
switchl2capacity	Field Added
switchl2count	Field Added
switchmirrorsession	Field Added
switchphysicalport	Field Added
switchsysteminterface	Field Added
switchtrunk	Field Added
switchtrunkinterface	Field Added
unit	Field Removed
vlan	Field Added

file-filter logs:

Field	Change
filtername	Field Removed
rulename	Field Added

icap logs:

Field	Change
reason	Field Added

traffic logs:

Field	Change
clientcert	Field Added
clientdeviceems	Field Added
durationdelta	Field Added
rcvdpktdelta	Field Added
sentpktdelta	Field Added

webfilter logs:

Field	Change
videodesc	Field Added
videotitle	Field Added

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
20139	LOG_ID_FGCS_ACC_LIC_EXPIRE	Log ID Added
20140	LOG_ID_FSPA_LIC_EXPIRE	Log ID Added
20141	LOG_ID_FSFG_LIC_EXPIRE	Log ID Added
22022	LOG_ID_ENTER_EXTREME_LOW_MEM_MODE	Log ID Added
22023	LOG_ID_LEAVE_EXTREME_LOW_MEM_MODE	Log ID Added
22104	LOG_ID_POWER_RESTORE	Log ID Removed
22817	LOG_ID_SCANUNIT_DLP_SIGNATURE_REMOVE	Log ID Added

Log ID	Message	Change
22874	LOG_ID_FLTUND_NEW_CONN	Log ID Added
22875	LOG_ID_FLTUND_CONN_DOWN	Log ID Added
22876	LOG_ID_FLTUND_RCV_BOOTSTRAP	Log ID Added
22877	LOG_ID_FLTUND_CONN_ONLINE	Log ID Added
22878	LOG_ID_FLTUND_CONN_OFFLINE	Log ID Added
34420	LOG_ID_NP6XLITE_HPE_PACKET_DROP	Log ID Added
34421	LOG_ID_NP6XLITE_HPE_PACKET_FLOOD	Log ID Added
45101	LOG_ID_EC_REG_SUCCEED	Log ID Added
45132	LOG_ID_EC_EMS_UPGRADE_FAIL	Log ID Added
45133	LOG_ID_EC_SHM_MISSING_QUERY	Log ID Added

ssl logs:

Log ID	Message	Change
62309	LOG_ID_SSL_ANOMALY_CERT_INVALID	Log ID Added

virtual-patch logs:

Log ID	Message	Change
64610	LOG_ID_LOCALIN_VPATCH_BLOCK	Log ID Added
64611	LOG_ID_LOCALIN_VPATCH_LOG	Log ID Added

virus logs:

Log ID	Message	Change
8982	MESGID_SCAN_AV_MAX_MEMORY_REACHED_ERROR	Log ID Added

webfilter logs:

Log ID	Message	Change
13617	LOG_ID_CONTENT_TYPE_EXEMPT	Log ID Added
13712	LOG_ID_VIDEOFILTER_TITLE_BLOCK	Log ID Added
13713	LOG_ID_VIDEOFILTER_TITLE_MONITOR	Log ID Added
13714	LOG_ID_VIDEOFILTER_TITLE_ALLOW	Log ID Added
13728	LOG_ID_VIDEOFILTER_DESCRIPTION_BLOCK	Log ID Added
13729	LOG_ID_VIDEOFILTER_DESCRIPTION_MONITOR	Log ID Added
13730	LOG_ID_VIDEOFILTER_DESCRIPTION_ALLOW	Log ID Added

FortiOS 7.4.1

Log type and subtype changes

The virtual-patch and casb log types are added.

Log field values

The following log field values are changed:

casb logs:

Field	Change
action	Field Added
activitycategory	Field Added
date	Field Added
devid	Field Added
dstintf	Field Added
dstintfrole	Field Added
dstip	Field Added
dstport	Field Added
eventtime	Field Added
eventtype	Field Added
group	Field Added
level	Field Added
logid	Field Added
msg	Field Added
policyid	Field Added
poluuid	Field Added
profile	Field Added
proto	Field Added
saasapp	Field Added
sessionid	Field Added
srcintf	Field Added
srcintfrole	Field Added

Field	Change
srcip	Field Added
srcport	Field Added
subtype	Field Added
time	Field Added
type	Field Added
tz	Field Added
url	Field Added
user	Field Added
useractivity	Field Added
vd	Field Added
vrf	Field Added

event logs:

Field	Change
connection_type	Field Removed
license_limit	Field Removed
snprev	Field Added
used_for_type	Field Removed

ssh logs:

Field	Change
poluuid	Field Added

traffic logs:

Field	Change
countcasb	Field Added
countvpatch	Field Added
replydstintf	Field Added
replysrcintf	Field Added

virtual-patch logs:

Field	Change
action	Field Added
agent	Field Added
attack	Field Added
attackcontext	Field Added
attackcontextid	Field Added
attackid	Field Added
authserver	Field Added
date	Field Added
devid	Field Added
direction	Field Added
dstauthserver	Field Added
dstcountry	Field Added
dstintf	Field Added
dstintfrole	Field Added
dstip	Field Added
dstport	Field Added
dstuser	Field Added
eventtime	Field Added
eventtype	Field Added
fctuid	Field Added
forwardedfor	Field Added
group	Field Added
hostname	Field Added
httpmethod	Field Added
level	Field Added
logid	Field Added
pdstport	Field Added
policyid	Field Added
policymode	Field Added
policytype	Field Added

Field	Change
poluuid	Field Added
profile	Field Added
proto	Field Added
psrcport	Field Added
rawdata	Field Added
rawdataid	Field Added
referralurl	Field Added
service	Field Added
sessionid	Field Added
severity	Field Added
srccountry	Field Added
srcdomain	Field Added
srcintf	Field Added
srcintfrole	Field Added
srcip	Field Added
srcport	Field Added
subtype	Field Added
time	Field Added
trueclntip	Field Added
type	Field Added
tz	Field Added
unauthuser	Field Added
unauthusersource	Field Added
url	Field Added
user	Field Added
vd	Field Added
vrf	Field Added

Log ID changes

The following log IDs are changed:

casb logs:

Log ID	Message	Change
10000	LOG_ID_CASB_ACCESS_BLOCKED	Log ID Added
10001	LOG_ID_CASB_ACCESS_BYPASS	Log ID Added
10002	LOG_ID_CASB_ACCESS_MONITOR	Log ID Added

event logs:

Log ID	Message	Change
20137	LOG_ID_FGSA_LIC_EXPIRE	Log ID Added
20138	LOG_ID_SWOS_LIC_EXPIRE	Log ID Added
20235	LOG_ID_SYS_SECURITY_MOUNT_VIOLATION	Log ID Added
22939	LOG_ID_EVENT_VWL_FAIL_DETECT	Log ID Added
22940	LOG_ID_EVENT_LINK_MONITOR_FAIL_DETECT	Log ID Added
32019	LOG_ID_CC_ENTER_ERR_MOD	Log ID Removed
32055	LOG_ID_CC_KAT_SUCCESS	Log ID Added
32264	LOG_ID_BLE_FIRMWARE_CHECK	Log ID Added
32265	LOG_ID_BLE_FIRMWARE_UPDATE	Log ID Added
45057	LOG_ID_FCC_ADD	Log ID Removed
45058	LOG_ID_FCC_CLOSE	Log ID Removed
45061	LOG_ID_FCC_CLOSE_BY_TYPE	Log ID Removed
46506	LOG_ID_INTERNAL_LTE_MODEM_BILLING_DAILY_LOG	Log ID Removed
46522	LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_ALERT	Log ID Added
46523	LOG_ID_INTERNAL_LTE_MODEM_BILLING_TIME_REFRESH	Log ID Added
46524	LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_DATA_PLAN	Log ID Added
46525	LOG_ID_INTERNAL_LTE_MODEM_BILLING_STOP_NETWORK	Log ID Added
46526	LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_PLAN_OVER	Log ID Added
53406	LOG_ID_2GB_CSF_UPGRADE	Log ID Added

ssl logs:

Log ID	Message	Change
62308	LOG_ID_SSL_ANOMALY_HANDSHAKE_FAILURE	Log ID Added

virtual-patch logs:

Log ID	Message	Change
64600	LOG_ID_VPATCH_BLOCK	Log ID Added
64601	LOG_ID_VPATCH_LOG	Log ID Added

FortiOS 7.4.0

Log field values

The following log field values are changed:

app-ctrl logs:

Field	Change
icmpcode	Field Added
icmpid	Field Added
icmptype	Field Added

event logs:

Field	Change
app	Field Added
apperror	Field Added
appid	Field Added
downbandwidthmeasured	Field Added
extension	Field Added
filename	Field Added
model	Field Added
networktransfertime	Field Added
product	Field Added
serveraddr	Field Added
servername	Field Added
serverresponsetime	Field Added
speedtestserver	Field Added
srccountry	Field Added
ticket	Field Added

Field	Change
timestamp	Field Added
upbandwidthmeasured	Field Added
vendor	Field Added
versionmax	Field Added
versionmin	Field Added
vulncnt	Field Added
vulnresult	Field Added

traffic logs:

Field	Change
fwdsrv	Field Added
realserverid	Field Added

virus logs:

Field	Change
fndraction	Field Removed
fndrconfidence	Field Removed
fndrfileid	Field Removed
fndrfiletype	Field Removed
fndrseverity	Field Removed
fndrverdict	Field Removed
fsaaction	Field Removed
fsafileid	Field Removed
fsafiletype	Field Removed
fsaseverity	Field Removed
icbaction	Field Added
icbconfidence	Field Added
icbfileid	Field Added
icbfiletype	Field Added
icbseverity	Field Added
icbverdict	Field Added

voip logs:

Field	Change
logsrc	Field Added

Log ID changes

The following log IDs are changed:

event logs:

Log ID	Message	Change
20136	LOG_ID_DLP_LIC_EXPIRE	Log ID Added
20150	LOG_ID_DEV_VUNL_FTGD_LOOKUP	Log ID Added
20230	LOG_ID_SYS_SECURITY_WRITE_VIOLATION	Log ID Added
20231	LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION	Log ID Added
20232	LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION	Log ID Added
20233	LOG_ID_SYS_SECURITY_FILE_HASH_MISSING	Log ID Added
20234	LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH	Log ID Added
22094	LOG_ID_FEDERATED_UPGRADE_ROOT_COMPLETED	Log ID Added
22095	LOG_ID_FEDERATED_UPGRADE_ROOT_NOT_COMPLETED	Log ID Added
22111	LOG_ID_PSU_ACTION_FPC_DOWN	Log ID Added
22112	LOG_ID_PSU_ACTION_FPC_UP	Log ID Added
22937	LOG_ID_EVENT_VWL_APP_PERF_METRICS	Log ID Added
22938	LOG_ID_EVENT_VWL_WAN_SPEEDTEST_RESULT	Log ID Added
32270	LOG_ID_SSH_HOST_KEY_REGEN	Log ID Added
35051	LOG_ID_PCP_MAPPING_CREATE	Log ID Added
35052	LOG_ID_PCP_MAPPING_DELETE	Log ID Added
35053	LOG_ID_PCP_MAPPING_RENEW	Log ID Added
40961	LOGID_EVENT_ICAP_REMOTE_SRV_STAT	Log ID Added
41011	LOG_ID_UPD_DB_UNSIGNED_INSTALLED	Log ID Added
42201	LOG_ID_NETX_VMX_ATTACH	Log ID Removed
42202	LOG_ID_NETX_VMX_DETACH	Log ID Removed
42203	LOG_ID_NETX_VMX_DENIED	Log ID Removed
46518	LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH	Log ID Added
46519	LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_CONNECTION_STATE	Log ID Added

Log ID	Message	Change
46520	LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_LINK_MONITOR	Log ID Added
46521	LOG_ID_INTERNAL_LTE_MODEM_SIM_FLIP	Log ID Added
53100	LOG_ID_VPN_OCVPN_REGISTERED	Log ID Removed
53101	LOG_ID_VPN_OCVPN_UNREGISTERED	Log ID Removed
53102	LOG_ID_VPN_OCVPN_COMM_ESTABLISHED	Log ID Removed
53103	LOG_ID_VPN_OCVPN_COMM_ERROR	Log ID Removed
53104	LOG_ID_VPN_OCVPN_DNS_ERROR	Log ID Removed
53105	LOG_ID_VPN_OCVPN_ROUTE_ERROR	Log ID Removed
53320	LOG_ID_FORTICONVERTER_RESULT_READY	Log ID Added
53321	LOG_ID_FORTICONVERTER_CONFIG_UPLOADED	Log ID Added

virus logs:

Log ID	Message	Change
8232	MESGID_ICB_FSA_WARNING	Log ID Removed
8233	MESGID_ICB_FSA_NOTIF	Log ID Removed
8234	MESGID_MIME_ICB_FSA_WARNING	Log ID Removed
8235	MESGID_MIME_ICB_FSA_NOTIF	Log ID Removed
8236	MESGID_ICB_FSA_TIMEOUT_WARNING	Log ID Removed
8237	MESGID_ICB_FSA_TIMEOUT_NOTIF	Log ID Removed
8238	MESGID_MIME_ICB_FSA_TIMEOUT_WARNING	Log ID Removed
8239	MESGID_MIME_ICB_FSA_TIMEOUT_NOTIF	Log ID Removed
8240	MESGID_ICB_FSA_ERROR_WARNING	Log ID Removed
8241	MESGID_ICB_FSA_ERROR_NOTIF	Log ID Removed
8242	MESGID_MIME_ICB_FSA_ERROR_WARNING	Log ID Removed
8243	MESGID_MIME_ICB_FSA_ERROR_NOTIF	Log ID Removed

Log types and subtypes

This section describes the log types, subtypes, and priority levels. It also describes the log field format.

Type

Each log entry contains a Type (type) or category field that indicates its log type and which log file stores the log entry.

Subtype

Each log entry contains a Sub Type (subtype) or subcategory field within a log type, based on the feature associated with the cause of the log entry.

For example:

- In event logs, some of the subtypes are compliance check, system, and user.
- In traffic logs, the subtypes are forward, local, multicast, and sniffer.

List of log types and subtypes

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

Type	Description	Subtype
traffic	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.	• forward • local • multicast • sniffer • ztna
event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	• cifs-auth-fail • connector • endpoint • fortiextender • ha

Type	Description	Subtype
		- rest-api - router - sdwan - security-rating - switch-controller - system - user - vpn - wanopt - webproxy - wireless
UTM	Records UTM events.	See list of UTM log subtypes below

UTM log subtypes

UTM Log Subtypes	Description	Event Type
virus	Records virus attacks.	- analytics - command-blocked - content-disarm - ems-threat-feed - exempt-hash - filename - filetype-executable - infected - inline-block - malware-list - mimefragmented - outbreak-prevention - oversize - scanerror - unknown - unknown
webfilter	Records web filter events.	- activexfilter - antiphishing - appletfilter - content - cookiefilter

UTM Log Subtypes	Description	Event Type
		• ftgd_allow • ftgd_blk • ftgd_err • ftgd_quota • ftgd_quota_counting • ftgd_quota_expired • http_header_change • scriptfilter • ssl-exempt • urlfilter • urlmonitor • videofilter-category • videofilter-channel • videofilter-description • videofilter-title • webfilter_command_block
ips	Records intrusion prevention events.	• botnet • malicious-url • signature
emailfilter	Records email filter events.	• bannedword • email • ftgd_err • spam • webmail
anomaly	Records intrusion attempts.	• anomaly
voip	Records voice over IP events.	• voip
dlp	Records data loss prevention events.	• dlp • dlp-docsource
app-ctrl	Records intrusion attempts. Application control log is output when a signature matches an application pattern.	• port-violation • protocol-violation • signature
waf	Records web application firewall information for FortiWeb appliances and virtual appliances.	• waf-address-list • waf-custom-signature • waf-http-constraint • waf-http-method • waf-signature • waf-url-access

UTM Log Subtypes	Description	Event Type
gtp	Records GTP events.	• gtp-all • pfcp-all
dns	Records domain name server events.	• dns-query • dns-response
ssh	Records Secure Socket Shell events.	• ssh-channel • ssh-command • ssh-hostkey • ssh-unsupport-proto
ssl	Records detected/blocked malicious SSL connections.	• ssl-anomaly • ssl-exempt • ssl-handshake • ssl-negotiation • ssl-server-cert-info
file-filter	Records file filter events.	• file-filter
icap	Records ICAP events.	• icap
forti-switch	Records FortiSwitch events.	• fsw-flow
virtual-patch	Records virtual-patch events.	• localin-vpatch • ot-vpatch
casb	Records CASB events.	• casb

FortiOS priority levels

Each log entry contains a Level (level) field that indicates the estimated severity of the event that caused the log entry, such as `level=warning`, and therefore how high a priority it is likely to be. Level (level) 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 (logid), not by Level (level).

Level (0 is highest)	Name	Description
0	Emergency	The system is unusable or not responding.
1	Alert	Immediate action required. Used in security logs.
2	Critical	Functionality is affected.
3	Error	An error exists and functionality could be affected.

Level (0 is highest)	Name	Description
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations. Used in event logs to record configuration changes.

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

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 subtypes follow this generic table format to present the log entry information.

Log Field Name	Description	Data Type	Length
appact	The security action from app control	string	16

Log schema structure

This section describes the schema of the FortiOS log messages.

Log message fields

Each log message consists of several sections of fields. In the FortiOS GUI, you can view the logs in the *Log & Report* pane, which displays the formatted view. If you want to view logs in raw format, you must download the log and view it in a text editor.

Following is an example of a traffic log message in raw format:

```
date=2017-11-15 time=11:44:16 logid="0000000013" type="traffic" subtype="forward" level="notice"
      vd="vdom1" eventtime=1510775056 srcip=10.1.100.155 srcname="pc1" srcport=40772
      srcintf="port12" srcintfrole="undefined" dstip=35.197.51.42 dstname="fortiguard.com"
      dstport=443 dstintf="port11" dstintfrole="undefined" poluuid="707a0d88-c972-51e7-bbc7-
      4d421660557b" sessionid=8058 proto=6 action="close" policyid=1 policytype="policy"
      policymode="learn" service="HTTPS" dstcountry="United States" srccountry="Reserved"
      trandisp="snat" transip=172.16.200.2 transport=40772 appid=40568 app="HTTPS.BROWSER"
      appcat="Web.Client" apprisk="medium" duration=2 sentbyte=1850 rcvdbyte=39898 sentpkt=25
      rcvdpkt=37 utmaction="allow" countapp=1 devtype="Linux PC" osname="Linux"
      mastersrcmac="a2:e9:00:ec:40:01" srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=0-220586
```

The following table provides an example of the log field information in the FortiOS GUI in the detailed view of the *Log & Report* pane and in the downloaded, raw log file.

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
General		
Date (date)	Day, month, and year when the log message was recorded.	`date=2017-11-15`
Direction (direction)	Indicates message/packets direction.	`direction=incoming`
Time (time)	Hour clock when the log message was recorded.	`time=11:44:16`
Duration (seconds)	Duration of the session, in seconds.	`duration=2`
Session ID (sessionid)	ID for the session.	`sessionid=8058`
Virtual Domain (vd)	Name of the virtual domain in which the log message was recorded.	`vd="vdom1"`

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
NAT Translation (transport)	NAT source port.	`transport=40772`
Source		
IP (srcip)	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=10.1.100.155`
NAT IP (transip)	NAT source IP.	`transip=172.16.200.2`
Source Port (srcport)	Port number of the traffic's origin.	`srcport=40772`
Country (srccountry)	Name of the source country.	`srccountry="Reserved"`
Source Interface (srcintf)	Interface name of the traffic's origin.	`srcintf="port12"`
Source Name (srcname)	Name of the source.	`srcname="pc1"`
Source Interface Name (srcintfrole)	Name of the source interface.	`srcintfrole="undefined"`
Device Type (devtype)	Device type of the source.	`devtype="Linux PC"`
OS Name (osname)	OS of the source.	`osname="Linux"`
Master Source MAC (mastersrcmac)	The master MAC address for a host that has multiple network interfaces.	`mastersrcmac="a2:e9:00:ec:40:01"`
Source MAC (srcmac)	MAC address associated with the source IP address.	`srcmac="a2:e9:00:ec:40:01"`
Source Server (srcserver)	Server of the source.	`srcserver=0`
Device ID (devid)	Serial number of the device for the traffic's origin.	`devid="FGVM02Q105060010"`
Destination		
IP (dstip)	Destination IP address for the web.	`dstip=35.197.51.42`
Port (dstport)	Port number of the traffic's destination.	`dstport=443`
Country (dstcountry)	Name of the destination country.	`dstcountry="United States"`

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
Destination Interface (dstintf)	Interface of the traffic's destination.	`dstintf="port11"`
Destination Name (dstname)	Name of the destination.	`dstname="fortiguard.com"`
Destination Interface Name (dstinfrole)	Name of the destination interface.	`dstintfrole="undefined"`
Application		
Application Name (app)	Name of the application.	`app="HTTPS.BROWSER"`
Category (appcat)	Category of the application.	`appcat="Web.Client"`
Service (service)	Name of the service.	`service="HTTPS"`
Application ID (appid)	ID of the application.	`appid=40568`
Application Risk (apprisk)	Risk level of the application.	`apprisk="medium"`
countapp	Number of App Ctrl logs associated with the session.	`countapp=1`
Data		
Received bytes (rcvdbyte)	Number of bytes received.	`rcvdbyte=39898`
Received packets (rcvdpkt)	Number of packets received.	`rcvdpkt=37`
Sent bytes (sentbyte)	Number of bytes sent.	`sentbyte=1850`
Sent packets (sentpkt)	Number of packets sent.	`sentpkt=25`
Action		
Action (action)	Status of the session. Uses following definitions: • 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.	`action=close`

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
Policy (policyid)	Name of the firewall policy governing the traffic which caused the log message.	`policyid=1`
Policy UUID (poluuid)	UUID for the firewall policy.	`poluuid="707a0d88-c972-51e7-bbc7-4d421660557b"`
Policy Type (policytype)		`policytype="policy"`
Policy Mode (policymode)	Firewall policy mode.	`policymode="learn"`
Security		
Level (level)	Security level rating.	`level="notice"`
Other		
Event Time (eventtime)	Epoch time the log was triggered by FortiGate. If you convert the epoch time to human readable time, it might not match the Date and Time in the header owing to a small delay between the time the log was triggered and recorded. The Log Time field is the same for the same log among all log devices, but the Date and Time might differ.	`eventtime=1510775056`
Protocol Number (proto)	tcp: The protocol used by web traffic (tcp by default)	`proto=6`
Type (type)	Log type. See Type on page 51	`type="traffic"`
Log ID (logid)	Log ID. See Log ID definitions on page 60	`logid="0000000013"`
Sub Type(subtype)	Subtype of the traffic. See Subtype on page 51.	`subtype="forward"`
trandisp	NAT translation type.	`trandisp="snat"`
UTM Action (utmaction)	Security action performed by UTM.	`utmaction="allow"`
UTM Reference (utmref)	UTM reference number.	`utmref=0-220586`
UTM Reference (utmref)	UTM reference number.	`utmref=0-220586`

Log ID numbers

The ID (logid) is a 10-digit field. 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 logid 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 logid.

Log ID definitions

Following are the definitions for the log type IDs and subtype IDs applicable to FortiOS:

Log Category IDs	Subtype IDs
traffic: 0	• forward: 0 • local: 1 • multicast: 2 • sniffer: 4 • ztna: 5
event: 1	• system: 0 • vpn: 1 • user: 2 • router: 3 • wireless: 4 • wanopt: 5 • endpoint: 7

Log Category IDs	Subtype IDs
	- ha: 8 - security-rating: 10 - fortiextender: 11 - connector: 12 - sdwan: 13 - cifs-auth-fail: 14 - switch-controller: 15 - rest-api: 16 - webproxy: 17
virus: 2	- analytics: 1 - exempt-hash: 2 - filetype-executable: 3 - outbreak-prevention: 4 - content-disarm: 5 - command-blocked: 6 - malware-list: 7 - ems-threat-feed: 8 - inline-block: 9 - infected: 11 - filename: 12 - oversize: 13 - unknown: 49 - mimefragmented: 61 - scanerror: 62 - unknown: 63
webfilter: 3	- content: 14 - urlfilter: 15 - ftgd_blk: 16 - ftgd_allow: 17 - ftgd_err: 18 - urlmonitor: 19 - activexfilter: 35 - cookiefilter: 36 - appletfilter: 37 - ftgd_quota_counting: 38 - ftgd_quota_expired: 39 - ftgd_quota: 40 - scriptfilter: 41 - webfilter_command_block: 43

Log Category IDs	Subtype IDs
	• http_header_change: 44 • ssl-exempt: 45 • antiphishing: 46 • videofilter-category: 47 • videofilter-channel: 48 • videofilter-title: 50 • videofilter-description: 51
ips: 4	• signature: 19 • malicious-url: 21 • botnet: 22
emailfilter: 5	• email: 12 • spam: 13 • bannedword: 14 • webmail: 20 • ftgd_err: 53
anomaly: 7	• anomaly: 20
voip: 8	• voip: 14
dlp: 9	• dlp: 54 • dlp-docsource: 55
app-ctrl: 10	• signature: 59 • port-violation: 60 • protocol-violation: 61
waf: 12	• waf-signature: 0 • waf-custom-signature: 1 • waf-http-method: 2 • waf-http-constraint: 3 • waf-address-list: 4 • waf-url-access: 5
gtp: 14	• gtp-all: 0 • pfcp-all: 1
dns: 15	• dns-query: 0 • dns-response: 1
ssh: 16	• ssh-command: 0 • ssh-channel: 1 • ssh-hostkey: 2 • ssh-unsupport-proto: 3

Log Category IDs	Subtype IDs
ssl: 17	• ssl-anomaly: 0 • ssl-exempt: 1 • ssl-negotiation: 2 • ssl-server-cert-info: 3 • ssl-handshake: 4
file-filter: 19	• file-filter: 0
icap: 20	• icap: 0
forti-switch: 23	• fsw-flow: 0
virtual-patch: 24	• ot-vpatch: 0 • localin-vpatch: 1
casb: 25	• casb: 0

FortiGuard web filter categories

The below details the mapping between FortiGuard Web Filter category names and numbers.

Number	Category
0	Unrated
1	Drug abuse
2	Alternative beliefs
3	Hacking
4	Illegal or unethical
5	Discrimination
6	Explicit violence
7	Abortion
8	Other adult materials
9	Advocacy organizations
11	Gambling
12	Extremist groups
13	Nudity and risque
14	Pornography
15	Dating
16	Weapons (sales)
17	Advertising
18	Brokerage and trading
19	Freeware and software downloads
20	Games
23	Web-based email
24	File sharing and storage
25	Streaming media and download
26	Malicious websites
28	Entertainment
29	Arts and culture
30	Education

Number	Category
31	Finance and banking
33	Health and wellness
34	Job search
35	Medicine
36	News and media
37	Social networking
38	Political organizations
39	Reference
40	Global religion
41	Search engines and portals
42	Shopping
43	General organizations
44	Society and lifestyles
46	Sports
47	Travel
48	Personal vehicles
49	Business
50	Information and computer security
51	Government and legal organizations
52	Information technology
53	Armed forces
54	Dynamic content
55	Meaningless content
56	Web hosting
57	Marijuana
58	Folklore
59	Proxy avoidance
61	Phishing
62	Plagiarism
63	Sex education

Number	Category
64	Alcohol
65	Tobacco
66	Lingerie and swimsuit
67	Sports hunting and war games
68	Web chat
69	Instant messaging
70	Newsgroups and message boards
71	Digital postcards
72	Peer-to-peer file sharing
75	Internet radio and TV
76	Internet telephony
77	Child education
78	Real estate
79	Restaurant and dining
80	Personal websites and blogs
81	Secure websites
82	Content servers
83	Child abuse
84	Web-based applications
85	Domain parking
86	Spam URLs
87	Personal privacy
88	Dynamic DNS
89	Auction
90	Newly observed domain
91	Newly registered domain
92	Charitable organizations
93	Remote access
94	Web analytics
95	Online meeting

Number	Category
96	Terrorism
97	URL Shortening
98	Crypto Mining
99	Potentially Unwanted Program
100	Artificial Intelligence Technology
101	Cryptocurrency
140	custom1
141	custom2

CEF support

You can configure FortiOS 7.4.9 to send logs to remote syslog servers in Common Event Format (CEF) by using the `config log syslogd setting` command.

When CEF is enabled, FortiOS sends logs to syslog servers in CEF. This section describes how FortiOS logs support CEF.

You can view logs in CEF on remote syslog servers or FortiAnalyzer, but not in the FortiOS GUI.

FortiOS to CEF log field mapping guidelines

The following CEF format:

```
Date/Time host CEF:Version|Device Vendor|Device Product|Device Version|Signature
      ID|Name|Severity|[Extension]
```

Displays as following in FortiOS logs with CEF enabled:

```
"MMM dd HH:mm:ss" "hostname of the fortigate" CEF:0|Fortinet|Fortigate|version|logid|type:subtype
      +[eventtype] +[action] +[status]|reversed level|...
```

The `SignatureId` field in FortiOS logs maps to the `logid` field in CEF and should be last 5 digits of `logid`.

The `Name` field in CEF uses the following formula:

```
type:subtype + [eventtype] + [action] + [status]
```

Following is an example of the header and one key-value pair for extension from the Event VPN log in CEF:

```
#Feb 12 10:31:04 syslog-800c CEF:0|Fortinet|Fortigate|v5.6.0|37127|event:vpn negotiate
      success|3|FTNTFGTlogid=0101037127
```

The `type:subtype` field in FortiOS logs maps to the `cat` field in CEF.

Any fields in FortiOS logs that are unmatched to fields in CEF include the `FTNTFGT` prefix.

Quotes ("") are removed from FortiOS logs to support CEF.

Forward slashes (//) in string values as well as the equal sign (=) and backward slashes (\) are escaped in FortiOS logs to support CEF.

CEF priority levels

Following are the CEF priority levels. They are opposite of FortiOS priority levels. See also FortiOS priority levels on page 54.

Level (8 is highest)	Name	Description
8	Emergency	The system is unusable or not responding.
7	Alert	Immediate action required. Used in security logs.
6	Critical	Functionality is affected.
5	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
3	Notification	Information about normal events.
2	Information	General information about system operations. Used in event logs to record configuration changes.
1	Debug	Debug information.

Examples of CEF support

This section includes examples of how the different types of log message support CEF.

Traffic log support for CEF

The following is an example of a traffic log on the FortiGate disk:

```
date=2018-12-27 time=11:07:55 logid="0000000013" type="traffic" subtype="forward" level="notice"
     vd="vdom1" eventtime=1545937675 srcip=10.1.100.11 srcport=54190 srcintf="port12"
     srcintfrole="undefined" dstip=52.53.140.235 dstport=443 dstintf="port11"
     dstintfrole="undefined" poluuid="c2d460aa-fe6f-51e8-9505-41b5117dfdd4" sessionid=402 proto=6
     action="close" policyid=1 policytype="policy" service="HTTPS" dstcountry="United States"
     srccountry="Reserved" trandisp="snat" transip=172.16.200.1 transport=54190 appid=40568
     app="HTTPS.BROWSER" appcat="Web.Client" apprisk="medium" applist="g-default" duration=2
     sentbyte=3652 rcvdbyte=146668 sentpkt=58 rcvdpkt=105 utmaction="allow" countapp=2
     utmref=65532-56
```

The following is an example of a traffic log sent in CEF format to a syslog server:

```
Dec 27 11:07:55 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|00013|traffic:forward
      close|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0000000013 cat=traffic:forward
      FTNTFGTsubtype=forward FTNTFGTlevel=notice FTNTFGTvd=vdom1 FTNTFGTeventtime=1545937675
      src=10.1.100.11 spt=54190 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined
      dst=52.53.140.235 dpt=443 deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined
      FTNTFGTpoluuid=c2d460aa-fe6f-51e8-9505-41b5117dfdd4 externalId=402 proto=6 act=close
      FTNTFGTpolicyid=1 FTNTFGTpolicytype=policy app=HTTPS FTNTFGTdstcountry=United States
      FTNTFGTsrccountry=Reserved FTNTFGTtrandisp=snat sourceTranslatedAddress=172.16.200.1
      sourceTranslatedPort=54190 FTNTFGTappid=40568 FTNTFGTapp=HTTPS.BROWSER
      FTNTFGTappcat=Web.Client FTNTFGTapprisk=medium FTNTFGTapplist=g-default FTNTFGTduration=2
      out=3652 in=146668 FTNTFGTsentpkt=58 FTNTFGTrcvdpkt=105 FTNTFGTutmaction=allow
      FTNTFGTcountapp=2
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
type: subtype	cat
srcip	src
srcport	spt
srcintf	deviceInboundInterface
dstip	dst
dstport	dpt
dstintf	deviceOutboundInterface
sessionid	externalID
proto	proto
action	act
transip	sourceTranslatedAddress
transport	sourceTranslatedPort
service	app
sentbyte	out
rcvdbyte	in

Custom fields

To configure the traffic log with custom fields, enter the following CLI commands:

```
config log custom-field
   edit 1
      set name "custom_name1"
      set value "HN123456"
   next
   edit 2
      set name "custom_name2"
      set value "accounting_dpt"
   next
   end
   config firewall policy
      edit 1
         set name "A-v4-out"
         set srcintf "port12"
         set dstintf "port11"
         set srcaddr "all"
         set dstaddr "all"
         set action accept
         set schedule "always"
         set service "ALL"
         set utm-status enable
         set logtraffic all
         set custom-log-fields "1" "2"
         set application-list "g-default"
         set ssl-ssh-profile "certificate-inspection"
         set nat enable
      next
   end
```

The following is an example of a traffic log with custom fields on the FortiGate disk:

```
date=2018-12-27 time=11:12:30 logid="0000000013" type="traffic" subtype="forward" level="notice"
      vd="vdom1" eventtime=1545937950 srcip=10.1.100.11 srcport=58843 srcintf="port12"
      srcintfrole="undefined" dstip=172.16.200.55 dstport=53 dstintf="port11"
      dstintfrole="undefined" poluuid="c2d460aa-fe6f-51e8-9505-41b5117dfdd4" sessionid=440
      proto=17 action="accept" policyid=1 policytype="policy" service="DNS" dstcountry="Reserved"
      srccountry="Reserved" trandisp="snat" transip=172.16.200.1 transport=58843 appid=16195
      app="DNS" appcat="Network.Service" apprisk="elevated" applist="g-default" duration=180
      sentbyte=70 rcvdbyte=528 sentpkt=1 rcvdpkt=1 custom_name1="HN123456" custom_
      name2="accounting_dpt"
```

The following is an example of a traffic log with custom fields sent in CEF format to a syslog server:

```
Dec 27 11:12:30 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|00013|traffic:forward
      accept|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0000000013 cat=traffic:forward
      FTNTFGTsubtype=forward FTNTFGTlevel=notice FTNTFGTvd=vdom1 FTNTFGTeventtime=1545937950
      src=10.1.100.11 spt=58843 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined
      dst=172.16.200.55 dpt=53 deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined
      FTNTFGTpoluuid=c2d460aa-fe6f-51e8-9505-41b5117dfdd4 externalId=440 proto=17 act=accept
      FTNTFGTpolicyid=1 FTNTFGTpolicytype=policy app=DNS FTNTFGTdstcountry=Reserved
      FTNTFGTsrccountry=Reserved FTNTFGTtrandisp=snat sourceTranslatedAddress=172.16.200.1
      sourceTranslatedPort=58843 FTNTFGTappid=16195 FTNTFGTapp=DNS FTNTFGTappcat=Network.Service
      FTNTFGTapprisk=elevated FTNTFGTapplist=g-default FTNTFGTduration=180 out=70 in=528
      FTNTFGTsentpkt=1 FTNTFGTrcvdpkt=1 FTNTFGTcustom_name1=HN123456 FTNTFGTcustom_
      name2=accounting_dpt
```

The following table maps FortiOS custom log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
custom_name1	FTNTFGTcustom_name1
custom_name2	FTNTFGTcustom_name2

Event log support for CEF

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
msg	msg
cookies	requestCookies
user	duser
status	outcome
role	sourceServiceName
ui	sproc
reason	reason
action	act

system subtype

The following is an example of a system subtype event log on the FortiGate disk:

```
date=2018-12-27 time=11:15:40 logid="0100032002" type="event" subtype="system" level="alert"
      vd="vdom1" eventtime=1545938140 logdesc="Admin login failed" sn="0" user="admin1" ui="https
      (172.16.200.254)" method="https" srcip=172.16.200.254 dstip=172.16.200.1 action="login"
      status="failed" reason="name_invalid" msg="Administrator admin1 login failed from https
      (172.16.200.254) because of invalid user name"
```

The following is an example of a system subtype event log sent in CEF format to a syslog server:

```
Dec 27 11:15:40 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|32002|event:system login
      failed|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0100032002 cat=event:system
      FTNTFGTsubtype=system FTNTFGTlevel=alert FTNTFGTvd=vdom1 FTNTFGTeventtime=1545938140
      FTNTFGTlogdesc=Admin login failed FTNTFGTsn=0 duser=admin1 sproc=https(172.16.200.254)
      FTNTFGTmethod=https src=172.16.200.254 dst=172.16.200.1 act=login outcome=failed
      reason=name_invalid msg=Administrator admin1 login failed from https(172.16.200.254) because
      of invalid user name
```

user subtype

The following is an example of a user subtype log on the FortiGate disk:

```
date=2018-12-27 time=11:17:35 logid="0102043008" type="event" subtype="user" level="notice"
      vd="vdom1" eventtime=1545938255 logdesc="Authentication success" srcip=10.1.100.11
      dstip=172.16.200.55 policyid=1 interface="port12" user="bob" group="N/A" authproto="TELNET
      (10.1.100.11)" action="authentication" status="success" reason="N/A" msg="User bob succeeded
      in authentication"
```

The following is an example of a user subtype log sent in CEF format to a syslog server:

```
Dec 27 11:17:35 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|43008|event:user authentication
      success|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0102043008 cat=event:user
      FTNTFGTsubtype=user FTNTFGTlevel=notice FTNTFGTvd=vdom1 FTNTFGTeventtime=1545938255
      FTNTFGTlogdesc=Authentication success src=10.1.100.11 dst=172.16.200.55 FTNTFGTpolicyid=1
      deviceInboundInterface=port12 duser=bob FTNTFGTgroup=N/A FTNTFGTauthproto=TELNET
      (10.1.100.11) act=authentication outcome=success reason=N/A msg=User bob succeeded in
      authentication
```

Antivirus log support for CEF

The following is an example of an antivirus log on the FortiGate disk:

```
date=2018-12-27 time=11:20:49 logid="0211008192" type="utm" subtype="virus" eventtype="infected"
      level="warning" vd="vdom1" eventtime=1545938448 msg="File is infected." action="blocked"
      service="HTTP" sessionid=695 srcip=10.1.100.11 dstip=172.16.200.55 srcport=44356 dstport=80
      srcintf="port12" srcintfrole="undefined" dstintf="port11" dstintfrole="undefined" policyid=1
      proto=6 direction="incoming" filename="eicar.com" quarskip="File-was-not-quarantined."
      virus="EICAR_TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
      virusid=2172 url="http://172.16.200.55/virus/eicar.com" profile="g-default" user="bob"
      agent="curl/7.47.0"
      analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f"
      analyticssubmit="false" crscore=50 crlevel="critical"
```

The following is an example of an antivirus log sent in CEF format to a syslog server:

```
Dec 27 11:20:48 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|08192|utm:virus infected
      blocked|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0211008192 cat=utm:virus
      FTNTFGTsubtype=virus FTNTFGTeventtype=infected FTNTFGTlevel=warning FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545938448 msg=File is infected. act=blocked app=HTTP externalId=695
      src=10.1.100.11 dst=172.16.200.55 spt=44356 dpt=80 deviceInboundInterface=port12
      FTNTFGTsrcintfrole=undefined deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined
      FTNTFGTpolicyid=1 proto=6 deviceDirection=0 fname=eicar.com FTNTFGTquarskip=File-was-not-
      quarantined. FTNTFGTvirus=EICAR_TEST_FILE FTNTFGTdtype=Virus
      FTNTFGTref=http://www.fortinet.com/ve?vn\=EICAR_TEST_FILE FTNTFGTvirusid=2172
      request=http://172.16.200.55/virus/eicar.com FTNTFGTprofile=g-default duser=bob
      requestClientApplication=curl/7.47.0
      FTNTFGTanalyticscksum=275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
      FTNTFGTanalyticssubmit=false FTNTFGTcrscore=50 FTNTFGTcrlevel=critical
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
direction	deviceDirection (inbound/outbound mapping to 0/1)
filename	fname
ref	FTNTFGTref (There is \ added to escape =)
url	request
agent	requestClientApplication

Webfilter log support for CEF

The following is an example of a webfilter log on the FortiGate disk:

```
date=2018-12-27 time=11:23:50 logid="0316013056" type="utm" subtype="webfilter" eventtype="ftgd_
      blk" level="warning" vd="vdom1" eventtime=1545938629 policyid=1 sessionid=764 user="bob"
      srcip=10.1.100.11 srcport=59194 srcintf="port12" srcintfrole="undefined"
      dstip=185.230.61.185 dstport=80 dstintf="port11" dstintfrole="undefined" proto=6
      service="HTTP" hostname="ambrishsriv.wixsite.com" profile="g-default" action="blocked"
      reqtype="direct" url="/bizsquads" sentbyte=96 rcvdbyte=0 direction="outgoing" msg="URL
      belongs to a denied category in policy" method="domain" cat=26 catdesc="Malicious Websites"
      crscore=60 crlevel="high"
```

The following is an example of a webfilter log sent in CEF format to a syslog server:

```
Dec 27 11:23:49 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|13056|utm:webfilter ftgd_blk
      blocked|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0316013056 cat=utm:webfilter
      FTNTFGTsubtype=webfilter FTNTFGTeventtype=ftgd_blk FTNTFGTlevel=warning FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545938629 FTNTFGTpolicyid=1 externalId=764 duser=bob src=10.1.100.11
      spt=59194 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined dst=185.230.61.185
      dpt=80 deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=HTTP
      dhost=ambrishsriv.wixsite.com FTNTFGTprofile=g-default act=blocked FTNTFGTreqtype=direct
      request=/bizsquads out=96 in=0 deviceDirection=1 msg=URL belongs to a denied category in
      policy FTNTFGTmethod=domain FTNTFGTcat=26 requestContext=Malicious Websites
      FTNTFGTcrscore=60 FTNTFGTcrlevel=high
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
hostname	dhost
catdesc	requestContext

IPS log support for CEF

The following is an example of an IPS log on the FortiGate disk:

```
date=2018-12-27 time=11:28:07 logid="0419016384" type="utm" subtype="ips" eventtype="signature"
      level="alert" vd="vdom1" eventtime=1545938887 severity="info" srcip=172.16.200.55
      srccountry="Reserved" dstip=10.1.100.11 srcintf="port11" srcintfrole="undefined"
      dstintf="port12" dstintfrole="undefined" sessionid=901 action="reset" proto=6 service="HTTP"
      policyid=1 attack="Eicar.Virus.Test.File" srcport=80 dstport=44362 hostname="172.16.200.55"
      url="/virus/eicar.com" direction="incoming" attackid=29844 profile="test-ips"
      ref="http://www.fortinet.com/ids/VID29844" user="bob" incidentserialno=877326946 msg="file_
      transfer: Eicar.Virus.Test.File,"
```

The following is an example of an IPS sent in CEF format to a syslog server:

```
Dec 27 11:28:07 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|16384|utm:ips signature
      reset|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0419016384 cat=utm:ips
      FTNTFGTsubtype=ips FTNTFGTeventtype=signature FTNTFGTlevel=alert FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545938887 FTNTFGTseverity=info src=172.16.200.55
      FTNTFGTsrccountry=Reserved dst=10.1.100.11 deviceInboundInterface=port11
      FTNTFGTsrcintfrole=undefined deviceOutboundInterface=port12 FTNTFGTdstintfrole=undefined
      externalId=901 act=reset proto=6 app=HTTP FTNTFGTpolicyid=1
      FTNTFGTattack=Eicar.Virus.Test.File spt=80 dpt=44362 dhost=172.16.200.55
      request=/virus/eicar.com deviceDirection=0 FTNTFGTattackid=29844 FTNTFGTprofile=test-ips
      FTNTFGTref=http://www.fortinet.com/ids/VID29844 duser=bob FTNTFGTincidentserialno=877326946
      msg=file_transfer: Eicar.Virus.Test.File,
```

Email Spamfilter log support for CEF

The following is an example of an email spamfilter log on the FortiGate disk:

```
date=2018-12-27 time=11:36:58 logid="0508020503" type="utm" subtype="emailfilter"
      eventtype="smtp" level="information" vd="vdom1" eventtime=1545939418 policyid=1
      sessionid=1135 user="bob" srcip=10.1.100.11 srcport=35969 srcintf="port12"
      srcintfrole="undefined" dstip=172.18.62.158 dstport=25 dstintf="port11"
      dstintfrole="undefined" proto=6 service="SMTP" profile="test-spam" action="log-only"
      from="testpc1@qa.fortinet.com" to="test1@server88.qa.fortinet.com"
      sender="testpc1@qa.fortinet.com" recipient="test1@server88.qa.fortinet.com"
      direction="outgoing" msg="general email log" subject="hello_world2" size="216"
      attachment="no"
```

The following is an example of an email spamfilter log sent in CEF format to a syslog server:

```
Dec 27 11:36:58 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|20503|utm:emailfilter smtp log-
      only|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0508020503 cat=utm:emailfilter
      FTNTFGTsubtype=emailfilter FTNTFGTeventtype=smtp FTNTFGTlevel=information FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545939418 FTNTFGTpolicyid=1 externalId=1135 duser=bob src=10.1.100.11
      spt=35969 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined dst=172.18.62.158
      dpt=25 deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=SMTP
      FTNTFGTprofile=test-spam act=log-only suser=testpc1@qa.fortinet.com
      duser=test1@server88.qa.fortinet.com FTNTFGTsender=testpc1@qa.fortinet.com
      FTNTFGTrecipient=test1@server88.qa.fortinet.com deviceDirection=1 msg=general email log
      FTNTFGTsubject=hello_world2 FTNTFGTsize=216 FTNTFGTattachment=no
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
from	suser
to	duser

Anomaly log support for CEF

The following is an example of an anomaly log on the FortiGate disk:

```
date=2018-12-27 time=11:40:04 logid="0720018433" type="utm" subtype="anomaly" eventtype="anomaly"
      level="alert" vd="vdom1" eventtime=1545939604 severity="critical" srcip=10.1.100.11
      srccountry="Reserved" dstip=172.16.200.55 srcintf="port12" srcintfrole="undefined"
      sessionid=0 action="clear_session" proto=1 service="PING" count=1 attack="icmp_flood"
      icmpid="0x3053" icmptype="0x08" icmpcode="0x00" attackid=16777316 policyid=1
      policytype="DoS-policy" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_
      flood, 51 > threshold 50" crscore=50 crlevel="critical"
```

The following is an example of an anomaly log sent in CEF format to a syslog server:

```
Dec 27 11:40:04 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|18433|utm:anomaly anomaly clear_
      session|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0720018433 cat=utm:anomaly
      FTNTFGTsubtype=anomaly FTNTFGTeventtype=anomaly FTNTFGTlevel=alert FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545939604 FTNTFGTseverity=critical src=10.1.100.11
      FTNTFGTsrccountry=Reserved dst=172.16.200.55 deviceInboundInterface=port12
      FTNTFGTsrcintfrole=undefined externalId=0 act=clear_session proto=1 app=PING cnt=1
      FTNTFGTattack=icmp_flood FTNTFGTicmpid=0x3053 FTNTFGTicmptype=0x08 FTNTFGTicmpcode=0x00
      FTNTFGTattackid=16777316 FTNTFGTpolicyid=1 FTNTFGTpolicytype=DoS-policy
      FTNTFGTref=http://www.fortinet.com/ids/VID16777316 msg=anomaly: icmp_flood, 51 > threshold
      50 FTNTFGTcrscore=50 FTNTFGTcrlevel=critical
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
count	cnt

VoIP log support for CEF

The following is an example of an VoIP log on the FortiGate disk:

```
date=2018-12-27 time=16:47:09 logid="0814044032" type="utm" subtype="voip" eventtype="voip"
      level="information" vd="vdom1" eventtime=1545958028 session_id=18975 epoch=0 event_id=6857
      srcip=10.1.100.11 src_port=5060 dstip=172.16.200.55 dst_port=5060 proto=17 src_int="port12"
      dst_int="port11" policy_id=1 profile="default" voip_proto="sip" kind="call" action="permit"
      status="start" duration=0 dir="session_origin" call_id="3444-13134@127.0.0.1"
      from="sip:sipp@127.0.0.1:5060" to="sip:service@172.16.200.55:5060"
```

The following is an example of an VoIP sent in CEF format to a syslog server:

```
Dec 27 16:47:08 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|44032|utm:voip voip permit
      start|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0814044032 cat=utm:voip
      FTNTFGTsubtype=voip FTNTFGTeventtype=voip FTNTFGTlevel=information FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545958028 externalId=18975 FTNTFGTepoch=0 FTNTFGTevent_id=6857
      src=10.1.100.11 spt=5060 dst=172.16.200.55 dpt=5060 proto=17 deviceInboundInterface=port12
      deviceOutboundInterface=port11 FTNTFGTpolicy_id=1 FTNTFGTprofile=default FTNTFGTvoip_
      proto=sip FTNTFGTkind=call act=permit outcome=start FTNTFGTduration=0 FTNTFGTdir=session_
      origin FTNTFGTcall_id=3444-13134@127.0.0.1 suser=sip:sipp@127.0.0.1:5060
      duser=sip:service@172.16.200.55:5060
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
status	outcome
from	suser
to	duser

DLP log support for CEF

The following is an example of a DLP log on the FortiGate disk:

```
date=2018-12-27 time=14:29:36 logid="0954024576" type="utm" subtype="dlp" eventtype="dlp"
      level="warning" vd="vdom1" eventtime=1545949776 filteridx=1 dlpextra="test-dlp3"
      filtertype="file-type" filtercat="file" severity="medium" policyid=1 sessionid=12680
      epoch=418303178 eventid=0 user="bob" srcip=10.1.100.11 srcport=33638 srcintf="port12"
      srcintfrole="undefined" dstip=172.18.62.158 dstport=80 dstintf="port11"
      dstintfrole="undefined" proto=6 service="HTTP" filetype="gif" direction="incoming"
      action="block" hostname="172.18.62.158" url="/dlp/flower.gif" agent="curl/7.47.0"
      filename="flower.gif" filesize=1209 profile="test-dlp"
```

The following is an example of a DLP log sent in CEF format to a syslog server:

```
Dec 27 14:29:36 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|24576|utm:dlp dlp
      block|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0954024576 cat=utm:dlp
      FTNTFGTsubtype=dlp FTNTFGTeventtype=dlp FTNTFGTlevel=warning FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545949776 FTNTFGTfilteridx=1 FTNTFGTdlpextra=test-dlp3
      FTNTFGTfiltertype=file-type FTNTFGTfiltercat=file FTNTFGTseverity=medium FTNTFGTpolicyid=1
      externalId=12680 FTNTFGTepoch=418303178 FTNTFGTeventid=0 duser=bob src=10.1.100.11 spt=33638
      deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined dst=172.18.62.158 dpt=80
      deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=HTTP
      FTNTFGTfiletype=gif deviceDirection=0 act=block dhost=172.18.62.158 request=/dlp/flower.gif
      requestClientApplication=curl/7.47.0 fname=flower.gif fsize=1209 FTNTFGTprofile=test-dlp
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
filename	fname

Application log support for CEF

The following is an example of an application log on the FortiGate disk:

```
date=2018-12-27 time=14:28:08 logid="1059028704" type="utm" subtype="app-ctrl" eventtype="app-
      ctrl-all" level="information" vd="vdom1" eventtime=1545949688 appid=34050 srcip=10.1.100.11
      dstip=104.80.89.24 srcport=56826 dstport=80 srcintf="port12" srcintfrole="undefined"
      dstintf="port11" dstintfrole="undefined" proto=6 service="HTTP" direction="outgoing"
      policyid=1 sessionid=12567 applist="g-default" appcat="Web.Client" app="HTTP.BROWSER_
      Firefox" action="pass" hostname="detectportal.firefox.com" incidentserialno=1702350499
      url="/success.txt" msg="Web.Client: HTTP.BROWSER_Firefox," apprisk="elevated"
```

The following is an example of an application sent in CEF format to a syslog server:

```
Dec 27 14:28:08 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|28704|utm:app-ctrl app-ctrl-all
      pass|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1059028704 cat=utm:app-ctrl
      FTNTFGTsubtype=app-ctrl FTNTFGTeventtype=app-ctrl-all FTNTFGTlevel=information
      FTNTFGTvd=vdom1 FTNTFGTeventtime=1545949688 FTNTFGTappid=34050 src=10.1.100.11
      dst=104.80.89.24 spt=56826 dpt=80 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined
      deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=HTTP
      deviceDirection=1 FTNTFGTpolicyid=1 externalId=12567 FTNTFGTapplist=g-default
      FTNTFGTappcat=Web.Client FTNTFGTapp=HTTP.BROWSER_Firefox act=pass
      dhost=detectportal.firefox.com FTNTFGTincidentserialno=1702350499 request=/success.txt
      msg=Web.Client: HTTP.BROWSER_Firefox, FTNTFGTapprisk=elevated
```

WAF log support for CEF

The following is an example of an WAF log on the FortiGate disk:

```
date=2018-12-27 time=14:55:20 logid="1203030258" type="utm" subtype="waf" eventtype="waf-http-
      constraint" level="warning" vd="vdom1" eventtime=1545951320 policyid=1 sessionid=13614
      user="bob" profile="waf_test" srcip=10.1.100.11 srcport=57304 dstip=172.16.200.55 dstport=80
      srcintf="port12" srcintfrole="lan" dstintf="port11" dstintfrole="wan" proto=6 service="HTTP"
      url="http://172.16.200.55/index.html?a=0123456789&b=0123456789&c=0123456789"
      severity="medium" action="passthrough" direction="request" agent="curl/7.47.0"
      constraint="url-param-num" rawdata="Method=GET|User-Agent=curl/7.47.0"
```

The following is an example of an WAF sent in CEF format to a syslog server:

```
Dec 27 14:55:20 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|30258|utm:waf waf-http-constraint
      passthrough|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1203030258 cat=utm:waf
      FTNTFGTsubtype=waf FTNTFGTeventtype=waf-http-constraint FTNTFGTlevel=warning FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545951320 FTNTFGTpolicyid=1 externalId=13614 duser=bob FTNTFGTprofile=waf_
      test src=10.1.100.11 spt=57304 dst=172.16.200.55 dpt=80 deviceInboundInterface=port12
      FTNTFGTsrcintfrole=lan deviceOutboundInterface=port11 FTNTFGTdstintfrole=wan proto=6
      app=HTTP request=http://172.16.200.55/index.html?a\=0123456789&b\=0123456789&c\=0123456789
      FTNTFGTseverity=medium act=passthrough deviceDirection=0
      requestClientApplication=curl/7.47.0 FTNTFGTconstraint=url-param-num
      FTNTFGTrawdata=Method\=GET|User-Agent\=curl/7.47.0
```

DNS log support for CEF

The following is an example of an DNS log on the FortiGate disk:

```
date=2018-12-27 time=14:45:26 logid="1501054802" type="dns" subtype="dns-response" level="notice"
      vd="vdom1" eventtime=1545950726 policyid=1 sessionid=13355 user="bob" srcip=10.1.100.11
      srcport=54621 srcintf="port12" srcintfrole="lan" dstip=172.16.200.55 dstport=53
      dstintf="port11" dstintfrole="wan" proto=17 profile="default" srcmac="a2:e9:00:ec:40:01"
      xid=5137 qname="detectportal.firefox.com" qtype="A" qtypeval=1 qclass="IN"
      ipaddr="104.80.89.26, 104.80.89.24" msg="Domain is monitored" action="pass" cat=52
      catdesc="Information Technology"
```

The following is an example of an DNS sent in CEF format to a syslog server:

```
Dec 27 14:45:26 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|54802|dns:dns-response
      pass|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1501054802 cat=dns:dns-response
      FTNTFGTsubtype=dns-response FTNTFGTlevel=notice FTNTFGTvd=vdom1 FTNTFGTeventtime=1545950726
      FTNTFGTpolicyid=1 externalId=13355 duser=bob src=10.1.100.11 spt=54621
      deviceInboundInterface=port12 FTNTFGTsrcintfrole=lan dst=172.16.200.55 dpt=53
      deviceOutboundInterface=port11 FTNTFGTdstintfrole=wan proto=17 FTNTFGTprofile=default
      FTNTFGTsrcmac=a2:e9:00:ec:40:01 FTNTFGTxid=5137 FTNTFGTqname=detectportal.firefox.com
      FTNTFGTqtype=A FTNTFGTqtypeval=1 FTNTFGTqclass=IN FTNTFGTipaddr=104.80.89.26, 104.80.89.24
      msg=Domain is monitored act=pass FTNTFGTcat=52 FTNTFGTcatdesc=Information Technology
```

SSH log support for CEF

The following is an example of an SSH log on the FortiGate disk:

```
date=2018-12-27 time=14:36:15 logid="1600061002" type="utm" subtype="ssh" eventtype="ssh-command"
      level="notice" vd="vdom1" eventtime=1545950175 policyid=1 sessionid=12921 user="bob"
      profile="test-ssh" srcip=10.1.100.11 srcport=56698 dstip=172.16.200.55 dstport=22
      srcintf="port12" srcintfrole="lan" dstintf="port11" dstintfrole="wan" proto=6
      action="passthrough" direction="outgoing" login="root" command="ls" severity="low"
```

The following is an example of an SSH sent in CEF format to a syslog server:

```
Dec 27 14:36:15 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|61002|utm:ssh ssh-command
      passthrough|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1600061002 cat=utm:ssh
      FTNTFGTsubtype=ssh FTNTFGTeventtype=ssh-command FTNTFGTlevel=notice FTNTFGTvd=vdom1
      FTNTFGTeventtime=1545950175 FTNTFGTpolicyid=1 externalId=12921 duser=bob
      FTNTFGTprofile=test-ssh src=10.1.100.11 spt=56698 dst=172.16.200.55 dpt=22
      deviceInboundInterface=port12 FTNTFGTsrcintfrole=lan deviceOutboundInterface=port11
      FTNTFGTdstintfrole=wan proto=6 act=passthrough FTNTFGTlogin=root FTNTFGTcommand=ls
      FTNTFGTseverity=low
```

UTM extended logging

FortiOS 6.0.0 and later supports extended logging for UTM log types to reliable Syslog servers over TCP. Extended logging adds HTTP header information to the `rawdata` field in UTM log types. You must enable extended logging before you can use the feature.

When extended logging is enabled, the following HTTP header information can be added to the *rawdata* field in UTM logs:

- Method
- X-Forwarded-For
- Request-Content-Type | Response-Content-Type
- Referer
- User-Agent

The full *rawdata* field of 20KB is only sent to reliable Syslog servers. Other logging devices, such as disk, FortiAnalyzer, and UDP Syslog servers, receive the information, but only keep a maximum of 2KB total log length, including the *rawdata* field, and discard the rest of the extended log information.

Enabling extended logging

You can enable extended logging for the following UTM profiles:

- antivirus
- application
- dlp
- ips
- waf
- webfilter

When you enable the `extended-log` option for UTM profiles, all HTTP header information for HTTP-deny traffic is logged.

When you enable the `web-extended-all-action-log-enable` option for webfilter profile, all HTTP header information for HTTP-allow traffic is logged.

Extended logging option in UTM profiles

The `extended-log` option has been added to all UTM profiles, for example:

```
config webfilter profile
    edit "test-webfilter"
        set extended-log enable
        set web-extended-all-action-log enable
    next
end
config antivirus profile
    edit "av-proxy-test"
        set extended-log enable
    next
end
config waf profile
    edit "test-waf"
        set extended-log enable
    next
end
```

Syslog server mode

The Syslog server `mode` changed to `udp`, `reliable`, and `legacy-reliable`. You must set the mode to `reliable` to support extended logging, for example:

```
config log syslogd setting
    set status enable
    set server "<ip address>"
    set mode reliable
    set facility local6
end
```

Example 1: Extended log

Following is an example extended log for a `utm` log type with a *webfilter* subtype for a reliable Syslog server. The `rawdata` field contains the extended log data.

```
2: date=2022-03-07 time=14:15:27 eventtime=1646691327786322587 tz="-0800" logid="0316013056"
type="utm" subtype="webfilter" eventtype="ftgd_blk" level="warning" vd="vdom1" policyid=1
poluuid="fe85f37c-9dd9-51ec-904d-5af91079efbb" policytype="policy" sessionid=7284
srcip=10.1.100.18 srcport=50856 srccountry="Reserved" srcintf="port2" srcintfrole="undefined"
srcuuid="69dc4a54-9d99-51ec-16ee-395d60cceac6" dstip=142.250.69.196 dstport=443 dstcountry="United
States" dstintf="port1" dstintfrole="undefined" dstuuid="69dc4a54-9d99-51ec-16ee-395d60cceac6"
proto=6 httpmethod="GET" service="HTTPS" hostname="http://www.google.com"
forwardedfor="192.168.0.99" agent="curl/7.56.0" profile="webfilter" action="blocked"
reqtype="referral" url="https://www.google.com/" referralurl="https://example.com/referer.html"
sentbyte=869 rcvdbyte=4313 direction="outgoing" msg="URL belongs to a denied category in policy"
ratemethod="domain" cat=41 catdesc="Search Engines and Portals" rawdata="x-forwarded-
for=192.168.0.99"
```

Example 2: Extended log for explicit proxy logging

The `rawdata` field with the `[REQ]` and `[RESP]` fields corresponds to the HTTP header monitor feature which monitors and logs headers in HTTP Request and Response. The request was sent through a FortiGate running transparent or explicit proxy.

```
1: date=2023-04-19 time=19:01:19 eventtime=1681956079146481995 tz="-0700" logid="0314012288"
type="utm" subtype="webfilter" eventtype="content" level="warning" vd="vdom1" policyid=1
poluuid="4d8dc396-46e3-51ea-7f3f-ee328a5bd07b" policytype="policy" sessionid=40980
srcip=10.1.100.13 srcport=54512 srccountry="Reserved" srcintf="port10" srcintfrole="undefined"
srcuuid="6ce0b8ca-30ae-51ea-a388-ceacbb4fb045" dstip=172.16.200.33 dstport=443
dstcountry="Reserved" dstintf="port9" dstintfrole="undefined" dstuuid="6ce0b8ca-30ae-51ea-a388-
ceacbb4fb045" proto=6 httpmethod="GET" service="HTTPS" hostname="172.16.200.33"
agent="curl/7.61.1" profile="header" reqtype="direct" url="https://172.16.200.33/" sentbyte=0
rcvdbyte=0 direction="incoming" action="blocked" banword="works" msg="URL was blocked because it
contained banned word(s)." rawdata="[REQ] test_request_header=aaaaa||[RESP] Content-
Type=text/html|ETag=\"34-5b23b9d3b67f4\""
```

Example 3: Extended log for DLP inspection

The following example shows DLP inspection being applied in a policy when `extended-log` is enabled in the DLP profile and DLP blocks the file.

```
config dlp profile
    edit "851560"
        set feature-set proxy
        config rule
            edit 1
                set name "851560"
                set proto http-get http-post
                set file-type 3
                set action block
            next
        end
        set extended-log enable
    next
end
```

```
1: date=2023-08-10 time=10:50:50 eventtime=1691689849954382569 tz="-0700" logid="0954024576"
type="utm" subtype="dlp" eventtype="dlp" level="warning" vd="vdom1" filteridx=1
filtername="851560" dlpextra="file-type:3" filtertype="none" filtercat="file" severity="medium"
policyid=1 poluuid="c3cd12ea-379f-51ee-c12b-ea7a6620d365" policytype="policy" sessionid=1024
epoch=1334644382 eventid=0 srcip=10.1.100.11 srcport=38182 srccountry="Reserved" srcintf="port2"
srcintfrole="undefined" srcuuid="8789d048-379f-51ee-ea7e-79004e2dda0c" dstip=172.16.200.55
dstport=80 dstcountry="Reserved" dstintf="port1" dstintfrole="undefined" dstuuid="8789d048-379f-
51ee-ea7e-79004e2dda0c" proto=6 service="HTTP" filetype="pdf" direction="incoming" action="block"
hostname="172.16.200.55" url="http://172.16.200.55/dlp/files/fortiauto.pdf" agent="curl/7.58.0"
httpmethod="GET" filename="fortiauto.pdf" filesize=285442 profile="851560" rawdata="[RESP]
Content-Type=application/pdf"
```

Log Messages

The following sections list the FortiOS 7.4.9 log messages by log ID number.

Anomaly

18432 - LOGID_ATTCK_ANOMALY_TCP_UDP

Message ID: 18432

Message Description: LOGID_ATTCK_ANOMALY_TCP_UDP

Message Meaning: Attack detected by UCP/TCP anomaly

Type: Anomaly

Category: anomaly

Severity: Alert

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual Domain Name	string	32
user	User	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64

Log Field Name	Description	Data Type	Length
severity	Severity	string	8
sessionid	Session ID	uint32	10
service	Name of Service	string	80
ref	Reference	string	4096
proto	Protocol	uint8	3
policytype	Policy type	string	24
policyid	Policy ID	uint32	10
msg	Log Message	string	518
logid	Log ID	string	10
level	Log Level	string	11
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
count	Count	uint32	10
attackid	Attack ID	uint32	10
attack	Attack	string	256
action	Action	string	16

18433 - LOGID_ATTCK_ANOMALY_ICMP

Message ID: 18433

Message Description: LOGID_ATTCK_ANOMALY_ICMP

Message Meaning: Attack detected by ICMP anomaly

Type: Anomaly

Category: anomaly

Severity: Alert

Log Field Name	Description	Data Type	Length
icmptype	ICMP Type	string	6
icmpid	ICMP ID	string	8
icmpcode	ICMP code	string	6
vrf	Virtual router forwarding	uint8	3
vd	Virtual Domain Name	string	32
user	User	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity	string	8
sessionid	Session ID	uint32	10
service	Name of Service	string	80
ref	Reference	string	4096
proto	Protocol	uint8	3
policytype	Policy type	string	24
policyid	Policy ID	uint32	10
msg	Log Message	string	518
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
count	Count	uint32	10
attackid	Attack ID	uint32	10
attack	Attack	string	256
action	Action	string	16

18434 - LOGID_ATTCK_ANOMALY_OTHERS

Message ID: 18434

Message Description: LOGID_ATTCK_ANOMALY_OTHERS

Message Meaning: Attack detected by other anomaly

Type: Anomaly

Category: anomaly

Severity: Alert

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual Domain Name	string	32
user	User	string	256

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity	string	8
sessionid	Session ID	uint32	10
service	Name of Service	string	80
ref	Reference	string	4096
proto	Protocol	uint8	3
policytype	Policy type	string	24
policyid	Policy ID	uint32	10
msg	Log Message	string	518
logid	Log ID	string	10
level	Log Level	string	11
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64

Log Field Name	Description	Data Type	Length
dstcountry		string	64
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
count	Count	uint32	10
attackid	Attack ID	uint32	10
attack	Attack	string	256
action	Action	string	16

APP-CTRL

28672 - LOGID_APP_CTRL_IM_BASIC

Message ID: 28672

Message Description: LOGID_APP_CTRL_IM_BASIC

Message Meaning: Application control IM-basic

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64

Log Field Name	Description	Data Type	Length
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28673 - LOGID_APP_CTRL_IM_BASIC_WITH_STATUS

Message ID: 28673

Message Description: LOGID_APP_CTRL_IM_BASIC_WITH_STATUS

Message Meaning: Application control IM

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28674 - LOGID_APP_CTRL_IM_BASIC_WITH_COUNT

Message ID: 28674

Message Description: LOGID_APP_CTRL_IM_BASIC_WITH_COUNT

Message Meaning: Application control IM (chat message count)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28675 - LOGID_APP_CTRL_IM_FILE

Message ID: 28675

Message Description: LOGID_APP_CTRL_IM_FILE

Message Meaning: Application control IM (file)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8

Log Field Name	Description	Data Type	Length
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28676 - LOGID_APP_CTRL_IM_CHAT

Message ID: 28676

Message Description: LOGID_APP_CTRL_IM_CHAT

Message Meaning: Application control IM (chat)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28677 - LOGID_APP_CTRL_IM_CHAT_BLOCK

Message ID: 28677

Message Description: LOGID_APP_CTRL_IM_CHAT_BLOCK

Message Meaning: Application control IM (chat blocked)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28678 - LOGID_APP_CTRL_IM_BLOCK

Message ID: 28678

Message Description: LOGID_APP_CTRL_IM_BLOCK

Message Meaning: Application control IM (blocked)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28704 - LOGID_APP_CTRL_IPS_PASS

Message ID: 28704

Message Description: LOGID_APP_CTRL_IPS_PASS

Message Meaning: Application control (IPS) (pass)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
url	The URL address	string	512
trueclntip	True-Client-IP	ip	39
scertissuer	server certificate issuer	string	64
scertcname	server certificate name	string	64

Log Field Name	Description	Data Type	Length
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
poluuid		string	37
policytype		string	24
policymode		string	8
pdstport		uint16	5
parameters		string	512
msg	Log message	string	512
incidentserialno	Incident serial number	uint32	10
icmptype		string	6
icmpid		string	8
icmpcode		string	6
httpmethod		string	20
hostname	The host name of a URL	string	256
forwardedfor	Forwarded For	string	128
filesize	File size in bytes	uint64	10
filename	File name	string	256
dstuser		string	256
dstauthserver		string	64
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
clouduser	User login ID detected by the Deep Application Control feature	string	256
clouddevice		string	256
cloudaction	Action performed by cloud application	string	32
ccertissuer		string	64

Log Field Name	Description	Data Type	Length
apprisk	Application risk level	string	16
appid	Application ID	uint32	10
agent		string	1024
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28705 - LOGID_APP_CTRL_IPS_BLOCK

Message ID: 28705

Message Description: LOGID_APP_CTRL_IPS_BLOCK

Message Meaning: Application control (IPS) (block)

Type: APP-CTRL

Category: signature

Severity: Warning

Log Field Name	Description	Data Type	Length
url	The URL address	string	512
trueclntip	True-Client-IP	ip	39
scertissuer	server certificate issuer	string	64
scertcname	server certificate name	string	64

Log Field Name	Description	Data Type	Length
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
poluuid		string	37
policytype		string	24
policymode		string	8
pdstport		uint16	5
parameters		string	512
msg	Log message	string	512
incidentserialno	Incident serial number	uint32	10
icmptype		string	6
icmpid		string	8
icmpcode		string	6
httpmethod		string	20
hostname	The host name of a URL	string	256
forwardedfor	Forwarded For	string	128
filesize	File size in bytes	uint64	10
filename	File name	string	256
dstuser		string	256
dstauthserver		string	64
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
clouduser	User login ID detected by the Deep Application Control feature	string	256
clouddevice		string	256
cloudaction	Action performed by cloud application	string	32
ccertissuer		string	64

Log Field Name	Description	Data Type	Length
apprisk	Application risk level	string	16
appid	Application ID	uint32	10
agent		string	1024
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28706 - LOGID_APP_CTRL_IPS_RESET

Message ID: 28706

Message Description: LOGID_APP_CTRL_IPS_RESET

Message Meaning: Application control (IPS) (reset)

Type: APP-CTRL

Category: signature

Severity: Warning

Log Field Name	Description	Data Type	Length
url	The URL address	string	512
trueclntip	True-Client-IP	ip	39
scertissuer	server certificate issuer	string	64
scertcname	server certificate name	string	64

Log Field Name	Description	Data Type	Length
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
poluuid		string	37
policytype		string	24
policymode		string	8
pdstport		uint16	5
parameters		string	512
msg	Log message	string	512
incidentserialno	Incident serial number	uint32	10
icmptype		string	6
icmpid		string	8
icmpcode		string	6
httpmethod		string	20
hostname	The host name of a URL	string	256
forwardedfor	Forwarded For	string	128
filesize	File size in bytes	uint64	10
filename	File name	string	256
dstuser		string	256
dstauthserver		string	64
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
clouduser	User login ID detected by the Deep Application Control feature	string	256
clouddevice		string	256
cloudaction	Action performed by cloud application	string	32
ccertissuer		string	64

Log Field Name	Description	Data Type	Length
apprisk	Application risk level	string	16
appid	Application ID	uint32	10
agent		string	1024
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28720 - LOGID_APP_CTRL_SSH_PASS

Message ID: 28720

Message Description: LOGID_APP_CTRL_SSH_PASS

Message Meaning: Application control IM (SSH) (pass)

Type: APP-CTRL

Category: signature

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28721 - LOGID_APP_CTRL_SSH_BLOCK

Message ID: 28721

Message Description: LOGID_APP_CTRL_SSH_BLOCK

Message Meaning: Application control IM (SSH) (block)

Type: APP-CTRL

Category: signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log level	string	11
group	User group name	string	512
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
authserver	Authentication server for the user	string	64
applist	Application Control profile name	string	64
appcat	Application category name	string	64
app	Application name	string	96

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28736 - LOGID_APP_CTRL_PORT_ENF

Message ID: 28736

Message Description: LOGID_APP_CTRL_PORT_ENF

Message Meaning: Application control port enforcement

Type: APP-CTRL

Category: port-violation

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
scertissuer	server certificate issuer	string	64
scertcname	server certificate name	string	64
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
parameters		string	512
msg	Log message	string	512
logid	Log ID	string	10
level	Log level	string	11
incidentserialno	Incident serial number	uint32	10
icmptype		string	6
icmpid		string	8
icmpcode		string	6
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	Forwarded For	string	128

Log Field Name	Description	Data Type	Length
filesize	File size in bytes	uint64	10
filename	File name	string	256
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
clouduser	User login ID detected by the Deep Application Control feature	string	256
clouddevice		string	256
cloudaction	Action performed by cloud application	string	32
ccertissuer		string	64
authserver	Authentication server for the user	string	64
apprisk	Application risk level	string	16
applist	Application Control profile name	string	64
appid	Application ID	uint32	10
appcat	Application category name	string	64
app	Application name	string	96
agent		string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

28737 - LOGID_APP_CTRL_PROTO_ENF

Message ID: 28737

Message Description: LOGID_APP_CTRL_PROTO_ENF

Message Meaning: Application control protocol enforcement

Type: APP-CTRL

Category: protocol-violation

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	80
scertissuer	server certificate issuer	string	64
scertcname	server certificate name	string	64
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profiletype	Profile Type	string	36
profile		string	36
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
parameters		string	512
msg	Log message	string	512
logid	Log ID	string	10
level	Log level	string	11
incidentserialno	Incident serial number	uint32	10
icmptype		string	6
icmpid		string	8
icmpcode		string	6
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	Forwarded For	string	128

Log Field Name	Description	Data Type	Length
filesize	File size in bytes	uint64	10
filename	File name	string	256
fctuid	FortiClient User ID	string	32
eventtype	App Control Event Type	string	32
eventtime	Event Time	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the packets	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Client Reputation Action	uint32	10
clouduser	User login ID detected by the Deep Application Control feature	string	256
clouddevice		string	256
cloudaction	Action performed by cloud application	string	32
ccertissuer		string	64
authserver	Authentication server for the user	string	64
apprisk	Application risk level	string	16
applist	Application Control profile name	string	64
appid	Application ID	uint32	10
appcat	Application category name	string	64
app	Application name	string	96
agent		string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

casb

10000 - LOG_ID_CASB_ACCESS_BLOCKED

Message ID: 10000

Message Description: LOG_ID_CASB_ACCESS_BLOCKED

Message Meaning: Web content banned activity found

Type: casb

Category: casb

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
useractivity		string	80
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10

Log Field Name	Description	Data Type	Length
srcintf		string	32
sessionid		uint32	10
saasapp		string	80
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
operation		string	80
msg		string	512
logid		string	10
level		string	11
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
activitycategory		string	30
action		string	11

10001 - LOG_ID_CASB_ACCESS_BYPASS

Message ID: 10001

Message Description: LOG_ID_CASB_ACCESS_BYPASS

Message Meaning: Web content activity found

Type: casb

Category: casb

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
useractivity		string	80
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
saasapp		string	80
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
operation		string	80
msg		string	512
logid		string	10
level		string	11
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
activitycategory		string	30
action		string	11

10002 - LOG_ID_CASB_ACCESS_MONITOR

Message ID: 10002

Message Description: LOG_ID_CASB_ACCESS_MONITOR

Message Meaning: Web content activity found

Type: casb

Category: casb

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
useractivity		string	80
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32

Log Field Name	Description	Data Type	Length
sessionid		uint32	10
saasapp		string	80
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
operation		string	80
msg		string	512
logid		string	10
level		string	11
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
activitycategory		string	30
action		string	11

DLP

24576 - LOG_ID_DLP_WARN

Message ID: 24576

Message Description: LOG_ID_DLP_WARN

Message Meaning: Data loss detected by specified DLP sensor rule

Type: DLP

Category: dlp

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True client's IP	ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Log subtype	string	20
subservice		string	16
subject	The subject title of the email message	string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of a DLP rule	string	8
sessionid	Session ID	uint32	10
service	Service name	string	36
sender	Email address from the SMTP envelope	string	128
rulename		string	128
ruleid		uint32	10

Log Field Name	Description	Data Type	Length
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata	Raw Data	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	DLP profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
logid	Log ID	string	10
level	Log Level	string	11
infectedfiletype	Infected File Type	string	23
infectedfilesize	Infected File Size	uint64	10
infectedfilename	Infected File Name	string	256
infectedfilelevel	Infected File Level (Critical,Warning etc)	uint32	10
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor	Forwarded For	string	128
filtertype	DLP filter type	string	23
filtercat	DLP filter category	string	8
filetype	File type	string	23
filesize	File size in bytes	uint64	10
filename	File name	string	256
fctuid	FortiClient User ID	string	32
eventtype	DLP event type	string	32
eventtime	Event Time, time when DLP event detected.	uint64	20

Log Field Name	Description	Data Type	Length
eventid	The serial number of the dlparchive file in the same epoch	uint32	10
epoch	Epoch used for locating file	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
dlpextra	DLP extra information	string	256
direction	Direction of packets	string	8
devid	Device ID	string	16
date	Date	string	10
cc		string	512
authserver	Authentication Server	string	64
attachment		string	3
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: log-only - DLP event is detected , but NOT blocked (similar to monitor action) block - Blocked exempt - Allowed ban - blocked (Not in used since FortiOS 5.0, replaced by blocked) ban-sender - blocks all data being sent by an ip or user (Not in used since FortiOS 5.0, replaced by quarantine) quarantine-ip - Blocked and band the source ip (Not in used since FortiOS 5.0) quarantine-interface - Blocked and band the source interface (Not in used since FortiOS 5.0)	string	20

24577 - LOG_ID_DLP_NOTIF

Message ID: 24577

Message Description: LOG_ID_DLP_NOTIF

Message Meaning: Data loss detected by specified DLP sensor rule

Type: DLP

Category: dlp

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual Routing Forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True client's IP	ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Log subtype	string	20
subservice		string	16
subject	The subject title of the email message	string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of a DLP rule	string	8
sessionid	Session ID	uint32	10
service	Service name	string	36
sender	Email address from the SMTP envelope	string	128

Log Field Name	Description	Data Type	Length
rulename		string	128
ruleid		uint32	10
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata	Raw Data	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	DLP profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
logid	Log ID	string	10
level	Log Level	string	11
infectedfiletype	Infected File Type	string	23
infectedfilesize	Infected File Size	uint64	10
infectedfilename	Infected File Name	string	256
infectedfilelevel	Infected File Level (Critical,Warning etc)	uint32	10
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor	Forwarded For	string	128
filtertype	DLP filter type	string	23
filtercat	DLP filter category	string	8
filetype	File type	string	23
filesize	File size in bytes	uint64	10
filename	File name	string	256
fctuid	FortiClient User ID	string	32

Log Field Name	Description	Data Type	Length
eventtype	DLP event type	string	32
eventtime	Event Time, time when DLP event detected.	uint64	20
eventid	The serial number of the dlparchive file in the same epoch	uint32	10
epoch	Epoch used for locating file	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
dlpextra	DLP extra information	string	256
direction	Direction of packets	string	8
devid	Device ID	string	16
date	Date	string	10
cc		string	512
authserver	Authentication Server	string	64
attachment		string	3
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: log-only - DLP event is detected , but NOT blocked (similar to monitor action) block - Blocked exempt - Allowed ban - blocked (Not in used since FortiOS 5.0, replaced by blocked) ban-sender - blocks all data being sent by an ip or user (Not in used since FortiOS 5.0, replaced by quarantine) quarantine-ip - Blocked and band the source ip (Not in used since FortiOS 5.0) quarantine-interface - Blocked and band the source interface (Not in used since FortiOS 5.0)	string	20

24578 - LOG_ID_DLP_DOC_SOURCE

Message ID: 24578

Message Description: LOG_ID_DLP_DOC_SOURCE

Message Meaning: DLP fingerprint document source notice

Type: DLP

Category: dlp-docsource

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
sensitivity	Sensitivity for document fingerprint	string	36
logid	Log ID	string	10
level	Log Level	string	11
eventtype	DLP event type	string	32
eventtime	Event Time, time when DLP event detected.	uint64	20
docsource	DLP fingerprint document source	string	515
dlpextra	DLP extra information	string	256
devid	Device ID	string	16
date	Date	string	10

24579 - LOG_ID_DLP_DOC_SOURCE_ERROR

Message ID: 24579

Message Description: LOG_ID_DLP_DOC_SOURCE_ERROR

Message Meaning: DLP fingerprint document source error

Type: DLP

Category: dlp-docsource

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
tz		string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
sensitivity	Sensitivity for document fingerprint	string	36
logid	Log ID	string	10
level	Log Level	string	11
eventtype	DLP event type	string	32
eventtime	Event Time, time when DLP event detected.	uint64	20
docsource	DLP fingerprint document source	string	515
dlpextra	DLP extra information	string	256
devid	Device ID	string	16
date	Date	string	10

DNS

54000 - LOG_ID_DNS_QUERY

Message ID: 54000

Message Description: LOG_ID_DNS_QUERY

Message Meaning: DNS query message

Type: DNS

Category: dns-query

Severity: Information

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log Level	string	11
group	User group name	string	512
fctuid	FortiClient ID	string	32
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
devid	Device ID	string	16
date	Date	string	10

54200 - LOG_ID_DNS_RESOLV_ERROR

Message ID: 54200

Message Description: LOG_ID_DNS_RESOLV_ERROR

Message Meaning: DNS resolution error message

Type: DNS

Category: dns-response

Severity: Error

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64

Log Field Name	Description	Data Type	Length
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54400 - LOG_ID_DNS_URL_FILTER_BLOCK

Message ID: 54400

Message Description: LOG_ID_DNS_URL_FILTER_BLOCK

Message Meaning: Domain blocked because it is in the domain-filter list

Type: DNS

Category: dns-response

Severity: Warning

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54401 - LOG_ID_DNS_URL_FILTER_ALLOW

Message ID: 54401

Message Description: LOG_ID_DNS_URL_FILTER_ALLOW

Message Meaning: Domain allowed because it is in the domain-filter list

Type: DNS

Category: dns-response

Severity: Information

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54600 - LOG_ID_DNS_BOTNET_IP

Message ID: 54600

Message Description: LOG_ID_DNS_BOTNET_IP

Message Meaning: Domain blocked by DNS botnet C&amp;C (IP)

Type: DNS

Category: dns-response

Severity: Warning

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256

Log Field Name	Description	Data Type	Length
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54601 - LOG_ID_DNS_BOTNET_DOMAIN

Message ID: 54601

Message Description: LOG_ID_DNS_BOTNET_DOMAIN

Message Meaning: Domain blocked by DNS botnet C&amp;C (Domain)

Type: DNS

Category: dns-response

Severity: Warning

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512

Log Field Name	Description	Data Type	Length
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54800 - LOG_ID_DNS_FTGD_WARNING

Message ID: 54800

Message Description: LOG_ID_DNS_FTGD_WARNING

Message Meaning: FortiGuard rating error warning

Type: DNS

Category: dns-response

Severity: Warning

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54801 - LOG_ID_DNS_FTGD_ERROR

Message ID: 54801

Message Description: LOG_ID_DNS_FTGD_ERROR

Message Meaning: FortiGuard rating error occurred

Type: DNS

Category: dns-response

Severity: Error

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54802 - LOG_ID_DNS_FTGD_CAT_ALLOW

Message ID: 54802

Message Description: LOG_ID_DNS_FTGD_CAT_ALLOW

Message Meaning: Domain is monitored

Type: DNS

Category: dns-response

Severity: Notice

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54803 - LOG_ID_DNS_FTGD_CAT_BLOCK

Message ID: 54803

Message Description: LOG_ID_DNS_FTGD_CAT_BLOCK

Message Meaning: Domain belongs to a denied category in policy

Type: DNS

Category: dns-response

Severity: Warning

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54804 - LOG_ID_DNS_SAFE_SEARCH

Message ID: 54804

Message Description: LOG_ID_DNS_SAFE_SEARCH

Message Meaning: DNS Safe Search enforced

Type: DNS

Category: dns-response

Severity: Notice

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

54805 - LOG_ID_DNS_LOCAL

Message ID: 54805

Message Description: LOG_ID_DNS_LOCAL

Message Meaning: DNS local query

Type: DNS

Category: dns-response

Severity: Information

Log Field Name	Description	Data Type	Length
xid	Transaction ID	uint16	5
vd	Virtual Domain Name	string	32
user	User name	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log Type	string	16
translationid		uint32	10
time	Time	string	8
subtype	Log Subtype	string	20
sscname	Safe Search CNAME	string	256
srcport	Source Port	uint16	5
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP	ip	39
srcintfrole	Source Interface Role	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
rcode		uint8	3
qtypeval	Query Type Value	uint16	5
qtype	Query type description	string	32
qname	Query domain name	string	256
qclass	Query class	string	32
proto	Protocol number	uint8	3
profile	Profile name for DNS filter	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
ipaddr	IP addresses from DNS response answer section	string	512
group	User group name	string	512
fctuid	FortiClient ID	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
eventtype	DNS Type (DNS query/DNS response)	string	32
eventtime	Event Timestamp	uint64	20
error	DNS filter service error message	string	256
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface Role	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
domainfilterlist	Domain Filter List	string	512
domainfilteridx	Domain Filter Index	uint8	3
devid	Device ID	string	16
date	Date	string	10
catdesc	DNS category description	string	64
cat	DNS category ID	uint8	3
botnetip	Botnet IP address	ip	39
botnetdomain	Botnet domain name	string	256
action	Security action performed by DNS filter	string	16

EmailFilter

20480 - LOGID_ANTISPAM_EMAIL_NOTIF

Message ID: 20480

Message Description: LOGID_ANTISPAM_EMAIL_NOTIF

Message Meaning: SPAM notification

Type: EmailFilter

Category: spam

Severity: Notice

Log Field Name	Description	Data Type	Length
webmailprovider		string	32
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
to		string	512
time		string	8
subtype		string	20
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
size		string	16
sessionid		uint32	10
service		string	36
sender		string	128
recipient		string	512
proto		uint8	3
profile		string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policymode		string	8
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
group		string	512
from		string	128
fortiguardresp		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	4096
banword		string	128
authserver		string	64
attachment		string	3
agent		string	1024
action		string	8

20481 - LOGID_EMAIL_GENERAL_NOTIF

Message ID: 20481

Message Description: LOGID_EMAIL_GENERAL_NOTIF

Message Meaning: Email message

Type: EmailFilter

Category: email

Severity: Information

Log Field Name	Description	Data Type	Length
webmailprovider		string	32
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
to		string	512
time		string	8
subtype		string	20
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
size		string	16
sessionid		uint32	10
service		string	36
sender		string	128

Log Field Name	Description	Data Type	Length
recipient		string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
group		string	512
from		string	128
fortiguardresp		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	4096
banword		string	128
authserver		string	64

Log Field Name	Description	Data Type	Length
attachment		string	3
agent		string	1024
action		string	8

20482 - LOGID_ANTISPAM_EMAIL_BWORD_NOTIF

Message ID: 20482

Message Description: LOGID_ANTISPAM_EMAIL_BWORD_NOTIF

Message Meaning: Banned word notification

Type: EmailFilter

Category: bannedword

Severity: Notice

Log Field Name	Description	Data Type	Length
webmailprovider		string	32
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
to		string	512
time		string	8
subtype		string	20
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
size		string	16
sessionid		uint32	10
service		string	36
sender		string	128
recipient		string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
group		string	512
from		string	128
fortiguardresp		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8

Log Field Name	Description	Data Type	Length
devid		string	16
date		string	10
cc		string	4096
banword		string	128
authserver		string	64
attachment		string	3
agent		string	1024
action		string	8

20509 - LOGID_ANTISPAM_FTGD_ERR

Message ID: 20509

Message Description: LOGID_ANTISPAM_FTGD_ERR

Message Meaning: FortiGuard error message

Type: EmailFilter

Category: ftgd_err

Severity: Notice

Log Field Name	Description	Data Type	Length
webmailprovider		string	32
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
to		string	512
time		string	8
subtype		string	20
subject		string	256
srcuuid		string	37

Log Field Name	Description	Data Type	Length
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
size		string	16
sessionid		uint32	10
service		string	36
sender		string	128
recipient		string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
group		string	512
from		string	128
fortiguardresp		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39

Log Field Name	Description	Data Type	Length
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	4096
banword		string	128
authserver		string	64
attachment		string	3
agent		string	1024
action		string	8

20510 - LOGID_ANTISPAM_EMAIL_WEBMAIL_NOTIF

Message ID: 20510

Message Description: LOGID_ANTISPAM_EMAIL_WEBMAIL_NOTIF

Message Meaning: Webmail message

Type: EmailFilter

Category: webmail

Severity: Information

Log Field Name	Description	Data Type	Length
webmailprovider		string	32
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16

Log Field Name	Description	Data Type	Length
to		string	512
time		string	8
subtype		string	20
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
size		string	16
sessionid		uint32	10
service		string	36
sender		string	128
recipient		string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
group		string	512
from		string	128
fortiguardresp		string	512
fctuid		string	32
eventtype		string	32

Log Field Name	Description	Data Type	Length
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	4096
banword		string	128
authserver		string	64
attachment		string	3
agent		string	1024
action		string	8

Event

20002 - LOG_ID_DOMAIN_UNRESOLVABLE

Message ID: 20002

Message Description: LOG_ID_DOMAIN_UNRESOLVABLE

Message Meaning: Domain name of alert email sender unresolvable

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20003 - LOG_ID_MAIL_SENT_FAIL

Message ID: 20003

Message Description: LOG_ID_MAIL_SENT_FAIL

Message Meaning: Alert email send status failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
count	Count	uint32	10
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20004 - LOG_ID_POLICY_TOO_BIG

Message ID: 20004

Message Description: LOG_ID_POLICY_TOO_BIG

Message Meaning: Policy too big for installation

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20005 - LOG_ID_PPP_LINK_UP

Message ID: 20005

Message Description: LOG_ID_PPP_LINK_UP

Message Meaning: Modem PPP link up

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20006 - LOG_ID_PPP_LINK_DOWN

Message ID: 20006

Message Description: LOG_ID_PPP_LINK_DOWN

Message Meaning: Modem PPP link down

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20007 - LOG_ID_SOCKET_EXHAUSTED

Message ID: 20007

Message Description: LOG_ID_SOCKET_EXHAUSTED

Message Meaning: Socket is exhausted

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
nat	NAT IP Address	ip	39
srcport	Source port	uint16	5

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
vrf		uint8	3
proto	Protocol Number	uint8	3
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20008 - LOG_ID_POLICY6_TOO_BIG

Message ID: 20008

Message Description: LOG_ID_POLICY6_TOO_BIG

Message Meaning: IPv6 policy too big for installation

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20010 - LOG_ID_KERNEL_ERROR

Message ID: 20010

Message Description: LOG_ID_KERNEL_ERROR

Message Meaning: Kernel error

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20016 - LOG_ID_MODEM_EXCEED_REDIAL_COUNT

Message ID: 20016

Message Description: LOG_ID_MODEM_EXCEED_REDIAL_COUNT

Message Meaning: Modem exceeded redial limit

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20017 - LOG_ID_MODEM_FAIL_TO_OPEN

Message ID: 20017

Message Description: LOG_ID_MODEM_FAIL_TO_OPEN

Message Meaning: Modem failed to open

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20020 - LOG_ID_MODEM_USB_DETECTED

Message ID: 20020

Message Description: LOG_ID_MODEM_USB_DETECTED

Message Meaning: USB modem detected

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20021 - LOG_ID_MAIL_RESENT

Message ID: 20021

Message Description: LOG_ID_MAIL_RESENT

Message Meaning: Alert email resent

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
count	Count	uint32	10
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20022 - LOG_ID_MODEM_USB_REMOVED

Message ID: 20022

Message Description: LOG_ID_MODEM_USB_REMOVED

Message Meaning: USB modem removed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20023 - LOG_ID_MODEM_USBLTE_DETECTED

Message ID: 20023

Message Description: LOG_ID_MODEM_USBLTE_DETECTED

Message Meaning: USB LTE modem detected

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20024 - LOG_ID_MODEM_USBLTE_REMOVED

Message ID: 20024

Message Description: LOG_ID_MODEM_USBLTE_REMOVED

Message Meaning: USB LTE modem removed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20025 - LOG_ID_REPORTD_REPORT_SUCCESS

Message ID: 20025

Message Description: LOG_ID_REPORTD_REPORT_SUCCESS

Message Meaning: Report generated successfully

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
processtime	Process time for reports	uint32	10
reporttype	Report Type	string	20
datarange	Data range for reports	string	50
filesize	Report File Size in Bytes	uint32	10
file	Report file full path	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20026 - LOG_ID_REPORTD_REPORT_FAILURE

Message ID: 20026

Message Description: LOG_ID_REPORTD_REPORT_FAILURE

Message Meaning: Report generation failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20028 - LOG_ID_REPORT_RECREATE_DB

Message ID: 20028

Message Description: LOG_ID_REPORT_RECREATE_DB

Message Meaning: Report database recreated

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20031 - LOG_ID_RAD_OUT_OF_MEM

Message ID: 20031

Message Description: LOG_ID_RAD_OUT_OF_MEM

Message Meaning: RADVD out of memory

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20032 - LOG_ID_RAD_NOT_FOUND

Message ID: 20032

Message Description: LOG_ID_RAD_NOT_FOUND

Message Meaning: RADVD interface not found

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20033 - LOG_ID_RAD_MOBILE_IPV6

Message ID: 20033

Message Description: LOG_ID_RAD_MOBILE_IPV6

Message Meaning: RADVD mobile IPv6 extensions used

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20034 - LOG_ID_RAD_IPV6_OUT_OF_RANGE

Message ID: 20034

Message Description: LOG_ID_RAD_IPV6_OUT_OF_RANGE

Message Meaning: RADVD mobile IPv6 MinRtrAdvInterval out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20035 - LOG_ID_RAD_MIN_OUT_OF_RANGE

Message ID: 20035

Message Description: LOG_ID_RAD_MIN_OUT_OF_RANGE

Message Meaning: RADVD MinRtrAdvInterval out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20036 - LOG_ID_RAD_MAX_OUT_OF_RANGE

Message ID: 20036

Message Description: LOG_ID_RAD_MAX_OUT_OF_RANGE

Message Meaning: RADVD mobile IPv6 MaxRtrAdvInterval out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20037 - LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE

Message ID: 20037

Message Description: LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE

Message Meaning: RADVD MaxRtrAdvInterval out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20039 - LOG_ID_RAD_MTU_TOO_SMALL

Message ID: 20039

Message Description: LOG_ID_RAD_MTU_TOO_SMALL

Message Meaning: RADVD AdvLinkMTU too small

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20040 - LOG_ID_RAD_TIME_TOO_SMALL

Message ID: 20040

Message Description: LOG_ID_RAD_TIME_TOO_SMALL

Message Meaning: RADVD AdvReachableTime too small

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20041 - LOG_ID_RAD_HOP_OUT_OF_RANGE

Message ID: 20041

Message Description: LOG_ID_RAD_HOP_OUT_OF_RANGE

Message Meaning: RADVD AdvCurHopLimit too big

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20042 - LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE

Message ID: 20042

Message Description: LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE

Message Meaning: RADVD AdvCurHopLimit out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20043 - LOG_ID_RAD_AGENT_OUT_OF_RANGE

Message ID: 20043

Message Description: LOG_ID_RAD_AGENT_OUT_OF_RANGE

Message Meaning: RADVD HomeAgentLifetime out of range

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20044 - LOG_ID_RAD_AGENT_FLAG_NOT_SET

Message ID: 20044

Message Description: LOG_ID_RAD_AGENT_FLAG_NOT_SET

Message Meaning: RADVD AdvHomeAgentFlag not set

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20045 - LOG_ID_RAD_PREFIX_TOO_LONG

Message ID: 20045

Message Description: LOG_ID_RAD_PREFIX_TOO_LONG

Message Meaning: RADVD invalid prefix length

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20046 - LOG_ID_RAD_PREF_TIME_TOO_SMALL

Message ID: 20046

Message Description: LOG_ID_RAD_PREF_TIME_TOO_SMALL

Message Meaning: RADVD AdvValidLifetime less than AdvPreferredLifetime

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20061 - LOG_ID_RAD_INV_ICMPV6_TYPE

Message ID: 20061

Message Description: LOG_ID_RAD_INV_ICMPV6_TYPE

Message Meaning: RADVD received unwanted ICMPv6 packet

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20062 - LOG_ID_RAD_INV_ICMPV6_RA_LEN

Message ID: 20062

Message Description: LOG_ID_RAD_INV_ICMPV6_RA_LEN

Message Meaning: RADVD received ICMPv6 RA packet with invalid length

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20063 - LOG_ID_RAD_ICMPV6_NO_SRC_ADDR

Message ID: 20063

Message Description: LOG_ID_RAD_ICMPV6_NO_SRC_ADDR

Message Meaning: RADVD received ICMPv6 RA packet with non-link local source address

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20064 - LOG_ID_RAD_INV_ICMPV6_RS_LEN

Message ID: 20064

Message Description: LOG_ID_RAD_INV_ICMPV6_RS_LEN

Message Meaning: RADVD received ICMPv6 RS packet with invalid length

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20065 - LOG_ID_RAD_INV_ICMPV6_CODE

Message ID: 20065

Message Description: LOG_ID_RAD_INV_ICMPV6_CODE

Message Meaning: RADVD received ICMPv6 RS/RA packet with invalid code

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20066 - LOG_ID_RAD_INV_ICMPV6_HOP

Message ID: 20066

Message Description: LOG_ID_RAD_INV_ICMPV6_HOP

Message Meaning: RADVD received ICMPv6 RS/RA packet with invalid hop limit

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20067 - LOG_ID_RAD_MISMATCH_HOP

Message ID: 20067

Message Description: LOG_ID_RAD_MISMATCH_HOP

Message Meaning: RADVD local AdvCurHopLimit disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20068 - LOG_ID_RAD_MISMATCH_MGR_FLAG

Message ID: 20068

Message Description: LOG_ID_RAD_MISMATCH_MGR_FLAG

Message Meaning: RADVD local AdvManagedFlag disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20069 - LOG_ID_RAD_MISMATCH_OTH_FLAG

Message ID: 20069

Message Description: LOG_ID_RAD_MISMATCH_OTH_FLAG

Message Meaning: RADVD local AdvOtherConfigFlag disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20070 - LOG_ID_RAD_MISMATCH_TIME

Message ID: 20070

Message Description: LOG_ID_RAD_MISMATCH_TIME

Message Meaning: RADVD local AdvReachableTime disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20071 - LOG_ID_RAD_MISMATCH_TIMER

Message ID: 20071

Message Description: LOG_ID_RAD_MISMATCH_TIMER

Message Meaning: RADVD local AdvRetransTimer disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20072 - LOG_ID_RAD_EXTRA_DATA

Message ID: 20072

Message Description: LOG_ID_RAD_EXTRA_DATA

Message Meaning: RADVD extra data in RA packet found

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20073 - LOG_ID_RAD_NO_OPT_DATA

Message ID: 20073

Message Description: LOG_ID_RAD_NO_OPT_DATA

Message Meaning: RADVD RA packet option length zero

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20074 - LOG_ID_RAD_INV_OPT_LEN

Message ID: 20074

Message Description: LOG_ID_RAD_INV_OPT_LEN

Message Meaning: RADVD RA packet option length greater than total length

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20075 - LOG_ID_RAD_MISMATCH_MTU

Message ID: 20075

Message Description: LOG_ID_RAD_MISMATCH_MTU

Message Meaning: RADVD local AdvLinkMTU disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20077 - LOG_ID_RAD_MISMATCH_PREF_TIME

Message ID: 20077

Message Description: LOG_ID_RAD_MISMATCH_PREF_TIME

Message Meaning: Interface AdvPreferredLifetime on our interface does not agree with a remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20078 - LOG_ID_RAD_INV_OPT

Message ID: 20078

Message Description: LOG_ID_RAD_INV_OPT

Message Meaning: RADVD found invalid option in RA packet from remote site

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20080 - LOG_ID_RAD_FAIL_TO_RCV

Message ID: 20080

Message Description: LOG_ID_RAD_FAIL_TO_RCV

Message Meaning: RADVD receive message failed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20081 - LOG_ID_RAD_INV_HOP

Message ID: 20081

Message Description: LOG_ID_RAD_INV_HOP

Message Meaning: RADVD received invalid IPv6 hop limit

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20082 - LOG_ID_RAD_INV_PKTINFO

Message ID: 20082

Message Description: LOG_ID_RAD_INV_PKTINFO

Message Meaning: RADVD received invalid IPv6 packet info

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20083 - LOG_ID_RAD_FAIL_TO_CHECK

Message ID: 20083

Message Description: LOG_ID_RAD_FAIL_TO_CHECK

Message Meaning: RADVD all-routers membership check failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20084 - LOG_ID_RAD_FAIL_TO_SEND

Message ID: 20084

Message Description: LOG_ID_RAD_FAIL_TO_SEND

Message Meaning: RADVD send message failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20085 - LOG_ID_SESSION_CLASH

Message ID: 20085

Message Description: LOG_ID_SESSION_CLASH

Message Meaning: Session clashed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
trace_id		string	32
proto	Protocol Number	uint8	3
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20090 - LOG_ID_INTF_LINK_STA_CHG

Message ID: 20090

Message Description: LOG_ID_INTF_LINK_STA_CHG

Message Meaning: Interface link status changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
intf	Interface	string	16
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20099 - LOG_ID_INTF_STA_CHG

Message ID: 20099

Message Description: LOG_ID_INTF_STA_CHG

Message Meaning: Interface status changed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20100 - LOG_ID_WEB_CAT_UPDATED

Message ID: 20100

Message Description: LOG_ID_WEB_CAT_UPDATED

Message Meaning: FortiGuard web filter category list updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20101 - LOG_ID_WEB_LIC_EXPIRE

Message ID: 20101

Message Description: LOG_ID_WEB_LIC_EXPIRE

Message Meaning: FortiGuard web filter license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20102 - LOG_ID_SPAM_LIC_EXPIRE

Message ID: 20102

Message Description: LOG_ID_SPAM_LIC_EXPIRE

Message Meaning: FortiGuard antispam license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20103 - LOG_ID_AV_LIC_EXPIRE

Message ID: 20103

Message Description: LOG_ID_AV_LIC_EXPIRE

Message Meaning: FortiGuard antivirus license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20104 - LOG_ID_IPS_LIC_EXPIRE

Message ID: 20104

Message Description: LOG_ID_IPS_LIC_EXPIRE

Message Meaning: FortiGuard IPS license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20107 - LOG_ID_LOG_UPLOAD_ERR

Message ID: 20107

Message Description: LOG_ID_LOG_UPLOAD_ERR

Message Meaning: Log upload error

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
port	Port Number	uint16	5
server	Server IP Address	string	64
error	Error Reason for Log Upload to Forticloud	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20108 - LOG_ID_LOG_UPLOAD_DONE

Message ID: 20108

Message Description: LOG_ID_LOG_UPLOAD_DONE

Message Meaning: Log upload completed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20109 - LOG_ID_WEB_LIC_EXPIRED

Message ID: 20109

Message Description: LOG_ID_WEB_LIC_EXPIRED

Message Meaning: FortiGuard web filter license expired

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20113 - LOG_ID_IPSA_DOWNLOAD_FAIL

Message ID: 20113

Message Description: LOG_ID_IPSA_DOWNLOAD_FAIL

Message Meaning: IPSA database download failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20114 - LOG_ID_IPSA_SELFTEST_FAIL

Message ID: 20114

Message Description: LOG_ID_IPSA_SELFTEST_FAIL

Message Meaning: IPSA disabled: self test failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20115 - LOG_ID_IPSA_STATUSUPD_FAIL

Message ID: 20115

Message Description: LOG_ID_IPSA_STATUSUPD_FAIL

Message Meaning: IPSA driver update failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20116 - LOG_ID_SPAM_LIC_EXPIRED

Message ID: 20116

Message Description: LOG_ID_SPAM_LIC_EXPIRED

Message Meaning: FortiGuard antispam license expired

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20117 - LOG_ID_AV_LIC_EXPIRED

Message ID: 20117

Message Description: LOG_ID_AV_LIC_EXPIRED

Message Meaning: FortiGuard antivirus license expired

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20118 - LOG_ID_WEBF_STATUS_REACH

Message ID: 20118

Message Description: LOG_ID_WEBF_STATUS_REACH

Message Meaning: FortiGuard webfilter reachable

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20119 - LOG_ID_WEBF_STATUS_UNREACH

Message ID: 20119

Message Description: LOG_ID_WEBF_STATUS_UNREACH

Message Meaning: FortiGuard webfilter unreachable

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20120 - LOG_ID_FMGC_LIC_EXPIRE

Message ID: 20120

Message Description: LOG_ID_FMGC_LIC_EXPIRE

Message Meaning: FortiManager Cloud license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20121 - LOG_ID_FAZC_LIC_EXPIRE

Message ID: 20121

Message Description: LOG_ID_FAZC_LIC_EXPIRE

Message Meaning: FortiAnalyzer Cloud license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20122 - LOG_ID_SWNO_LIC_EXPIRE

Message ID: 20122

Message Description: LOG_ID_SWNO_LIC_EXPIRE

Message Meaning: SD-WAN Overlay Controller license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20123 - LOG_ID_SWNM_LIC_EXPIRE

Message ID: 20123

Message Description: LOG_ID_SWNM_LIC_EXPIRE

Message Meaning: SD-WAN Monitoring license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20124 - LOG_ID_VMLS_LIC_EXPIRE

Message ID: 20124

Message Description: LOG_ID_VMLS_LIC_EXPIRE

Message Meaning: VM-S license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20125 - LOG_ID_SFAS_LIC_EXPIRE

Message ID: 20125

Message Description: LOG_ID_SFAS_LIC_EXPIRE

Message Meaning: Security Rating license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20126 - LOG_ID_IPMC_LIC_EXPIRE

Message ID: 20126

Message Description: LOG_ID_IPMC_LIC_EXPIRE

Message Meaning: IPAM Controller license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20127 - LOG_ID_IOTH_LIC_EXPIRE

Message ID: 20127

Message Description: LOG_ID_IOTH_LIC_EXPIRE

Message Meaning: IoT device identification license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20128 - LOG_ID_FSAC_LIC_EXPIRE

Message ID: 20128

Message Description: LOG_ID_FSAC_LIC_EXPIRE

Message Meaning: FortiSandbox Cloud license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20129 - LOG_ID_AFAC_LIC_EXPIRE

Message ID: 20129

Message Description: LOG_ID_AFAC_LIC_EXPIRE

Message Meaning: FortiAnalyzer Cloud premium license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20130 - LOG_ID_EMSC_ACC_LIC_EXPIRE

Message ID: 20130

Message Description: LOG_ID_EMSC_ACC_LIC_EXPIRE

Message Meaning: FortiClient EMS Cloud license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20131 - LOG_ID_FMGC_ACC_LIC_EXPIRE

Message ID: 20131

Message Description: LOG_ID_FMGC_ACC_LIC_EXPIRE

Message Meaning: FortiManager Cloud Account Level license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20132 - LOG_ID_FSAP_ACC_LIC_EXPIRE

Message ID: 20132

Message Description: LOG_ID_FSAP_ACC_LIC_EXPIRE

Message Meaning: FortiSandbox Cloud Account Level license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

20133 - LOG_ID_FIREWALL_POLICY_EXPIRE

Message ID: 20133

Message Description: LOG_ID_FIREWALL_POLICY_EXPIRE

Message Meaning: Firewall policy expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20134 - LOG_ID_FIREWALL_POLICY_EXPIRED

Message ID: 20134

Message Description: LOG_ID_FIREWALL_POLICY_EXPIRED

Message Meaning: Firewall policy expired

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20135 - LOG_ID_FAIS_LIC_EXPIRE

Message ID: 20135

Message Description: LOG_ID_FAIS_LIC_EXPIRE

Message Meaning: FortiGuard AI-Based Sandbox Service license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20136 - LOG_ID_DLP_LIC_EXPIRE

Message ID: 20136

Message Description: LOG_ID_DLP_LIC_EXPIRE

Message Meaning: FortiGuard Data loss prevention (DLP) server license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20137 - LOG_ID_FGSA_LIC_EXPIRE

Message ID: 20137

Message Description: LOG_ID_FGSA_LIC_EXPIRE

Message Meaning: Attack Surface Security Rating Service license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20138 - LOG_ID_SWOS_LIC_EXPIRE

Message ID: 20138

Message Description: LOG_ID_SWOS_LIC_EXPIRE

Message Meaning: FortiGuard SD-WAN Overlay as a Service license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20139 - LOG_ID_FGCS_ACC_LIC_EXPIRE

Message ID: 20139

Message Description: LOG_ID_FGCS_ACC_LIC_EXPIRE

Message Meaning: FortiGSLB Cloud Account Level license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20140 - LOG_ID_FSPA_LIC_EXPIRE

Message ID: 20140

Message Description: LOG_ID_FSPA_LIC_EXPIRE

Message Meaning: FortiSASE Secure Private Access license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20141 - LOG_ID_FSFG_LIC_EXPIRE

Message ID: 20141

Message Description: LOG_ID_FSFG_LIC_EXPIRE

Message Meaning: FortiSASE LAN Extension license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20150 - LOG_ID_DEV_VUNL_FTGD_LOOKUP

Message ID: 20150

Message Description: LOG_ID_DEV_VUNL_FTGD_LOOKUP

Message Meaning: Device vulnerability lookup on FortiGuard

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
vulncnt		uint32	10
vulnresult		string	64
versionmax		string	64
versionmin		string	64
model		string	64
product		string	64
vendor		string	64
ip		ip	39
mac	MAC Address	string	17
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20200 - LOG_ID_FIPS_SELF_TEST

Message ID: 20200

Message Description: LOG_ID_FIPS_SELF_TEST

Message Meaning: FIPS CC self-test initiated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20201 - LOG_ID_FIPS_SELF_ALL_TEST

Message ID: 20201

Message Description: LOG_ID_FIPS_SELF_ALL_TEST

Message Meaning: FIPS ALL CC self-tests initiated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20202 - LOG_ID_DISK_FORMAT_ERROR

Message ID: 20202

Message Description: LOG_ID_DISK_FORMAT_ERROR

Message Meaning: Disk partitioning or formatting Error

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20203 - LOG_ID_DAEMON_SHUTDOWN

Message ID: 20203

Message Description: LOG_ID_DAEMON_SHUTDOWN

Message Meaning: Daemon shutdown

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
pid	Process ID	uint32	10
daemon	Daemon Name	string	32
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20204 - LOG_ID_DAEMON_START

Message ID: 20204

Message Description: LOG_ID_DAEMON_START

Message Meaning: Daemon started

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
pid	Process ID	uint32	10
daemon	Daemon Name	string	32
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20205 - LOG_ID_DISK_FORMAT_REQ

Message ID: 20205

Message Description: LOG_ID_DISK_FORMAT_REQ

Message Meaning: Format disk requested

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20206 - LOG_ID_DISK_SCAN_REQ

Message ID: 20206

Message Description: LOG_ID_DISK_SCAN_REQ

Message Meaning: Scan disk requested

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20207 - LOG_ID_RAD_MISMATCH_VALID_TIME

Message ID: 20207

Message Description: LOG_ID_RAD_MISMATCH_VALID_TIME

Message Meaning: RADVD local AdvValidLifetime disagrees with remote site

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20208 - LOG_ID_ZOMBIE_DAEMON_CLEANUP

Message ID: 20208

Message Description: LOG_ID_ZOMBIE_DAEMON_CLEANUP

Message Meaning: Zombie daemon cleanup

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
pid	Process ID	uint32	10
daemon	Daemon Name	string	32
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20209 - LOG_ID_DISK_UNAVAIL

Message ID: 20209

Message Description: LOG_ID_DISK_UNAVAIL

Message Meaning: Disk unavailable

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20210 - LOG_ID_DISK_TRIM_START

Message ID: 20210

Message Description: LOG_ID_DISK_TRIM_START

Message Meaning: SSD TRIM started

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20211 - LOG_ID_DISK_TRIM_END

Message ID: 20211

Message Description: LOG_ID_DISK_TRIM_END

Message Meaning: SSD TRIM finished

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20212 - LOG_ID_DISK_SCAN_NEEDED

Message ID: 20212

Message Description: LOG_ID_DISK_SCAN_NEEDED

Message Meaning: Disk scan is needed

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20213 - LOG_ID_DISK_LOG_CORRUPTED

Message ID: 20213

Message Description: LOG_ID_DISK_LOG_CORRUPTED

Message Meaning: Log file on disk is corrupted

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20214 - LOG_ID_LOCAL_OUT_IOC

Message ID: 20214

Message Description: LOG_ID_LOCAL_OUT_IOC

Message Meaning: Locally generated traffic goes to IoC location

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
session_id	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
proto	Protocol Number	uint8	3
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20220 - LOGID_EVENT_SHAPER_OUTBOUND_MAXED_OUT

Message ID: 20220

Message Description: LOGID_EVENT_SHAPER_OUTBOUND_MAXED_OUT

Message Meaning: Outbound bandwidth rate exceeded

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
limit	Virtual Domain Resource Limit	uint32	10
intf	Interface	string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20221 - LOGID_EVENT_SHAPER_INBOUND_MAXED_OUT

Message ID: 20221

Message Description: LOGID_EVENT_SHAPER_INBOUND_MAXED_OUT

Message Meaning: Inbound bandwidth rate exceeded

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
limit	Virtual Domain Resource Limit	uint32	10
intf	Interface	string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20230 - LOG_ID_SYS_SECURITY_WRITE_VIOLATION

Message ID: 20230

Message Description: LOG_ID_SYS_SECURITY_WRITE_VIOLATION

Message Meaning: Write Permission Violation

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20231 - LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION

Message ID: 20231

Message Description: LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION

Message Meaning: Hard Link Creation Violation

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20232 - LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION

Message ID: 20232

Message Description: LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION

Message Meaning: Load Kernel/Kernel Module/Firmware Violation

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20233 - LOG_ID_SYS_SECURITY_FILE_HASH_MISSING

Message ID: 20233

Message Description: LOG_ID_SYS_SECURITY_FILE_HASH_MISSING

Message Meaning: Integrity check of Running/loading Executable File failed without Integrity measure

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
severity		string	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20234 - LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH

Message ID: 20234

Message Description: LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH

Message Meaning: Integrity check of Running/loading Executable File failed with mismatched measure

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
severity		string	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20235 - LOG_ID_SYS_SECURITY_MOUNT_VIOLATION

Message ID: 20235

Message Description: LOG_ID_SYS_SECURITY_MOUNT_VIOLATION

Message Meaning: Filesystem Mount Violation

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20300 - LOG_ID_BGP_NB_STAT_CHG

Message ID: 20300

Message Description: LOG_ID_BGP_NB_STAT_CHG

Message Meaning: BGP neighbor status changed

Type: Event

Category: router

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20301 - LOG_ID_VZ_LOG_INFO

Message ID: 20301

Message Description: LOG_ID_VZ_LOG_INFO

Message Meaning: Routing log information

Type: Event

Category: router

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20302 - LOG_ID_OSPF_NB_STAT_CHG

Message ID: 20302

Message Description: LOG_ID_OSPF_NB_STAT_CHG

Message Meaning: OSPF neighbor status changed

Type: Event

Category: router

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20303 - LOG_ID_OSPF6_NB_STAT_CHG

Message ID: 20303

Message Description: LOG_ID_OSPF6_NB_STAT_CHG

Message Meaning: OSPF6 neighbor status changed

Type: Event

Category: router

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20304 - LOG_ID_VZ_LOG_WARNING

Message ID: 20304

Message Description: LOG_ID_VZ_LOG_WARNING

Message Meaning: Routing log warning

Type: Event

Category: router

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20305 - LOG_ID_VZ_LOG_CRITICAL

Message ID: 20305

Message Description: LOG_ID_VZ_LOG_CRITICAL

Message Meaning: Routing log critical event

Type: Event

Category: router

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20306 - LOG_ID_VZ_LOG_ERROR

Message ID: 20306

Message Description: LOG_ID_VZ_LOG_ERROR

Message Meaning: Routing log error

Type: Event

Category: router

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

20401 - LOG_ID_ROUTER_CLEAR

Message ID: 20401

Message Description: LOG_ID_ROUTER_CLEAR

Message Meaning: Router cleared

Type: Event

Category: router

Severity: Notice

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22000 - LOG_ID_INV_PKT_LEN

Message ID: 22000

Message Description: LOG_ID_INV_PKT_LEN

Message Meaning: Packet length mismatch

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22001 - LOG_ID_UNSUPPORTED_PROT_VER

Message ID: 22001

Message Description: LOG_ID_UNSUPPORTED_PROT_VER

Message Meaning: Protocol version unsupported

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22002 - LOG_ID_INV_REQ_TYPE

Message ID: 22002

Message Description: LOG_ID_INV_REQ_TYPE

Message Meaning: Request type not supported

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22003 - LOG_ID_FAIL_SET_SIG_HANDLER

Message ID: 22003

Message Description: LOG_ID_FAIL_SET_SIG_HANDLER

Message Meaning: Signal handler setup failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22004 - LOG_ID_FAIL_CREATE_SOCKET

Message ID: 22004

Message Description: LOG_ID_FAIL_CREATE_SOCKET

Message Meaning: Socket creation failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22005 - LOG_ID_FAIL_CREATE_SOCKET_RETRY

Message ID: 22005

Message Description: LOG_ID_FAIL_CREATE_SOCKET_RETRY

Message Meaning: Socket creation retry failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22006 - LOG_ID_FAIL_REG_CMDB_EVENT

Message ID: 22006

Message Description: LOG_ID_FAIL_REG_CMDB_EVENT

Message Meaning: Registration for CMDB events failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22009 - LOG_ID_FAIL_FIND_AV_PROFILE

Message ID: 22009

Message Description: LOG_ID_FAIL_FIND_AV_PROFILE

Message Meaning: AntiVirus profile not found

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22010 - LOG_ID_SENDTO_FAIL

Message ID: 22010

Message Description: LOG_ID_SENDTO_FAIL

Message Meaning: URL filter packet send failure

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
process	Process	string	4096
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22011 - LOG_ID_ENTER_MEM_CONSERVE_MODE

Message ID: 22011

Message Description: LOG_ID_ENTER_MEM_CONSERVE_MODE

Message Meaning: Memory conserve mode entered

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
green	Green threshold for conserve mode	string	32
red		string	32
used	Number of Used IPs	uint32	10
total	Total	uint32	10
conserve	Flag for Conserve Mode	string	32
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22012 - LOG_ID_LEAVE_MEM_CONSERVE_MODE

Message ID: 22012

Message Description: LOG_ID_LEAVE_MEM_CONSERVE_MODE

Message Meaning: Memory conserve mode exited

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
green	Green threshold for conserve mode	string	32
red		string	32
used	Number of Used IPs	uint32	10
total	Total	uint32	10
conserve	Flag for Conserve Mode	string	32
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22013 - LOG_ID_IPPOOLPBA_BLOCK_EXHAUSTED

Message ID: 22013

Message Description: LOG_ID_IPPOOLPBA_BLOCK_EXHAUSTED

Message Meaning: IP pool PBA block exhausted

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36
saddr	Source Address IP	string	80
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22014 - LOG_ID_IPPOOLPBA_NATIP_EXHAUSTED

Message ID: 22014

Message Description: LOG_ID_IPPOOLPBA_NATIP_EXHAUSTED

Message Meaning: IP pool PBA NAT IP exhausted

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36
saddr	Source Address IP	string	80
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22015 - LOG_ID_IPPOOLPBA_CREATE

Message ID: 22015

Message Description: LOG_ID_IPPOOLPBA_CREATE

Message Meaning: IP pool PBA created

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
authserver		string	64
portend	Port Number to End	uint16	5

Log Field Name	Description	Data Type	Length
portbegin	Port Number to Begin	uint16	5
poolname	IP Pool Name	string	36
saddr	Source Address IP	string	80
nat	NAT IP Address	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22016 - LOG_ID_IPPOOLPBA_DEALLOCATE

Message ID: 22016

Message Description: LOG_ID_IPPOOLPBA_DEALLOCATE

Message Meaning: Deallocate IP pool PBA

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
portend	Port Number to End	uint16	5
portbegin	Port Number to Begin	uint16	5

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36
saddr	Source Address IP	string	80
nat	NAT IP Address	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22017 - LOG_ID_EXCEED_GLOB_RES_LIMIT

Message ID: 22017

Message Description: LOG_ID_EXCEED_GLOB_RES_LIMIT

Message Meaning: Global resource limit exceeded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22018 - LOG_ID_EXCEED_VD_RES_LIMIT

Message ID: 22018

Message Description: LOG_ID_EXCEED_VD_RES_LIMIT

Message Meaning: VDOM resource limit exceeded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22019 - LOG_ID_LOGRATE_OVER_LIMIT

Message ID: 22019

Message Description: LOG_ID_LOGRATE_OVER_LIMIT

Message Meaning: Log rate limit exceeded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22020 - LOG_ID_FAIL_CREATE_HA_SOCKET

Message ID: 22020

Message Description: LOG_ID_FAIL_CREATE_HA_SOCKET

Message Meaning: HA socket creation failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22021 - LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY

Message ID: 22021

Message Description: LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY

Message Meaning: UDP socket creation to relay URL request failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22022 - LOG_ID_ENTER_EXTREME_LOW_MEM_MODE

Message ID: 22022

Message Description: LOG_ID_ENTER_EXTREME_LOW_MEM_MODE

Message Meaning: Extreme low memory mode entered

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22023 - LOG_ID_LEAVE_EXTREME_LOW_MEM_MODE

Message ID: 22023

Message Description: LOG_ID_LEAVE_EXTREME_LOW_MEM_MODE

Message Meaning: Extreme low memory mode exited

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22024 - LOG_ID_IPPOOLPBA_INTERIM

Message ID: 22024

Message Description: LOG_ID_IPPOOLPBA_INTERIM

Message Meaning: IP pool PBA interim log

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
portend	Port Number to End	uint16	5
portbegin	Port Number to Begin	uint16	5
poolname	IP Pool Name	string	36
saddr	Source Address IP	string	80
nat	NAT IP Address	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22031 - LOG_ID_SUCCESS_CSF_LOG_SYNC_CONFIG_CHANGED

Message ID: 22031

Message Description: LOG_ID_SUCCESS_CSF_LOG_SYNC_CONFIG_CHANGED

Message Meaning: Settings modified by Security Fabric service

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22032 - LOG_ID_CSF_LOOP_FOUND

Message ID: 22032

Message Description: LOG_ID_CSF_LOOP_FOUND

Message Meaning: Looped configuration in Security Fabric service

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
path		string	512
sn	Serial Number	string	64
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22035 - LOG_ID_CSF_UPSTREAM_SN_CHANGED

Message ID: 22035

Message Description: LOG_ID_CSF_UPSTREAM_SN_CHANGED

Message Meaning: Serial number of upstream is changed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
oldsn	Security fabric upstream FGT old serial number	string	64
sn	Serial Number	string	64
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22036 - LOG_ID_CSF_FGT_CONNECTED

Message ID: 22036

Message Description: LOG_ID_CSF_FGT_CONNECTED

Message Meaning: Connection with Security Fabric member established and authorized.

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
direction		string	16
sn	Serial Number	string	64
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22037 - LOG_ID_CSF_FGT_DISCONNECTED

Message ID: 22037

Message Description: LOG_ID_CSF_FGT_DISCONNECTED

Message Meaning: Connection with authorized Security Fabric member terminated.

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
direction		string	16
sn	Serial Number	string	64
reason	Reason	string	256
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22038 - LOG_ID_CSF_GLOBAL_SYNC_FAILED

Message ID: 22038

Message Description: LOG_ID_CSF_GLOBAL_SYNC_FAILED

Message Meaning: Synchronization of global object failed.

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
path		string	512
sn	Serial Number	string	64
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22039 - LOG_ID_CSF_GLOBAL_SYNC_REPORT

Message ID: 22039

Message Description: LOG_ID_CSF_GLOBAL_SYNC_REPORT

Message Meaning: Synchronization of global object report.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
path		string	512
sn	Serial Number	string	64
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22040 - LOG_ID_CSF_DEVICE_JOIN

Message ID: 22040

Message Description: LOG_ID_CSF_DEVICE_JOIN

Message Meaning: Device joined the Security Fabric.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
scope		string	16
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22041 - LOG_ID_CSF_DEVICE_LEAVE

Message ID: 22041

Message Description: LOG_ID_CSF_DEVICE_LEAVE

Message Meaning: Device left the Security Fabric.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
scope		string	16
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22042 - LOG_ID_CSF_DEVICE_UPDATE

Message ID: 22042

Message Description: LOG_ID_CSF_DEVICE_UPDATE

Message Meaning: Device in the Security Fabric was updated.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
scope		string	16
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22043 - LOG_ID_CSF_NEW_AUTH_REQ

Message ID: 22043

Message Description: LOG_ID_CSF_NEW_AUTH_REQ

Message Meaning: An authorization request was added.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22044 - LOG_ID_CSF_UPDATE_AUTH_REQ

Message ID: 22044

Message Description: LOG_ID_CSF_UPDATE_AUTH_REQ

Message Meaning: An authorization request was updated.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22045 - LOG_ID_CSF_REMOVE_AUTH_REQ

Message ID: 22045

Message Description: LOG_ID_CSF_REMOVE_AUTH_REQ

Message Meaning: An authorization request was removed.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22046 - LOG_ID_CSF_ROLE_CHANGE

Message ID: 22046

Message Description: LOG_ID_CSF_ROLE_CHANGE

Message Meaning: Device's authorization privilege changed.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
desc	Description	string	128
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22047 - LOG_ID_CSF_FILE_MEM_USAGE

Message ID: 22047

Message Description: LOG_ID_CSF_FILE_MEM_USAGE

Message Meaning: CSF daemon files memory usage warning.

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22048 - LOG_ID_CSF_ADVPN_SYNC

Message ID: 22048

Message Description: LOG_ID_CSF_ADVPN_SYNC

Message Meaning: Fabric ADVPN configuration synchronized from root.

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22049 - LOG_ID_CSF_DAEMON_CLOSE

Message ID: 22049

Message Description: LOG_ID_CSF_DAEMON_CLOSE

Message Meaning: Daemon csfd has closed.

Type: Event

Category: system

Severity: Debug

Log Field Name	Description	Data Type	Length
desc	Description	string	128
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22050 - LOG_ID_IPAMD_ADDRESS_ALLOCATED

Message ID: 22050

Message Description: LOG_ID_IPAMD_ADDRESS_ALLOCATED

Message Meaning: Address allocated by FortiIPAM and applied to an interface

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22051 - LOG_ID_IPAMD_ADDRESS_SET_FAILED

Message ID: 22051

Message Description: LOG_ID_IPAMD_ADDRESS_SET_FAILED

Message Meaning: Address received from FortiIPAM could not be applied to the interface

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22052 - LOG_ID_IPAMD_ADDRESS_INVALIDATED

Message ID: 22052

Message Description: LOG_ID_IPAMD_ADDRESS_INVALIDATED

Message Meaning: FortiIPAM indicated that the address was no longer allocated to the interface

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22053 - LOG_ID_IPAMD_VALIDATION_COMPLETE

Message ID: 22053

Message Description: LOG_ID_IPAMD_VALIDATION_COMPLETE

Message Meaning: Startup validation of IPAM addresses was completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22060 - LOG_ID_IPAMSD_ADD_ENTRY

Message ID: 22060

Message Description: LOG_ID_IPAMSD_ADD_ENTRY

Message Meaning: Add new entry to IPAM

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22061 - LOG_ID_IPAMSD_DELETE_ENTRY

Message ID: 22061

Message Description: LOG_ID_IPAMSD_DELETE_ENTRY

Message Meaning: Delete entry from IPAM

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22062 - LOG_ID_IPAMSD_FLAG_CONFLICT

Message ID: 22062

Message Description: LOG_ID_IPAMSD_FLAG_CONFLICT

Message Meaning: Flag IPAM entry as conflict

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22063 - LOG_ID_IPAMSD_UNFLAG_CONFLICT

Message ID: 22063

Message Description: LOG_ID_IPAMSD_UNFLAG_CONFLICT

Message Meaning: Unflag IPAM entry as conflict

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22070 - LOG_ID_FORTIGSLB_COMMUNICATION_ERROR

Message ID: 22070

Message Description: LOG_ID_FORTIGSLB_COMMUNICATION_ERROR

Message Meaning: Error communicating with the FortiGSLB cloud server

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
error_num		string	53
requesttype		string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22071 - LOG_ID_FORTIGSLB_CLOUD_CONFIG_UPDATED

Message ID: 22071

Message Description: LOG_ID_FORTIGSLB_CLOUD_CONFIG_UPDATED

Message Meaning: Config successfully sent to the FortiGSLB cloud server

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22080 - LOG_ID_PROVISION_LATEST_SUCCEEDED

Message ID: 22080

Message Description: LOG_ID_PROVISION_LATEST_SUCCEEDED

Message Meaning: Provisioning of latest firmware was completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
upgradedevice		string	80

Log Field Name	Description	Data Type	Length
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22081 - LOG_ID_PROVISION_LATEST_FAILED

Message ID: 22081

Message Description: LOG_ID_PROVISION_LATEST_FAILED

Message Meaning: Provisioning of latest firmware failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
upgradedevice		string	80
version	Version	string	64
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22085 - LOG_ID_DEVICE_UPGRADE_SUCCEEDED

Message ID: 22085

Message Description: LOG_ID_DEVICE_UPGRADE_SUCCEEDED

Message Meaning: A device upgrade was completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
upgradedevice		string	80
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22086 - LOG_ID_DEVICE_UPGRADE_FAILED

Message ID: 22086

Message Description: LOG_ID_DEVICE_UPGRADE_FAILED

Message Meaning: A device upgrade failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
upgradedevice		string	80
version	Version	string	64
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22090 - LOG_ID_FEDERATED_UPGRADE_CANCELLED

Message ID: 22090

Message Description: LOG_ID_FEDERATED_UPGRADE_CANCELLED

Message Meaning: A federated upgrade was cancelled due to the CSF tree not being ready

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
failuredev		string	80
localdevcount		uint32	5
version	Version	string	64
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22091 - LOG_ID_FEDERATED_UPGRADE_SUCCEEDED

Message ID: 22091

Message Description: LOG_ID_FEDERATED_UPGRADE_SUCCEEDED

Message Meaning: A federated upgrade was completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
localdevcount		uint32	5
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22092 - LOG_ID_FEDERATED_UPGRADE_FAILED

Message ID: 22092

Message Description: LOG_ID_FEDERATED_UPGRADE_FAILED

Message Meaning: A federated upgrade failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
failuredev		string	80
localdevcount		uint32	5
version	Version	string	64
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22093 - LOG_ID_FEDERATED_UPGRADE_STEP_COMPLETE

Message ID: 22093

Message Description: LOG_ID_FEDERATED_UPGRADE_STEP_COMPLETE

Message Meaning: A step in a multi-step federated upgrade was completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22094 - LOG_ID_FEDERATED_UPGRADE_ROOT_COMPLETED

Message ID: 22094

Message Description: LOG_ID_FEDERATED_UPGRADE_ROOT_COMPLETED

Message Meaning: A federated upgrade was completed by the root FortiGate

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22095 - LOG_ID_FEDERATED_UPGRADE_ROOT_NOT_COMPLETED

Message ID: 22095

Message Description: LOG_ID_FEDERATED_UPGRADE_ROOT_NOT_COMPLETED

Message Meaning: A federated upgrade could not be completed by the root FortiGate

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
failuredev		string	80
version	Version	string	64

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22100 - LOG_ID_QUAR_DROP_TRAN_JOB

Message ID: 22100

Message Description: LOG_ID_QUAR_DROP_TRAN_JOB

Message Meaning: Files dropped by quarantine daemon

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
fams_pause	Fortinet Analysis and Management Service Pause	uint32	10
duration	Duration	uint32	10
used	Number of Used IPs	uint32	10
reason	Reason	string	256
limit	Virtual Domain Resource Limit	uint32	10
count	Count	uint32	10
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22101 - LOG_ID_QUAR_DROP_TLL_JOB

Message ID: 22101

Message Description: LOG_ID_QUAR_DROP_TLL_JOB

Message Meaning: Files dropped due to poor network connection

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
count	Count	uint32	10
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22102 - LOG_ID_LOG_DISK_FAILURE

Message ID: 22102

Message Description: LOG_ID_LOG_DISK_FAILURE

Message Meaning: Log disk failure imminent

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22103 - LOG_ID_QUAR_LIMIT_REACHED

Message ID: 22103

Message Description: LOG_ID_QUAR_LIMIT_REACHED

Message Meaning: Sandbox limit reached

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
limit	Virtual Domain Resource Limit	uint32	10
count	Count	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22105 - LOG_ID_POWER_FAILURE

Message ID: 22105

Message Description: LOG_ID_POWER_FAILURE

Message Meaning: Power supply failed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22106 - LOG_ID_POWER_OPTIONAL_NOT_DETECTED

Message ID: 22106

Message Description: LOG_ID_POWER_OPTIONAL_NOT_DETECTED

Message Meaning: Optional power supply not detected

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22107 - LOG_ID_VOLT_ANOM

Message ID: 22107

Message Description: LOG_ID_VOLT_ANOM

Message Meaning: Voltage anomaly

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22108 - LOG_ID_FAN_ANOM

Message ID: 22108

Message Description: LOG_ID_FAN_ANOM

Message Meaning: Fan anomaly

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22109 - LOG_ID_TEMP_TOO_HIGH

Message ID: 22109

Message Description: LOG_ID_TEMP_TOO_HIGH

Message Meaning: Temperature too high

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22110 - LOG_ID_SPARE_BLOCK_LOW

Message ID: 22110

Message Description: LOG_ID_SPARE_BLOCK_LOW

Message Meaning: Spare blocks availability low

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22111 - LOG_ID_PSU_ACTION_FPC_DOWN

Message ID: 22111

Message Description: LOG_ID_PSU_ACTION_FPC_DOWN

Message Meaning: FPC down due to PSU action

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22112 - LOG_ID_PSU_ACTION_FPC_UP

Message ID: 22112

Message Description: LOG_ID_PSU_ACTION_FPC_UP

Message Meaning: FPC up due to PSU action

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22113 - LOG_ID_FNBAM_FAILURE

Message ID: 22113

Message Description: LOG_ID_FNBAM_FAILURE

Message Meaning: Authentication error

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22114 - LOG_ID_POWER_FAILURE_WARNING

Message ID: 22114

Message Description: LOG_ID_POWER_FAILURE_WARNING

Message Meaning: Power supply failed warning

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22115 - LOG_ID_POWER_RESTORE_NOTIF

Message ID: 22115

Message Description: LOG_ID_POWER_RESTORE_NOTIF

Message Meaning: Power supply restored notification

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22116 - LOG_ID_POWER_REDUNDANCY_DEGRADE

Message ID: 22116

Message Description: LOG_ID_POWER_REDUNDANCY_DEGRADE

Message Meaning: Power Supply Redundancy Degrade

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22117 - LOG_ID_POWER_REDUNDANCY_FAILURE

Message ID: 22117

Message Description: LOG_ID_POWER_REDUNDANCY_FAILURE

Message Meaning: Power Supply Redundancy Lost

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22118 - LOG_ID_HW_MONITOR_EMERGENCY

Message ID: 22118

Message Description: LOG_ID_HW_MONITOR_EMERGENCY

Message Meaning: IPMC monitor emergency

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22119 - LOG_ID_HW_MONITOR_WARNING

Message ID: 22119

Message Description: LOG_ID_HW_MONITOR_WARNING

Message Meaning: IPMC monitor warning

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22120 - LOG_ID_HW_MONITOR_NOTIF

Message ID: 22120

Message Description: LOG_ID_HW_MONITOR_NOTIF

Message Meaning: IPMC monitor notification

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22150 - LOG_ID_VOLT_NOM

Message ID: 22150

Message Description: LOG_ID_VOLT_NOM

Message Meaning: Voltage normal

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22151 - LOG_ID_FAN_NOM

Message ID: 22151

Message Description: LOG_ID_FAN_NOM

Message Meaning: Fan normal

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22152 - LOG_ID_TEMP_TOO_LOW

Message ID: 22152

Message Description: LOG_ID_TEMP_TOO_LOW

Message Meaning: Temperature too low

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22153 - LOG_ID_TEMP_NORM

Message ID: 22153

Message Description: LOG_ID_TEMP_NORM

Message Meaning: Temperature normal

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22200 - LOG_ID_AUTO_UPT_CERT

Message ID: 22200

Message Description: LOG_ID_AUTO_UPT_CERT

Message Meaning: Certificate will be auto-updated

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
cert	Certificate	string	36
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22201 - LOG_ID_AUTO_GEN_CERT

Message ID: 22201

Message Description: LOG_ID_AUTO_GEN_CERT

Message Meaning: Certificate will be auto-regenerated

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
cert	Certificate	string	36
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22203 - LOG_ID_AUTO_GEN_CERT_FAIL

Message ID: 22203

Message Description: LOG_ID_AUTO_GEN_CERT_FAIL

Message Meaning: Certificate failed to auto-generate

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22204 - LOG_ID_AUTO_GEN_CERT_PENDING

Message ID: 22204

Message Description: LOG_ID_AUTO_GEN_CERT_PENDING

Message Meaning: Certificate pending to auto-generate

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22205 - LOG_ID_AUTO_GEN_CERT_SUCC

Message ID: 22205

Message Description: LOG_ID_AUTO_GEN_CERT_SUCC

Message Meaning: Certificate succeed to auto-generate

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22206 - LOG_ID_CRL_EXPIRED

Message ID: 22206

Message Description: LOG_ID_CRL_EXPIRED

Message Meaning: CRL is expired

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22207 - LOG_ID_CERT_EXPIRE_WARNING

Message ID: 22207

Message Description: LOG_ID_CERT_EXPIRE_WARNING

Message Meaning: Certificate will expire soon

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
cert	Certificate	string	36
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22220 - LOG_ID_EXT_RESOURCE

Message ID: 22220

Message Description: LOG_ID_EXT_RESOURCE

Message Meaning: Threat feed updated

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
desc	Description	string	128
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22221 - LOG_ID_EXT_RESOURCE_FAIL

Message ID: 22221

Message Description: LOG_ID_EXT_RESOURCE_FAIL

Message Meaning: Threat feed update failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
desc	Description	string	128
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22222 - LOG_ID_EXT_RESOURCE_LOAD

Message ID: 22222

Message Description: LOG_ID_EXT_RESOURCE_LOAD

Message Meaning: Threat feed loaded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
new_status	New Status	string	512
informationsource	Information Source	string	4096
desc	Description	string	128
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22223 - LOG_ID_EXT_RESOURCE_DEBUG

Message ID: 22223

Message Description: LOG_ID_EXT_RESOURCE_DEBUG

Message Meaning: Threat feed debug

Type: Event

Category: system

Severity: Debug

Log Field Name	Description	Data Type	Length
old_status	Original Status	string	512
host		string	256
hostname	Hostname	string	128
profile	Profile Name	string	64
informationsource	Information Source	string	4096
desc	Description	string	128
path		string	512
dstport	Destination Protocol Port	uint16	5
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22224 - LOG_ID_EXT_RESOURCE_OVERFLOW

Message ID: 22224

Message Description: LOG_ID_EXT_RESOURCE_OVERFLOW

Message Meaning: Threat feed overflow

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22700 - LOG_ID_IPS_FAIL_OPEN

Message ID: 22700

Message Description: LOG_ID_IPS_FAIL_OPEN

Message Meaning: IPS session scan paused

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22701 - LOG_ID_IPS_FAIL_OPEN_END

Message ID: 22701

Message Description: LOG_ID_IPS_FAIL_OPEN_END

Message Meaning: IPS session scan resumed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22750 - LOG_ID_METERED_BILLING_ACCEPTED

Message ID: 22750

Message Description: LOG_ID_METERED_BILLING_ACCEPTED

Message Meaning: Metered billing usage event accepted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22751 - LOG_ID_METERED_BILLING_FAIL

Message ID: 22751

Message Description: LOG_ID_METERED_BILLING_FAIL

Message Meaning: Metered billing usage event bad reuest

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22752 - LOG_ID_METERED_BILLING_VALID

Message ID: 22752

Message Description: LOG_ID_METERED_BILLING_VALID

Message Meaning: Metered billing status is valid

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22753 - LOG_ID_METERED_BILLING_INVALID

Message ID: 22753

Message Description: LOG_ID_METERED_BILLING_INVALID

Message Meaning: Metered billing status is invalid

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22800 - LOG_ID_SCAN_SERV_FAIL

Message ID: 22800

Message Description: LOG_ID_SCAN_SERV_FAIL

Message Meaning: Scan services session failed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
mode	Mode	string	32
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22802 - LOG_ID_ENTER_FD_CONSERVE_MODE

Message ID: 22802

Message Description: LOG_ID_ENTER_FD_CONSERVE_MODE

Message Meaning: File descriptor conserve mode entered

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
green	Green threshold for conserve mode	string	32
red		string	32
used	Number of Used IPs	uint32	10
total	Total	uint32	10
conserve	Flag for Conserve Mode	string	32
daemon	Daemon Name	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22803 - LOG_ID_LEAVE_FD_CONSERVE_MODE

Message ID: 22803

Message Description: LOG_ID_LEAVE_FD_CONSERVE_MODE

Message Meaning: File descriptor conserve mode exited

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
green	Green threshold for conserve mode	string	32
red		string	32
used	Number of Used IPs	uint32	10
total	Total	uint32	10
conserve	Flag for Conserve Mode	string	32
daemon	Daemon Name	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22804 - LOG_ID_LIC_STATUS_CHG

Message ID: 22804

Message Description: LOG_ID_LIC_STATUS_CHG

Message Meaning: License status changed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22805 - LOG_ID_FAIL_TO_VALIDATE_LIC

Message ID: 22805

Message Description: LOG_ID_FAIL_TO_VALIDATE_LIC

Message Meaning: License validation failure

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22806 - LOG_ID_DUP_LIC

Message ID: 22806

Message Description: LOG_ID_DUP_LIC

Message Meaning: Duplicate license detected

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22807 - LOG_ID_VDOM_LIC

Message ID: 22807

Message Description: LOG_ID_VDOM_LIC

Message Meaning: VDOM license status changed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22808 - LOG_ID_LIC_EXPIRE

Message ID: 22808

Message Description: LOG_ID_LIC_EXPIRE

Message Meaning: VM license expired

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22809 - LOG_ID_LIC_WILL_EXPIRE

Message ID: 22809

Message Description: LOG_ID_LIC_WILL_EXPIRE

Message Meaning: VM license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
service	Name of Service	string	64
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22810 - LOG_ID_SCANUNIT_ERROR_BLOCK

Message ID: 22810

Message Description: LOG_ID_SCANUNIT_ERROR_BLOCK

Message Meaning: Scan error - traffic blocked

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
dir	Direction	string	8
dst_int	Destination Interface	string	64
src_int	Source Interface	string	64
session_id	Session ID	uint32	10
file	Report file full path	string	256
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
proto	Protocol Number	uint8	3
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22811 - LOG_ID_SCANUNIT_ERROR_PASS

Message ID: 22811

Message Description: LOG_ID_SCANUNIT_ERROR_PASS

Message Meaning: Scan error - traffic passed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
dir	Direction	string	8
dst_int	Destination Interface	string	64
src_int	Source Interface	string	64
session_id	Session ID	uint32	10
file	Report file full path	string	256
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
proto	Protocol Number	uint8	3
service	Name of Service	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22812 - LOG_ID_SCANUNIT_AVENG_RELOAD

Message ID: 22812

Message Description: LOG_ID_SCANUNIT_AVENG_RELOAD

Message Meaning: Scanunit is reloading AV engine

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22813 - LOG_ID_SCANUNIT_AVDB_RELOAD

Message ID: 22813

Message Description: LOG_ID_SCANUNIT_AVDB_RELOAD

Message Meaning: Scanunit reloaded AV Database

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22814 - LOG_ID_SCANUNIT_AVDB_RELOAD_ERROR

Message ID: 22814

Message Description: LOG_ID_SCANUNIT_AVDB_RELOAD_ERROR

Message Meaning: Scanunit AV Database reload error

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22815 - LOG_ID_SCANUNIT_AVDB_LOAD

Message ID: 22815

Message Description: LOG_ID_SCANUNIT_AVDB_LOAD

Message Meaning: Scanunit loaded AV Database

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22816 - LOG_ID_SCANUNIT_AVDB_LOAD_ERROR

Message ID: 22816

Message Description: LOG_ID_SCANUNIT_AVDB_LOAD_ERROR

Message Meaning: Scanunit AV Database load error

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22817 - LOG_ID_SCANUNIT_DLP_SIGNATURE_REMOVE

Message ID: 22817

Message Description: LOG_ID_SCANUNIT_DLP_SIGNATURE_REMOVE

Message Meaning: Scanunit DLP signature update error

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22850 - LOG_ID_USER_QUARANTINE_MAC_ADD

Message ID: 22850

Message Description: LOG_ID_USER_QUARANTINE_MAC_ADD

Message Meaning: User quarantine MAC added

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22851 - LOG_ID_USER_QUARANTINE_MAC_DELETE

Message ID: 22851

Message Description: LOG_ID_USER_QUARANTINE_MAC_DELETE

Message Meaning: User quarantine MAC deleted

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22852 - LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_HIT

Message ID: 22852

Message Description: LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_HIT

Message Meaning: User quarantine MAC bounce port hit

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22853 - LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_MISS

Message ID: 22853

Message Description: LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_MISS

Message Meaning: User quarantine MAC bounce port miss

Type: Event

Category: switch-controller

Severity: Warning

Log Field Name	Description	Data Type	Length
sn		string	64

Log Field Name	Description	Data Type	Length
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22861 - LOG_ID_FLPOLD_NAC_ADD

Message ID: 22861

Message Description: LOG_ID_FLPOLD_NAC_ADD

Message Meaning: NAC device addition

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64

Log Field Name	Description	Data Type	Length
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22862 - LOG_ID_FLPOLD_NAC_DELETE

Message ID: 22862

Message Description: LOG_ID_FLPOLD_NAC_DELETE

Message Meaning: NAC device deletion

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22863 - LOG_ID_FLPOLD_NAC_MODIFY

Message ID: 22863

Message Description: LOG_ID_FLPOLD_NAC_MODIFY

Message Meaning: NAC device modify

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20

Log Field Name	Description	Data Type	Length
type		string	16
logid		string	10
time		string	8
date		string	10

22864 - LOG_ID_FLPOLD_DPP_ADD

Message ID: 22864

Message Description: LOG_ID_FLPOLD_DPP_ADD

Message Meaning: DPP device addition

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22865 - LOG_ID_FLPOLD_DPP_DELETE

Message ID: 22865

Message Description: LOG_ID_FLPOLD_DPP_DELETE

Message Meaning: DPP device deletion

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22866 - LOG_ID_FLPOLD_DPP_MODIFY

Message ID: 22866

Message Description: LOG_ID_FLPOLD_DPP_MODIFY

Message Meaning: DPP device modify

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22867 - LOG_ID_FLPOLD_DPP_INTF_TAGS_ADD

Message ID: 22867

Message Description: LOG_ID_FLPOLD_DPP_INTF_TAGS_ADD

Message Meaning: DPP interface tags add

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128

Log Field Name	Description	Data Type	Length
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22868 - LOG_ID_FLPOLD_DPP_INTF_TAGS_DELETE

Message ID: 22868

Message Description: LOG_ID_FLPOLD_DPP_INTF_TAGS_DELETE

Message Meaning: DPP interface tags delete

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256

Log Field Name	Description	Data Type	Length
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22869 - LOG_ID_FLPOLD_NAC_DYNAMIC_ADDRESS_ADD

Message ID: 22869

Message Description: LOG_ID_FLPOLD_NAC_DYNAMIC_ADDRESS_ADD

Message Meaning: NAC device dynamic address addition

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32

Log Field Name	Description	Data Type	Length
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22870 - LOG_ID_FLPOLD_NAC_DYNAMIC_ADDRESS_DELETE

Message ID: 22870

Message Description: LOG_ID_FLPOLD_NAC_DYNAMIC_ADDRESS_DELETE

Message Meaning: NAC device dynamic address deletion

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20

Log Field Name	Description	Data Type	Length
type		string	16
logid		string	10
time		string	8
date		string	10

22871 - LOG_ID_FLPOLD_NAC_MAC_CACHE_SYNC

Message ID: 22871

Message Description: LOG_ID_FLPOLD_NAC_MAC_CACHE_SYNC

Message Meaning: NAC MAC cache sync

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22872 - LOG_ID_FLPOLD_NAC_MAX_ERROR

Message ID: 22872

Message Description: LOG_ID_FLPOLD_NAC_MAX_ERROR

Message Meaning: NAC device Max Limit Error

Type: Event

Category: switch-controller

Severity: Warning

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22873 - LOG_ID_FLPOLD_DPP_MAX_ERROR

Message ID: 22873

Message Description: LOG_ID_FLPOLD_DPP_MAX_ERROR

Message Meaning: DPP device Max Limit Error

Type: Event

Category: switch-controller

Severity: Warning

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22874 - LOG_ID_FLTUND_NEW_CONN

Message ID: 22874

Message Description: LOG_ID_FLTUND_NEW_CONN

Message Meaning: Switch-controller FortilinkLite new connection

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64

Log Field Name	Description	Data Type	Length
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22875 - LOG_ID_FLTUND_CONN_DOWN

Message ID: 22875

Message Description: LOG_ID_FLTUND_CONN_DOWN

Message Meaning: Switch-controller FortilinkLite connection down

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
sn		string	64
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16

Log Field Name	Description	Data Type	Length
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22876 - LOG_ID_FLTUND_RCV_BOOTSTRAP

Message ID: 22876

Message Description: LOG_ID_FLTUND_RCV_BOOTSTRAP

Message Meaning: Switch-controller FortilinkLite received bootstrap

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22877 - LOG_ID_FLTUND_CONN_ONLINE

Message ID: 22877

Message Description: LOG_ID_FLTUND_CONN_ONLINE

Message Meaning: Switch-controller FortilinkLite tunnel online

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22878 - LOG_ID_FLTUND_CONN_OFFLINE

Message ID: 22878

Message Description: LOG_ID_FLTUND_CONN_OFFLINE

Message Meaning: Switch-controller FortilinkLite tunnel offline

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22890 - LOG_ID_FORTILINKD

Message ID: 22890

Message Description: LOG_ID_FORTILINKD

Message Meaning: Switch-Controller Daemon Log (Notification)

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64

Log Field Name	Description	Data Type	Length
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22891 - LOG_ID_FLCFGD_SYNC_ERROR

Message ID: 22891

Message Description: LOG_ID_FLCFGD_SYNC_ERROR

Message Meaning: Switch-Controller Switch Sync Error

Type: Event

Category: switch-controller

Severity: Error

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32

Log Field Name	Description	Data Type	Length
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22892 - LOG_ID_FLCFGD_SYNC_COMPLETE

Message ID: 22892

Message Description: LOG_ID_FLCFGD_SYNC_COMPLETE

Message Meaning: Switch-Controller Switch Sync Complete

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10

Log Field Name	Description	Data Type	Length
time		string	8
date		string	10

22893 - LOG_ID_FLCFGD_SYNC_STATE

Message ID: 22893

Message Description: LOG_ID_FLCFGD_SYNC_STATE

Message Meaning: Switch-Controller Switch Sync State

Type: Event

Category: switch-controller

Severity: Debug

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22894 - LOG_ID_FLCFGD_UPGRADE_ERROR

Message ID: 22894

Message Description: LOG_ID_FLCFGD_UPGRADE_ERROR

Message Meaning: Switch-Controller Switch Upgrade Error

Type: Event

Category: switch-controller

Severity: Error

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22895 - LOG_ID_FLCFGD_UPGRADE_STATUS

Message ID: 22895

Message Description: LOG_ID_FLCFGD_UPGRADE_STATUS

Message Meaning: Switch-Controller Switch Upgrade Status

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22896 - LOG_ID_FORTILINKD_CRITICAL

Message ID: 22896

Message Description: LOG_ID_FORTILINKD_CRITICAL

Message Meaning: Switch-Controller Daemon Log (Critical)

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256

Log Field Name	Description	Data Type	Length
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22897 - LOG_ID_FORTILINKD_SPLIT_PORT_INFO

Message ID: 22897

Message Description: LOG_ID_FORTILINKD_SPLIT_PORT_INFO

Message Meaning: Switch-controller split-port related configuration change detected

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16

Log Field Name	Description	Data Type	Length
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22900 - LOG_ID_CAPUTP_SESSION

Message ID: 22900

Message Description: LOG_ID_CAPUTP_SESSION

Message Meaning: CAPUTP session status

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
msg		string	4096
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

22901 - LOG_ID_FAZ_CON

Message ID: 22901

Message Description: LOG_ID_FAZ_CON

Message Meaning: FortiAnalyzer connection up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22902 - LOG_ID_FAZ_DISCON

Message ID: 22902

Message Description: LOG_ID_FAZ_DISCON

Message Meaning: FortiAnalyzer connection down

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22903 - LOG_ID_FAZ_CON_ERR

Message ID: 22903

Message Description: LOG_ID_FAZ_CON_ERR

Message Meaning: FortiAnalyzer connection failed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22904 - LOG_ID_CAPUTP_SESSION_NOTIF

Message ID: 22904

Message Description: LOG_ID_CAPUTP_SESSION_NOTIF

Message Meaning: CAPUTP session status notification

Type: Event

Category: switch-controller

Severity: Notice

Log Field Name	Description	Data Type	Length
srcip		ip	39
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20

Log Field Name	Description	Data Type	Length
type		string	16
logid		string	10
time		string	8
date		string	10

22905 - LOG_ID_LOGDEV_STATUS_CHANGE

Message ID: 22905

Message Description: LOG_ID_LOGDEV_STATUS_CHANGE

Message Meaning: Log device status has changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22906 - LOG_ID_SECURITY_LEVEL_CHANGE

Message ID: 22906

Message Description: LOG_ID_SECURITY_LEVEL_CHANGE

Message Meaning: Hardware security level is changed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22907 - LOG_ID_INPUT_DETECTION

Message ID: 22907

Message Description: LOG_ID_INPUT_DETECTION

Message Meaning: Digital-IO input state change

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
state	State	string	64
connector		string	64

Log Field Name	Description	Data Type	Length
mode	Mode	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22908 - LOG_ID_OUTPUT_DETECTION

Message ID: 22908

Message Description: LOG_ID_OUTPUT_DETECTION

Message Meaning: Digital-IO output state change

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
state	State	string	64
connector		string	64
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22912 - LOG_ID_FDS_SRV_ERRCON

Message ID: 22912

Message Description: LOG_ID_FDS_SRV_ERRCON

Message Meaning: FortiGate Cloud server connection failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
server	Server IP Address	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22913 - LOG_ID_FDS_SRV_DISCON

Message ID: 22913

Message Description: LOG_ID_FDS_SRV_DISCON

Message Meaning: FortiGate Cloud server disconnected

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
server	Server IP Address	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22915 - LOG_ID_FDS_SRV_CON

Message ID: 22915

Message Description: LOG_ID_FDS_SRV_CON

Message Meaning: FortiGate Cloud server connected

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
server	Server IP Address	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22916 - LOG_ID_FDS_STATUS

Message ID: 22916

Message Description: LOG_ID_FDS_STATUS

Message Meaning: FortiGuard Message Service status

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22917 - LOG_ID_FDS_SMS_QUOTA

Message ID: 22917

Message Description: LOG_ID_FDS_SMS_QUOTA

Message Meaning: SMS quota reached

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22918 - LOG_ID_FDS_CTRL_STATUS

Message ID: 22918

Message Description: LOG_ID_FDS_CTRL_STATUS

Message Meaning: FortiGuard Message Service controller status

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22919 - LOG_ID_SVR_LOG_STATUS_CHANGED

Message ID: 22919

Message Description: LOG_ID_SVR_LOG_STATUS_CHANGED

Message Meaning: Server logging status changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22921 - LOG_ID_EVENT_ROUTE_INFO_CHANGED

Message ID: 22921

Message Description: LOG_ID_EVENT_ROUTE_INFO_CHANGED

Message Meaning: Routing information changed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22922 - LOG_ID_EVENT_LINK_MONITOR_STATUS

Message ID: 22922

Message Description: LOG_ID_EVENT_LINK_MONITOR_STATUS

Message Meaning: Link monitor status

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
probeproto	Link Monitor Probe Protocol	string	16
interface	Interface	string	32
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22923 - LOG_ID_EVENT_VWL_LQTY_STATUS

Message ID: 22923

Message Description: LOG_ID_EVENT_VWL_LQTY_STATUS

Message Meaning: SD-WAN status

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
numpassmember		uint32	10
service	Name of Service	string	64
serviceid		uint32	10
member		string	512
interface	Interface	string	32
newvalue		string	32
oldvalue		string	32
slatargetid		uint32	10
healthcheck		string	64
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22924 - LOG_ID_EVENT_VWL_VOLUME_STATUS

Message ID: 22924

Message Description: LOG_ID_EVENT_VWL_VOLUME_STATUS

Message Meaning: SD-WAN volume status

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
member		string	512
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22925 - LOG_ID_EVENT_VWL_SLA_INFO

Message ID: 22925

Message Description: LOG_ID_EVENT_VWL_SLA_INFO

Message Meaning: SD-WAN SLA information

Type: Event

Category: sdwan

Severity: Information

Log Field Name	Description	Data Type	Length
slamap		string	24
bibandwidthused		string	24
outbandwidthused		string	24
inbandwidthused		string	24
bibandwidthavailable		string	24
outbandwidthavailable		string	24
inbandwidthavailable		string	24
mosvalue		string	24
moscodec		string	24
packetloss		string	24
jitter		string	24
latency		string	24
status	Status	string	23
msg	Log Message	string	4096
interface	Interface	string	32
healthcheck		string	64
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

22926 - LOG_ID_EVENT_VWL_NEIGHBOR_STATUS

Message ID: 22926

Message Description: LOG_ID_EVENT_VWL_NEIGHBOR_STATUS

Message Meaning: SD-WAN Neighbor status

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
neighbor		string	46
msg	Log Message	string	4096
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22927 - LOG_ID_EVENT_VWL_NEIGHBOR_STANDALONE

Message ID: 22927

Message Description: LOG_ID_EVENT_VWL_NEIGHBOR_STANDALONE

Message Meaning: SD-WAN Neighbor standalone

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
newvalue		string	32
oldvalue		string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22928 - LOG_ID_EVENT_VWL_NEIGHBOR_PRIMARY

Message ID: 22928

Message Description: LOG_ID_EVENT_VWL_NEIGHBOR_PRIMARY

Message Meaning: SD-WAN Neighbor primary

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
newvalue		string	32
oldvalue		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22929 - LOG_ID_EVENT_VWL_NEIGHBOR_SECONDARY

Message ID: 22929

Message Description: LOG_ID_EVENT_VWL_NEIGHBOR_SECONDARY

Message Meaning: SD-WAN Neighbor secondary

Type: Event

Category: sdwan

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
newvalue		string	32
oldvalue		string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22930 - LOG_ID_EVENT_VWL_LQTY_STATUS_WARNING

Message ID: 22930

Message Description: LOG_ID_EVENT_VWL_LQTY_STATUS_WARNING

Message Meaning: SD-WAN status warning

Type: Event

Category: sdwan

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
service	Name of Service	string	64
serviceid		uint32	10
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22931 - LOG_ID_EVENT_VWL_SLA_INFO_WARNING

Message ID: 22931

Message Description: LOG_ID_EVENT_VWL_SLA_INFO_WARNING

Message Meaning: SD-WAN SLA information warning

Type: Event

Category: sdwan

Severity: Warning

Log Field Name	Description	Data Type	Length
probeproto	Link Monitor Probe Protocol	string	16
msg	Log Message	string	4096
interface	Interface	string	32
newvalue		string	32
oldvalue		string	32
healthcheck		string	64
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22932 - LOG_ID_EVENT_LINK_MONITOR_STATUS_WARNING

Message ID: 22932

Message Description: LOG_ID_EVENT_LINK_MONITOR_STATUS_WARNING

Message Meaning: Link monitor status warning

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
probeproto	Link Monitor Probe Protocol	string	16
interface	Interface	string	32
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22933 - LOG_ID_EVENT_VWL_SLA_INFO_NOTIF

Message ID: 22933

Message Description: LOG_ID_EVENT_VWL_SLA_INFO_NOTIF

Message Meaning: SD-WAN SLA notification

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
probeproto	Link Monitor Probe Protocol	string	16
slamap		string	24

Log Field Name	Description	Data Type	Length
bibandwidthused		string	24
outbandwidthused		string	24
inbandwidthused		string	24
bibandwidthavailable		string	24
outbandwidthavailable		string	24
inbandwidthavailable		string	24
mosvalue		string	24
moscodec		string	24
packetloss		string	24
jitter		string	24
latency		string	24
status	Status	string	23
msg	Log Message	string	4096
interface	Interface	string	32
newvalue		string	32
oldvalue		string	32
healthcheck		string	64
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22934 - LOG_ID_EVENT_VWL_LQTY_STATUS_INFO

Message ID: 22934

Message Description: LOG_ID_EVENT_VWL_LQTY_STATUS_INFO

Message Meaning: SD-WAN status information

Type: Event

Category: sdwan

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
member		string	512
slatargetid		uint32	10
healthcheck		string	64
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22935 - LOG_ID_EVENT_VWL_LQTY_STATUS_DEBUG

Message ID: 22935

Message Description: LOG_ID_EVENT_VWL_LQTY_STATUS_DEBUG

Message Meaning: SD-WAN status debug

Type: Event

Category: sdwan

Severity: Debug

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
service	Name of Service	string	64
serviceid		uint32	10
member		string	512
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22936 - LOG_ID_EVENT_VWL_INET_SVC_PQTY_STATUS_INFO

Message ID: 22936

Message Description: LOG_ID_EVENT_VWL_INET_SVC_PQTY_STATUS_INFO

Message Meaning: SD-WAN internet service passive quality information

Type: Event

Category: sdwan

Severity: Information

Log Field Name	Description	Data Type	Length
bibandwidthused		string	24

Log Field Name	Description	Data Type	Length
outbandwidthused		string	24
inbandwidthused		string	24
packetloss		string	24
jitter		string	24
latency		string	24
msg	Log Message	string	4096
service	Name of Service	string	64
serviceid		uint32	10
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22937 - LOG_ID_EVENT_VWL_APP_PERF_METRICS

Message ID: 22937

Message Description: LOG_ID_EVENT_VWL_APP_PERF_METRICS

Message Meaning: SD-WAN application performance metrics via FortiMonitor

Type: Event

Category: sdwan

Severity: Information

Log Field Name	Description	Data Type	Length
timestamp		string	24
apperror		string	24
networktransfertime		string	24
serverresponsetime		string	24
appid		uint32	10
app		string	80
packetloss		string	24
jitter		string	24
latency		string	24
msg	Log Message	string	4096
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22938 - LOG_ID_EVENT_VWL_WAN_SPEEDTEST_RESULT

Message ID: 22938

Message Description: LOG_ID_EVENT_VWL_WAN_SPEEDTEST_RESULT

Message Meaning: SD-WAN Bandwidth monitoring result

Type: Event

Category: sdwan

Severity: Information

Log Field Name	Description	Data Type	Length
downbandwidthmeasured		string	24
upbandwidthmeasured		string	24
protocol		string	128
mode	Mode	string	32
speedtestserver		string	80
timestamp		string	24
latency		string	24
msg	Log Message	string	4096
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22939 - LOG_ID_EVENT_VWL_FAIL_DETECT

Message ID: 22939

Message Description: LOG_ID_EVENT_VWL_FAIL_DETECT

Message Meaning: SD-WAN fail detect

Type: Event

Category: sdwan

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
interface	Interface	string	32
eventtype		string	48
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22940 - LOG_ID_EVENT_LINK_MONITOR_FAIL_DETECT

Message ID: 22940

Message Description: LOG_ID_EVENT_LINK_MONITOR_FAIL_DETECT

Message Meaning: Link monitor fail detect

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22949 - LOG_ID_FDS_JOIN

Message ID: 22949

Message Description: LOG_ID_FDS_JOIN

Message Meaning: FortiGate Cloud auto-join attempted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22950 - LOG_ID_FDS_LOGIN_SUCC

Message ID: 22950

Message Description: LOG_ID_FDS_LOGIN_SUCC

Message Meaning: FortiGate Cloud activation successful

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22951 - LOG_ID_FDS_LOGOUT

Message ID: 22951

Message Description: LOG_ID_FDS_LOGOUT

Message Meaning: FortiGate Cloud logout

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22952 - LOG_ID_FDS_LOGIN_FAIL

Message ID: 22952

Message Description: LOG_ID_FDS_LOGIN_FAIL

Message Meaning: FortiGate Cloud activation failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22954 - LOG_ID_INET_SVC_OBSOLETE

Message ID: 22954

Message Description: LOG_ID_INET_SVC_OBSOLETE

Message Meaning: Internet Service obsolete

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22955 - LOG_ID_INET_SVC_NAME_FAILURE

Message ID: 22955

Message Description: LOG_ID_INET_SVC_NAME_FAILURE

Message Meaning: Internet Service name update failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

22956 - LOG_ID_INET_SVC_NAME_UPDATE

Message ID: 22956

Message Description: LOG_ID_INET_SVC_NAME_UPDATE

Message Meaning: Internet Service name update

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

23101 - LOG_ID_IPSEC_TUNNEL_UP

Message ID: 23101

Message Description: LOG_ID_IPSEC_TUNNEL_UP

Message Meaning: IPsec VPN tunnel up

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

23102 - LOG_ID_IPSEC_TUNNEL_DOWN

Message ID: 23102

Message Description: LOG_ID_IPSEC_TUNNEL_DOWN

Message Meaning: IPsec VPN tunnel down

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

23103 - LOG_ID_IPSEC_TUNNEL_STAT

Message ID: 23103

Message Description: LOG_ID_IPSEC_TUNNEL_STAT

Message Meaning: IPsec VPN tunnel statistics

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26001 - LOG_ID_DHCP_ACK

Message ID: 26001

Message Description: LOG_ID_DHCP_ACK

Message Meaning: DHCP Ack log

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
lease	DHCP lease time	uint32	10
dhcp_msg	DHCP Message	string	4096
hostname	Hostname	string	128
interface	Interface	string	32
ip		ip	39
mac	MAC Address	string	17
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

26002 - LOG_ID_DHCP_RELEASE

Message ID: 26002

Message Description: LOG_ID_DHCP_RELEASE

Message Meaning: DHCP Release log

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
dhcp_msg	DHCP Message	string	4096
hostname	Hostname	string	128
interface	Interface	string	32
ip		ip	39
mac	MAC Address	string	17
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26003 - LOG_ID_DHCP_STAT

Message ID: 26003

Message Description: LOG_ID_DHCP_STAT

Message Meaning: DHCP statistics

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
used	Number of Used IPs	uint32	10
total	Total	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26004 - LOG_ID_DHCP_CLIENT_LEASE

Message ID: 26004

Message Description: LOG_ID_DHCP_CLIENT_LEASE

Message Meaning: DHCP client lease granted

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26005 - LOG_ID_DHCP_LEASE_USAGE_HIGH

Message ID: 26005

Message Description: LOG_ID_DHCP_LEASE_USAGE_HIGH

Message Meaning: DHCP lease usage high

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26006 - LOG_ID_DHCP_LEASE_USAGE_FULL

Message ID: 26006

Message Description: LOG_ID_DHCP_LEASE_USAGE_FULL

Message Meaning: DHCP lease usage full

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26007 - LOG_ID_DHCP_BLOCKED_MAC

Message ID: 26007

Message Description: LOG_ID_DHCP_BLOCKED_MAC

Message Meaning: DHCP client blocked log

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
mac	MAC Address	string	17
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26008 - LOG_ID_DHCP_DDNS_ADD

Message ID: 26008

Message Description: LOG_ID_DHCP_DDNS_ADD

Message Meaning: DHCP DDNS add query

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
fqdn	Fully Qualified Domain Name	string	256
ddnsserver	DDNS Server	ip	39
dhcp_msg	DHCP Message	string	4096

Log Field Name	Description	Data Type	Length
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26009 - LOG_ID_DHCP_DDNS_DELETE

Message ID: 26009

Message Description: LOG_ID_DHCP_DDNS_DELETE

Message Meaning: DHCP DDNS delete query

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
fqdn	Fully Qualified Domain Name	string	256
ddnsserver	DDNS Server	ip	39
dhcp_msg	DHCP Message	string	4096
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26010 - LOG_ID_DHCP_DDNS_COMPLETED

Message ID: 26010

Message Description: LOG_ID_DHCP_DDNS_COMPLETED

Message Meaning: DHCP DDNS query completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
fqdn	Fully Qualified Domain Name	string	256
ddnsserver	DDNS Server	ip	39
dhcp_msg	DHCP Message	string	4096
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26011 - LOG_ID_DHCPV6_REPLY

Message ID: 26011

Message Description: LOG_ID_DHCPV6_REPLY

Message Meaning: DHCPv6 Ack log

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
iaid	DHCPv6 Identity Association Identifier	uint32	10
duid	DHCPv6 unique identifier	string	128
lease	DHCP lease time	uint32	10
dhcp_msg	DHCP Message	string	4096
interface	Interface	string	32
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

26012 - LOG_ID_DHCPV6_RELEASE

Message ID: 26012

Message Description: LOG_ID_DHCPV6_RELEASE

Message Meaning: DHCPv6 Release log

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
iaid	DHCPv6 Identity Association Identifier	uint32	10
duid	DHCPv6 unique identifier	string	128
lease	DHCP lease time	uint32	10
dhcp_msg	DHCP Message	string	4096
interface	Interface	string	32
ip		ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

27001 - LOG_ID_VRRP_STATE_CHG

Message ID: 27001

Message Description: LOG_ID_VRRP_STATE_CHG

Message Meaning: VRRP state changed

Type: Event

Category: router

Severity: Information

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29001 - LOG_ID_PPPD_MSG

Message ID: 29001

Message Description: LOG_ID_PPPD_MSG

Message Meaning: PPP status

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
assigned	Assigned IP Address through PPPoE	ip	39
remote	IP Address of the PPP Remote end	ip	39
local	Local IP for a PPPD Connection	ip	39
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29002 - LOG_ID_PPPD_AUTH_SUC

Message ID: 29002

Message Description: LOG_ID_PPPD_AUTH_SUC

Message Meaning: PPP authentication successful

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
assigned	Assigned IP Address through PPPoE	ip	39
remote	IP Address of the PPP Remote end	ip	39
local	Local IP for a PPPD Connection	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29003 - LOG_ID_PPPD_AUTH_FAIL

Message ID: 29003

Message Description: LOG_ID_PPPD_AUTH_FAIL

Message Meaning: PPP authentication failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
assigned	Assigned IP Address through PPPoE	ip	39
remote	IP Address of the PPP Remote end	ip	39
local	Local IP for a PPPD Connection	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29004 - LOG_ID_PPPD_MSG_ERROR

Message ID: 29004

Message Description: LOG_ID_PPPD_MSG_ERROR

Message Meaning: PPP status error message

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
assigned	Assigned IP Address through PPPoE	ip	39
remote	IP Address of the PPP Remote end	ip	39
local	Local IP for a PPPD Connection	ip	39
msg	Log Message	string	4096
status	Status	string	23
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29005 - LOG_ID_PPPD_MSG_DEBUG

Message ID: 29005

Message Description: LOG_ID_PPPD_MSG_DEBUG

Message Meaning: PPP status debug message

Type: Event

Category: system

Severity: Debug

Log Field Name	Description	Data Type	Length
assigned	Assigned IP Address through PPPoE	ip	39
remote	IP Address of the PPP Remote end	ip	39
local	Local IP for a PPPD Connection	ip	39
msg	Log Message	string	4096
status	Status	string	23
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29010 - LOG_ID_PPPOE_STATUS_REPORT_NOTIF

Message ID: 29010

Message Description: LOG_ID_PPPOE_STATUS_REPORT_NOTIF

Message Meaning: PPPoE status report

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
mtu	Max Transmission Unit Value	uint32	10
gateway	Gateway ip address for PPPoE status report	ip	39
assigned	Assigned IP Address through PPPoE	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29011 - LOG_ID_PPPD_FAIL_TO_EXEC

Message ID: 29011

Message Description: LOG_ID_PPPD_FAIL_TO_EXEC

Message Meaning: PPP execution failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29013 - LOG_ID_PPPD_START

Message ID: 29013

Message Description: LOG_ID_PPPD_START

Message Meaning: PPP daemon started

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29014 - LOG_ID_PPPD_EXIT

Message ID: 29014

Message Description: LOG_ID_PPPD_EXIT

Message Meaning: PPP daemon exited

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29015 - LOG_ID_PPP_RCV_BAD_PEER_IP

Message ID: 29015

Message Description: LOG_ID_PPP_RCV_BAD_PEER_IP

Message Meaning: PPP received invalid peer IP

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29016 - LOG_ID_PPP_RCV_BAD_LOCAL_IP

Message ID: 29016

Message Description: LOG_ID_PPP_RCV_BAD_LOCAL_IP

Message Meaning: PPP received invalid local IP

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

29021 - LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED

Message ID: 29021

Message Description: LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED

Message Meaning: SNMP query failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
community	Community	string	36
version	Version	string	64
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
msg	Log Message	string	4096
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

29022 - LOG_ID_DDNS_UPDATE_FAIL

Message ID: 29022

Message Description: LOG_ID_DDNS_UPDATE_FAIL

Message Meaning: DDNS update failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32001 - LOG_ID_ADMIN_LOGIN_SUCC

Message ID: 32001

Message Description: LOG_ID_ADMIN_LOGIN_SUCC

Message Meaning: Admin login successful

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64

Log Field Name	Description	Data Type	Length
profile	Profile Name	string	64
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
reason	Reason	string	256
name	Display Name of the Connection	string	128
dstip	Destination IP	ip	39
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32002 - LOG_ID_ADMIN_LOGIN_FAIL

Message ID: 32002

Message Description: LOG_ID_ADMIN_LOGIN_FAIL

Message Meaning: Admin login failed

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
method	Method	string	64
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
reason	Reason	string	256
name	Display Name of the Connection	string	128
dstip	Destination IP	ip	39
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32003 - LOG_ID_ADMIN_LOGOUT

Message ID: 32003

Message Description: LOG_ID_ADMIN_LOGOUT

Message Meaning: Admin logout successful

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
state	State	string	64
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
duration	Duration	uint32	10
reason	Reason	string	256
name	Display Name of the Connection	string	128
dstip	Destination IP	ip	39
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32005 - LOG_ID_ADMIN_OVERIDE_VDOM

Message ID: 32005

Message Description: LOG_ID_ADMIN_OVERIDE_VDOM

Message Meaning: Admin overrode VDOM

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32006 - LOG_ID_ADMIN_ENTER_VDOM

Message ID: 32006

Message Description: LOG_ID_ADMIN_ENTER_VDOM

Message Meaning: Super admin entered VDOM

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32007 - LOG_ID_ADMIN_LEFT_VDOM

Message ID: 32007

Message Description: LOG_ID_ADMIN_LEFT_VDOM

Message Meaning: Super admin left VDOM

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32008 - LOG_ID_VIEW_DISK_LOG_FAIL

Message ID: 32008

Message Description: LOG_ID_VIEW_DISK_LOG_FAIL

Message Meaning: Disk log access failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32009 - LOG_ID_SYSTEM_START

Message ID: 32009

Message Description: LOG_ID_SYSTEM_START

Message Meaning: FortiGate started

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32010 - LOG_ID_DISK_LOG_FULL

Message ID: 32010

Message Description: LOG_ID_DISK_LOG_FULL

Message Meaning: Disk full

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32011 - LOG_ID_LOG_ROLL

Message ID: 32011

Message Description: LOG_ID_LOG_ROLL

Message Meaning: Disk log rolled

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
log	Log Name for Log Rotation	string	32
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32014 - LOG_ID_CS_LIC_EXPIRE

Message ID: 32014

Message Description: LOG_ID_CS_LIC_EXPIRE

Message Meaning: Support license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32015 - LOG_ID_DISK_LOG_USAGE

Message ID: 32015

Message Description: LOG_ID_DISK_LOG_USAGE

Message Meaning: Log disk full

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32017 - LOG_ID_FDS_DAILY_QUOTA_FULL

Message ID: 32017

Message Description: LOG_ID_FDS_DAILY_QUOTA_FULL

Message Meaning: FortiGate Cloud daily quota full

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32018 - LOG_ID_FIPS_ENTER_ERR_MOD

Message ID: 32018

Message Description: LOG_ID_FIPS_ENTER_ERR_MOD

Message Meaning: FIPS CC entered error mode

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32020 - LOG_ID_SSH_CORRPUT_MAC

Message ID: 32020

Message Description: LOG_ID_SSH_CORRPUT_MAC

Message Meaning: Message Authentication Code corrupted

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32021 - LOG_ID_ADMIN_LOGIN_DISABLE

Message ID: 32021

Message Description: LOG_ID_ADMIN_LOGIN_DISABLE

Message Meaning: Admin login disabled

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32022 - LOG_ID_VDOM_ENABLED

Message ID: 32022

Message Description: LOG_ID_VDOM_ENABLED

Message Meaning: VDOM enabled

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32023 - LOG_ID_MEM_LOG_FIRST_FULL

Message ID: 32023

Message Description: LOG_ID_MEM_LOG_FIRST_FULL

Message Meaning: Memory log full over first warning level

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32024 - LOG_ID_ADMIN_PASSWD_EXPIRE

Message ID: 32024

Message Description: LOG_ID_ADMIN_PASSWD_EXPIRE

Message Meaning: Admin password expired

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32025 - LOG_ID_SSH_REKEY

Message ID: 32025

Message Description: LOG_ID_SSH_REKEY

Message Meaning: SSH server re-key

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32026 - LOG_ID_SSH_BAD_PACKET_LENGTH

Message ID: 32026

Message Description: LOG_ID_SSH_BAD_PACKET_LENGTH

Message Meaning: SSH server received bad length packet

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32027 - LOG_ID_VIEW_DISK_LOG_SUCC

Message ID: 32027

Message Description: LOG_ID_VIEW_DISK_LOG_SUCC

Message Meaning: Disk logs viewed successfully

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32028 - LOG_ID_LOG_DEL_DIR

Message ID: 32028

Message Description: LOG_ID_LOG_DEL_DIR

Message Meaning: Disk log directory deleted

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32029 - LOG_ID_LOG_DEL_FILE

Message ID: 32029

Message Description: LOG_ID_LOG_DEL_FILE

Message Meaning: Disk log file deleted

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
filesize	Report File Size in Bytes	uint32	10

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32030 - LOG_ID_SEND_FDS_STAT

Message ID: 32030

Message Description: LOG_ID_SEND_FDS_STAT

Message Meaning: FDS statistics sent

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32031 - LOG_ID_VIEW_MEM_LOG_FAIL

Message ID: 32031

Message Description: LOG_ID_VIEW_MEM_LOG_FAIL

Message Meaning: Memory log access failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32032 - LOG_ID_DISK_DLP_ARCH_FULL

Message ID: 32032

Message Description: LOG_ID_DISK_DLP_ARCH_FULL

Message Meaning: DLP archive full

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32033 - LOG_ID_DISK_QUAR_FULL

Message ID: 32033

Message Description: LOG_ID_DISK_QUAR_FULL

Message Meaning: Quarantine full

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32034 - LOG_ID_DISK_REPORT_FULL

Message ID: 32034

Message Description: LOG_ID_DISK_REPORT_FULL

Message Meaning: Report db data full

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32035 - LOG_ID_VDOM_DISABLED

Message ID: 32035

Message Description: LOG_ID_VDOM_DISABLED

Message Meaning: VDOM disabled

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32036 - LOG_ID_DISK_IPS_ARCH_FULL

Message ID: 32036

Message Description: LOG_ID_DISK_IPS_ARCH_FULL

Message Meaning: IPS archive full

Type: Event

Category: system

Severity: Emergency

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32037 - LOG_ID_DISK_LOG_FIRST_FULL

Message ID: 32037

Message Description: LOG_ID_DISK_LOG_FIRST_FULL

Message Meaning: Disk log full over first warning

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32038 - LOG_ID_LOG_ROLL_FORTICRON

Message ID: 32038

Message Description: LOG_ID_LOG_ROLL_FORTICRON

Message Meaning: Log rotation requested by FortiCron

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
log	Log Name for Log Rotation	string	32
reason	Reason	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32039 - LOG_ID_VIEW_MEM_LOG_SUCC

Message ID: 32039

Message Description: LOG_ID_VIEW_MEM_LOG_SUCC

Message Meaning: Memory logs viewed successfully

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
log	Log Name for Log Rotation	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32040 - LOG_ID_REPORT_DELETED

Message ID: 32040

Message Description: LOG_ID_REPORT_DELETED

Message Meaning: Report deleted

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32041 - LOG_ID_REPORT_DELETED_GUI

Message ID: 32041

Message Description: LOG_ID_REPORT_DELETED_GUI

Message Meaning: Report deleted from GUI

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32042 - LOG_ID_MEM_LOG_SECOND_FULL

Message ID: 32042

Message Description: LOG_ID_MEM_LOG_SECOND_FULL

Message Meaning: Memory log full over second warning level

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32043 - LOG_ID_MEM_LOG_FINAL_FULL

Message ID: 32043

Message Description: LOG_ID_MEM_LOG_FINAL_FULL

Message Meaning: Memory log full over final warning level

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32044 - LOG_ID_LOG_DELETE

Message ID: 32044

Message Description: LOG_ID_LOG_DELETE

Message Meaning: Log deleted by user

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
log	Log Name for Log Rotation	string	32
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32045 - LOG_ID_MGR_LIC_EXPIRE

Message ID: 32045

Message Description: LOG_ID_MGR_LIC_EXPIRE

Message Meaning: FortiGuard management service license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32048 - LOG_ID_SCHEDULE_EXPIRE

Message ID: 32048

Message Description: LOG_ID_SCHEDULE_EXPIRE

Message Meaning: One time schedule expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32049 - LOG_ID_FC_EXPIRE

Message ID: 32049

Message Description: LOG_ID_FC_EXPIRE

Message Meaning: FortiGate Cloud license expiring

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32050 - LOG_ID_POL_PKT_CAPTURE_FULL

Message ID: 32050

Message Description: LOG_ID_POL_PKT_CAPTURE_FULL

Message Meaning: Policy packet capture full

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32051 - LOG_ID_LOG_UPLOAD

Message ID: 32051

Message Description: LOG_ID_LOG_UPLOAD

Message Meaning: Disk logs upload started

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32052 - LOG_ID_UPLOAD_RUN_SCRIPT

Message ID: 32052

Message Description: LOG_ID_UPLOAD_RUN_SCRIPT

Message Meaning: Upload and run a script

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32055 - LOG_ID_CC_KAT_SUCCESS

Message ID: 32055

Message Description: LOG_ID_CC_KAT_SUCCESS

Message Meaning: KAT tests succeeded

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32057 - LOG_ID_VIEW_FAZ_LOG_FAIL

Message ID: 32057

Message Description: LOG_ID_VIEW_FAZ_LOG_FAIL

Message Meaning: FortiAnalyzer log access failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32058 - LOG_ID_VIEW_FAZ_LOG_SUCC

Message ID: 32058

Message Description: LOG_ID_VIEW_FAZ_LOG_SUCC

Message Meaning: FortiAnalyzer logs viewed successfully

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32095 - LOG_ID_GUI_CHG_SUB_MODULE

Message ID: 32095

Message Description: LOG_ID_GUI_CHG_SUB_MODULE

Message Meaning: Admin performed an action from GUI

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32096 - LOG_ID_GUI_DOWNLOAD_LOG

Message ID: 32096

Message Description: LOG_ID_GUI_DOWNLOAD_LOG

Message Meaning: Log file downloaded from GUI

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32097 - LOG_ID_DELETE_CAPTURE_PKT

Message ID: 32097

Message Description: LOG_ID_DELETE_CAPTURE_PKT

Message Meaning: Policy packet capture file deleted

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32099 - LOG_ID_CHG_CONFIG_INFO

Message ID: 32099

Message Description: LOG_ID_CHG_CONFIG_INFO

Message Meaning: Configuration changed information

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
submodule	Sub-module name. For example autoupdate is sub-module in log of "config system autoupdate schedule"	string	32
module	Configuration Module Name	string	32
informationsource	Information Source	string	4096
desc	Description	string	128
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32100 - LOG_ID_FORTI_TOKEN_SYNC

Message ID: 32100

Message Description: LOG_ID_FORTI_TOKEN_SYNC

Message Meaning: FortiToken synchronized

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32102 - LOG_ID_CHG_CONFIG

Message ID: 32102

Message Description: LOG_ID_CHG_CONFIG

Message Meaning: Configuration changed

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32103 - LOG_ID_NEW_FIRMWARE

Message ID: 32103

Message Description: LOG_ID_NEW_FIRMWARE

Message Meaning: New firmware available on FortiGuard

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32104 - LOG_ID_CHG_CONFIG_GUI

Message ID: 32104

Message Description: LOG_ID_CHG_CONFIG_GUI

Message Meaning: Configuration changed via GUI

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
submodule	Sub-module name. For example autoupdate is sub-module in log of "config system autoupdate schedule"	string	32

Log Field Name	Description	Data Type	Length
module	Configuration Module Name	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32105 - LOG_ID_NTP_SVR_STAUS_CHG_REACHABLE

Message ID: 32105

Message Description: LOG_ID_NTP_SVR_STAUS_CHG_REACHABLE

Message Meaning: NTP server status changes to reachable

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32106 - LOG_ID_NTP_SVR_STAUS_CHG_RESOLVABLE

Message ID: 32106

Message Description: LOG_ID_NTP_SVR_STAUS_CHG_RESOLVABLE

Message Meaning: NTP server status changes to resolvable

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32107 - LOG_ID_NTP_SVR_STAUS_CHG_UNRESOLVABLE

Message ID: 32107

Message Description: LOG_ID_NTP_SVR_STAUS_CHG_UNRESOLVABLE

Message Meaning: NTP server status changes to unresolvable

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32108 - LOG_ID_NTP_SVR_STAUS_CHG_UNREACHABLE

Message ID: 32108

Message Description: LOG_ID_NTP_SVR_STAUS_CHG_UNREACHABLE

Message Meaning: NTP server status changes to unreachable

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32109 - LOG_ID_UPD_SIGN_AV_DB

Message ID: 32109

Message Description: LOG_ID_UPD_SIGN_AV_DB

Message Meaning: Updating virus database

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32110 - LOG_ID_UPD_SIGN_IPS_DB

Message ID: 32110

Message Description: LOG_ID_UPD_SIGN_IPS_DB

Message Meaning: IPS database updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32111 - LOG_ID_UPD_SIGN_AVIPS_DB

Message ID: 32111

Message Description: LOG_ID_UPD_SIGN_AVIPS_DB

Message Meaning: AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate databases updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32113 - LOG_ID_UPD_SIGN_SRCVIS_DB

Message ID: 32113

Message Description: LOG_ID_UPD_SIGN_SRCVIS_DB

Message Meaning: SRC-VIS object updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32114 - LOG_ID_UPD_SIGN_GEOIP_DB

Message ID: 32114

Message Description: LOG_ID_UPD_SIGN_GEOIP_DB

Message Meaning: GeoIP object updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32116 - LOG_ID_UPD_SIGN_AVPKG_FAILURE

Message ID: 32116

Message Description: LOG_ID_UPD_SIGN_AVPKG_FAILURE

Message Meaning: AV package update by SCP failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32117 - LOG_ID_UPD_SIGN_AVPKG_SUCCESS

Message ID: 32117

Message Description: LOG_ID_UPD_SIGN_AVPKG_SUCCESS

Message Meaning: AV package update by SCP successful

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32118 - LOG_ID_UPD_ADMIN_AV_DB

Message ID: 32118

Message Description: LOG_ID_UPD_ADMIN_AV_DB

Message Meaning: AV updated by admin

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32119 - LOG_ID_UPD_SCANUNIT_AV_DB

Message ID: 32119

Message Description: LOG_ID_UPD_SCANUNIT_AV_DB

Message Meaning: AV database updated by scanunit

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32129 - LOG_ID_ADD_GUEST

Message ID: 32129

Message Description: LOG_ID_ADD_GUEST

Message Meaning: Guest user added

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32130 - LOG_ID_CHG_USER

Message ID: 32130

Message Description: LOG_ID_CHG_USER

Message Meaning: User changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
passwd	Password	string	20
old_status	Original Status	string	512
new_status	New Status	string	512
name	Display Name of the Connection	string	128
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32131 - LOG_ID_DEL_GUEST

Message ID: 32131

Message Description: LOG_ID_DEL_GUEST

Message Meaning: Guest user deleted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32132 - LOG_ID_ADD_USER

Message ID: 32132

Message Description: LOG_ID_ADD_USER

Message Meaning: Local user added

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32138 - LOG_ID_REBOOT

Message ID: 32138

Message Description: LOG_ID_REBOOT

Message Meaning: Device rebooted

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32139 - LOG_ID_WAKE_ON_LAN

Message ID: 32139

Message Description: LOG_ID_WAKE_ON_LAN

Message Meaning: Wake on LAN device

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32140 - LOG_ID_TIME_USER_SETTING_CHG

Message ID: 32140

Message Description: LOG_ID_TIME_USER_SETTING_CHG

Message Meaning: Global time setting changed by user

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32141 - LOG_ID_TIME_NTP_SETTING_CHG

Message ID: 32141

Message Description: LOG_ID_TIME_NTP_SETTING_CHG

Message Meaning: Global time setting changed by NTP

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32142 - LOG_ID_BACKUP_CONF

Message ID: 32142

Message Description: LOG_ID_BACKUP_CONF

Message Meaning: System configuration backed up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32143 - LOG_ID_BACKUP_CONF_BY_SCP

Message ID: 32143

Message Description: LOG_ID_BACKUP_CONF_BY_SCP

Message Meaning: System configuration backed up by SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32144 - LOG_ID_BACKUP_CONF_ERROR

Message ID: 32144

Message Description: LOG_ID_BACKUP_CONF_ERROR

Message Meaning: System configuration backed up error

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32145 - LOG_ID_BACKUP_CONF_ALERT

Message ID: 32145

Message Description: LOG_ID_BACKUP_CONF_ALERT

Message Meaning: System configuration backed up alert

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32146 - LOG_ID_TIME_PTP_SETTING_CHG

Message ID: 32146

Message Description: LOG_ID_TIME_PTP_SETTING_CHG

Message Meaning: Global time setting changed by PTP

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32148 - LOG_ID_GET_CRL

Message ID: 32148

Message Description: LOG_ID_GET_CRL

Message Meaning: CRL update requested

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
crl	Certificate revocation lists	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32149 - LOG_ID_COMMAND_FAIL

Message ID: 32149

Message Description: LOG_ID_COMMAND_FAIL

Message Meaning: Command failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32151 - LOG_ID_ADD_IP6_LOCAL_POL

Message ID: 32151

Message Description: LOG_ID_ADD_IP6_LOCAL_POL

Message Meaning: IPv6 firewall local in policy added

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32152 - LOG_ID_CHG_IP6_LOCAL_POL

Message ID: 32152

Message Description: LOG_ID_CHG_IP6_LOCAL_POL

Message Meaning: IPv6 firewall local in policy setting changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32153 - LOG_ID_DEL_IP6_LOCAL_POL

Message ID: 32153

Message Description: LOG_ID_DEL_IP6_LOCAL_POL

Message Meaning: IPv6 firewall local in policy deleted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32155 - LOG_ID_ACT_FTOKEN_REQ

Message ID: 32155

Message Description: LOG_ID_ACT_FTOKEN_REQ

Message Meaning: FortiToken activation requested

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
serialno	Serial Number	string	16
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32156 - LOG_ID_ACT_FTOKEN_SUCC

Message ID: 32156

Message Description: LOG_ID_ACT_FTOKEN_SUCC

Message Meaning: FortiToken activation successful

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
serialno	Serial Number	string	16
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32157 - LOG_ID_SYNC_FTOKEN_SUCC

Message ID: 32157

Message Description: LOG_ID_SYNC_FTOKEN_SUCC

Message Meaning: FortiToken re-synchronized

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
serialno	Serial Number	string	16
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32158 - LOG_ID_SYNC_FTOKEN_FAIL

Message ID: 32158

Message Description: LOG_ID_SYNC_FTOKEN_FAIL

Message Meaning: FortiToken re-synchronization failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
serialno	Serial Number	string	16
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32159 - LOG_ID_ACT_FTOKEN_FAIL

Message ID: 32159

Message Description: LOG_ID_ACT_FTOKEN_FAIL

Message Meaning: FortiToken activation failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
serialno	Serial Number	string	16
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32160 - LOG_ID_FTM_PUSH_SUCC

Message ID: 32160

Message Description: LOG_ID_FTM_PUSH_SUCC

Message Meaning: FortiToken mobile push message succeeded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32161 - LOG_ID_FTM_PUSH_FAIL

Message ID: 32161

Message Description: LOG_ID_FTM_PUSH_FAIL

Message Meaning: FortiToken mobile push message failed

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32168 - LOG_ID_REACH_VDOM_LIMIT

Message ID: 32168

Message Description: LOG_ID_REACH_VDOM_LIMIT

Message Meaning: VDOM limit reached

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32169 - LOG_ID_ALARM_DLP_DB

Message ID: 32169

Message Description: LOG_ID_ALARM_DLP_DB

Message Meaning: DLP database space alarm

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32170 - LOG_ID_ALARM_MSG

Message ID: 32170

Message Description: LOG_ID_ALARM_MSG

Message Meaning: Alarm created

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
groupid	User Group ID	uint32	10
alarmid	Alarm ID	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32171 - LOG_ID_ALARM_ACK

Message ID: 32171

Message Description: LOG_ID_ALARM_ACK

Message Meaning: Alarm acknowledged

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
acktime	Alarm Acknowledge Time	string	24
alarmid	Alarm ID	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32172 - LOG_ID_ADD_IP4_LOCAL_POL

Message ID: 32172

Message Description: LOG_ID_ADD_IP4_LOCAL_POL

Message Meaning: IPv4 firewall local in policy added

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32173 - LOG_ID_CHG_IP4_LOCAL_POL

Message ID: 32173

Message Description: LOG_ID_CHG_IP4_LOCAL_POL

Message Meaning: IPv4 firewall local in policy's setting changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32174 - LOG_ID_DEL_IP4_LOCAL_POL

Message ID: 32174

Message Description: LOG_ID_DEL_IP4_LOCAL_POL

Message Meaning: IPv4 firewall local in policy deleted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
iptype	IP type	string	16
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
seq		string	512
saddr	Source Address IP	string	80
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32180 - LOG_ID_GEOIP_DB_INIT_FAIL

Message ID: 32180

Message Description: LOG_ID_GEOIP_DB_INIT_FAIL

Message Meaning: IP Geography DB initialization failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32190 - LOG_ID_UPT_INVALID_IMG

Message ID: 32190

Message Description: LOG_ID_UPT_INVALID_IMG

Message Meaning: Invalid image loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32191 - LOG_ID_UPT_INVALID_IMG_CC

Message ID: 32191

Message Description: LOG_ID_UPT_INVALID_IMG_CC

Message Meaning: Image with invalid CC signature loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32192 - LOG_ID_UPT_INVALID_IMG_RSA

Message ID: 32192

Message Description: LOG_ID_UPT_INVALID_IMG_RSA

Message Meaning: Image with invalid RSA signature loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32193 - LOG_ID_UPT_IMG_RSA

Message ID: 32193

Message Description: LOG_ID_UPT_IMG_RSA

Message Meaning: Image with valid RSA signature loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32194 - LOG_ID_UPT_IMG_FAIL

Message ID: 32194

Message Description: LOG_ID_UPT_IMG_FAIL

Message Meaning: System upgrade failed due to file operation failure

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32200 - LOG_ID_SHUTDOWN

Message ID: 32200

Message Description: LOG_ID_SHUTDOWN

Message Meaning: Device shutdown

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32201 - LOG_ID_LOAD_IMG_SUCC

Message ID: 32201

Message Description: LOG_ID_LOAD_IMG_SUCC

Message Meaning: Image loaded successfully

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32202 - LOG_ID_RESTORE_IMG

Message ID: 32202

Message Description: LOG_ID_RESTORE_IMG

Message Meaning: Image restored

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32203 - LOG_ID_RESTORE_CONF

Message ID: 32203

Message Description: LOG_ID_RESTORE_CONF

Message Meaning: Configuration restored

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32204 - LOG_ID_RESTORE_FGD_SVR

Message ID: 32204

Message Description: LOG_ID_RESTORE_FGD_SVR

Message Meaning: FortiGuard service restored

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32205 - LOG_ID_RESTORE_VDOM_LIC

Message ID: 32205

Message Description: LOG_ID_RESTORE_VDOM_LIC

Message Meaning: VM license restored

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32206 - LOG_ID_RESTORE_SCRIPT

Message ID: 32206

Message Description: LOG_ID_RESTORE_SCRIPT

Message Meaning: Script restored from management station

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32207 - LOG_ID_RETRIEVE_CONF_LIST

Message ID: 32207

Message Description: LOG_ID_RETRIEVE_CONF_LIST

Message Meaning: Configuration list retrieval failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32208 - LOG_ID_IMP_PKCS12_CERT

Message ID: 32208

Message Description: LOG_ID_IMP_PKCS12_CERT

Message Meaning: PKCS12 certificate imported

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32209 - LOG_ID_RESTORE_USR_DEF_IPS

Message ID: 32209

Message Description: LOG_ID_RESTORE_USR_DEF_IPS

Message Meaning: IPS custom signatures restored

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32210 - LOG_ID_BACKUP_IMG_SUCC

Message ID: 32210

Message Description: LOG_ID_BACKUP_IMG_SUCC

Message Meaning: Firmware image backed up successfully

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32211 - LOG_ID_UPLOAD_REVISION

Message ID: 32211

Message Description: LOG_ID_UPLOAD_REVISION

Message Meaning: Revision uploaded to flash disk

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32212 - LOG_ID_DEL_REVISION

Message ID: 32212

Message Description: LOG_ID_DEL_REVISION

Message Meaning: Revision deleted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32213 - LOG_ID_RESTORE_TEMPLATE

Message ID: 32213

Message Description: LOG_ID_RESTORE_TEMPLATE

Message Meaning: Template restored

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32214 - LOG_ID_RESTORE_FILE

Message ID: 32214

Message Description: LOG_ID_RESTORE_FILE

Message Meaning: File restore failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32215 - LOG_ID_UPT_IMG

Message ID: 32215

Message Description: LOG_ID_UPT_IMG

Message Meaning: Image updated

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32217 - LOG_ID_UPD_IPS

Message ID: 32217

Message Description: LOG_ID_UPD_IPS

Message Meaning: IPS package - Admin update successful

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32218 - LOG_ID_UPD_DLP

Message ID: 32218

Message Description: LOG_ID_UPD_DLP

Message Meaning: DLP fingerprint database update via SCP failed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32219 - LOG_ID_BACKUP_OUTPUT

Message ID: 32219

Message Description: LOG_ID_BACKUP_OUTPUT

Message Meaning: Error output backup via SCP successful

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32220 - LOG_ID_BACKUP_COMMAND

Message ID: 32220

Message Description: LOG_ID_BACKUP_COMMAND

Message Meaning: Batch mode command output backup via SCP successful

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32221 - LOG_ID_UPD_VDOM_LIC

Message ID: 32221

Message Description: LOG_ID_UPD_VDOM_LIC

Message Meaning: VM license installed via SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32222 - LOG_ID_GLB_SETTING_CHG

Message ID: 32222

Message Description: LOG_ID_GLB_SETTING_CHG

Message Meaning: Global setting changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
new_value	New Virtual Domain Name	string	128
old_value	Original Virtual Domain name	string	128
field	NTP date-time field	string	32
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32223 - LOG_ID_BACKUP_USER_DEF_IPS

Message ID: 32223

Message Description: LOG_ID_BACKUP_USER_DEF_IPS

Message Meaning: IPS custom signatures backup success

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32224 - LOG_ID_BACKUP_DISK_LOG

Message ID: 32224

Message Description: LOG_ID_BACKUP_DISK_LOG

Message Meaning: Disk logs backed up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
hash	Hash Value of Downloaded File	string	32
file	Report file full path	string	256
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32225 - LOG_ID_DEL_ALL_REVISION

Message ID: 32225

Message Description: LOG_ID_DEL_ALL_REVISION

Message Meaning: Revision database reset due to data corruption

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32226 - LOG_ID_LOAD_IMG_FAIL

Message ID: 32226

Message Description: LOG_ID_LOAD_IMG_FAIL

Message Meaning: Image failed to load

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32227 - LOG_ID_UPD_DLP_FAIL

Message ID: 32227

Message Description: LOG_ID_UPD_DLP_FAIL

Message Meaning: DLP fingerprint database failed to update by SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32228 - LOG_ID_LOAD_IMG_FAIL_WRONG_IMG

Message ID: 32228

Message Description: LOG_ID_LOAD_IMG_FAIL_WRONG_IMG

Message Meaning: Firmware image loaded incorrect

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32229 - LOG_ID_LOAD_IMG_FAIL_NO_RSA

Message ID: 32229

Message Description: LOG_ID_LOAD_IMG_FAIL_NO_RSA

Message Meaning: Firmware image without valid RSA signature loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32230 - LOG_ID_LOAD_IMG_FAIL_INVALID_RSA

Message ID: 32230

Message Description: LOG_ID_LOAD_IMG_FAIL_INVALID_RSA

Message Meaning: Firmware image with invalid RSA signature loaded

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32231 - LOG_ID_RESTORE_FGD_SVR_FAIL

Message ID: 32231

Message Description: LOG_ID_RESTORE_FGD_SVR_FAIL

Message Meaning: FortiGuard service failed to restore

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32232 - LOG_ID_RESTORE_VDOM_LIC_FAIL

Message ID: 32232

Message Description: LOG_ID_RESTORE_VDOM_LIC_FAIL

Message Meaning: VM license failed to restore

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32233 - LOG_ID_BACKUP_IMG_FAIL

Message ID: 32233

Message Description: LOG_ID_BACKUP_IMG_FAIL

Message Meaning: Firmware image backup failed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32234 - LOG_ID_RESTORE_IMG_INVALID_CC

Message ID: 32234

Message Description: LOG_ID_RESTORE_IMG_INVALID_CC

Message Meaning: Image with invalid CC signature restored

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32235 - LOG_ID_RESTORE_IMG_FORTIGUARD

Message ID: 32235

Message Description: LOG_ID_RESTORE_IMG_FORTIGUARD

Message Meaning: Image restored from FortiGuard Management

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32236 - LOG_ID_BACKUP_MEM_LOG

Message ID: 32236

Message Description: LOG_ID_BACKUP_MEM_LOG

Message Meaning: Memory logs backed up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32237 - LOG_ID_BACKUP_MEM_LOG_FAIL

Message ID: 32237

Message Description: LOG_ID_BACKUP_MEM_LOG_FAIL

Message Meaning: Memory logs failed to back up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32238 - LOG_ID_BACKUP_DISK_LOG_FAIL

Message ID: 32238

Message Description: LOG_ID_BACKUP_DISK_LOG_FAIL

Message Meaning: Disk logs failed to back up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32239 - LOG_ID_BACKUP_DISK_LOG_USB

Message ID: 32239

Message Description: LOG_ID_BACKUP_DISK_LOG_USB

Message Meaning: Disk logs backed up to USB

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32240 - LOG_ID_SYS_USB_MODE

Message ID: 32240

Message Description: LOG_ID_SYS_USB_MODE

Message Meaning: System operating in USB mode

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32241 - LOG_ID_BACKUP_DISK_LOG_USB_FAIL

Message ID: 32241

Message Description: LOG_ID_BACKUP_DISK_LOG_USB_FAIL

Message Meaning: Disk logs failed to back up to USB

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32242 - LOG_ID_UPD_VDOM_LIC_FAIL

Message ID: 32242

Message Description: LOG_ID_UPD_VDOM_LIC_FAIL

Message Meaning: VM license failed to install via SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32243 - LOG_ID_UPD_IPS_SCP

Message ID: 32243

Message Description: LOG_ID_UPD_IPS_SCP

Message Meaning: IPS package updated via SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32244 - LOG_ID_UPD_IPS_SCP_FAIL

Message ID: 32244

Message Description: LOG_ID_UPD_IPS_SCP_FAIL

Message Meaning: IPS package failed to update via SCP

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32245 - LOG_ID_BACKUP_USER_DEF_IPS_FAIL

Message ID: 32245

Message Description: LOG_ID_BACKUP_USER_DEF_IPS_FAIL

Message Meaning: IPS custom signatures backup failed

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32246 - LOG_ID_RESTORE_USR_DEF_IPS_CRITICAL

Message ID: 32246

Message Description: LOG_ID_RESTORE_USR_DEF_IPS_CRITICAL

Message Meaning: IPS custom signatures restored critical

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32247 - LOG_ID_SSH_NEGOTIATION_FAILURE

Message ID: 32247

Message Description: LOG_ID_SSH_NEGOTIATION_FAILURE

Message Meaning: SSH protocol cannot be negotiated

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
addr	IP Address	string	80
port	Port Number	uint16	5
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32252 - LOG_ID_FACTORY_RESET

Message ID: 32252

Message Description: LOG_ID_FACTORY_RESET

Message Meaning: Factory settings reset

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32253 - LOG_ID_FORMAT_RAID

Message ID: 32253

Message Description: LOG_ID_FORMAT_RAID

Message Meaning: RAID disk formatted

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32254 - LOG_ID_ENABLE_RAID

Message ID: 32254

Message Description: LOG_ID_ENABLE_RAID

Message Meaning: RAID enabled

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32255 - LOG_ID_DISABLE_RAID

Message ID: 32255

Message Description: LOG_ID_DISABLE_RAID

Message Meaning: RAID disabled

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32260 - LOG_ID_RESTORE_IMG_FORTIGUARD_NOTIF

Message ID: 32260

Message Description: LOG_ID_RESTORE_IMG_FORTIGUARD_NOTIF

Message Meaning: Image restored from FortiGuard Management notification

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32261 - LOG_ID_RESTORE_SCRIPT_NOTIF

Message ID: 32261

Message Description: LOG_ID_RESTORE_SCRIPT_NOTIF

Message Meaning: Script restored by user

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32262 - LOG_ID_RESTORE_IMG_CONFIRM

Message ID: 32262

Message Description: LOG_ID_RESTORE_IMG_CONFIRM

Message Meaning: Image restore confirmed by user

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32263 - LOG_ID_AUTO_IMG_UPD_SCHEDULED

Message ID: 32263

Message Description: LOG_ID_AUTO_IMG_UPD_SCHEDULED

Message Meaning: Automatic firmware upgrade schedule changed

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32264 - LOG_ID_BLE_FIRMWARE_CHECK

Message ID: 32264

Message Description: LOG_ID_BLE_FIRMWARE_CHECK

Message Meaning: Bluetooth firmware check

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32265 - LOG_ID_BLE_FIRMWARE_UPDATE

Message ID: 32265

Message Description: LOG_ID_BLE_FIRMWARE_UPDATE

Message Meaning: Bluetooth firmware update

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32270 - LOG_ID_SSH_HOST_KEY_REGEN

Message ID: 32270

Message Description: LOG_ID_SSH_HOST_KEY_REGEN

Message Meaning: SSH host keys regenerated.

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32300 - LOG_ID_UPLOAD_RPT_IMG

Message ID: 32300

Message Description: LOG_ID_UPLOAD_RPT_IMG

Message Meaning: Report image file uploaded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32301 - LOG_ID_ADD_VDOM

Message ID: 32301

Message Description: LOG_ID_ADD_VDOM

Message Meaning: VDOM added

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32302 - LOG_ID_DEL_VDOM

Message ID: 32302

Message Description: LOG_ID_DEL_VDOM

Message Meaning: VDOM deleted

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32545 - LOG_ID_SYS_RESTART

Message ID: 32545

Message Description: LOG_ID_SYS_RESTART

Message Meaning: Scheduled daily reboot started

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32546 - LOG_ID_APPLICATION_CRASH

Message ID: 32546

Message Description: LOG_ID_APPLICATION_CRASH

Message Meaning: Application crashed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32547 - LOG_ID_AUTOSCRIPT_START

Message ID: 32547

Message Description: LOG_ID_AUTOSCRIPT_START

Message Meaning: Autoscript start

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32548 - LOG_ID_AUTOSCRIPT_STOP

Message ID: 32548

Message Description: LOG_ID_AUTOSCRIPT_STOP

Message Meaning: Autoscript stop

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32549 - LOG_ID_AUTOSCRIPT_STOP_AUTO

Message ID: 32549

Message Description: LOG_ID_AUTOSCRIPT_STOP_AUTO

Message Meaning: Autoscript stop automatically

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32550 - LOG_ID_AUTOSCRIPT_DELETE_RSLT

Message ID: 32550

Message Description: LOG_ID_AUTOSCRIPT_DELETE_RSLT

Message Meaning: Autoscript delete result

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32551 - LOG_ID_AUTOSCRIPT_BACKUP_RSLT

Message ID: 32551

Message Description: LOG_ID_AUTOSCRIPT_BACKUP_RSLT

Message Meaning: Autoscript backup result

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32552 - LOG_ID_AUTOSCRIPT_CHECK_STATUS

Message ID: 32552

Message Description: LOG_ID_AUTOSCRIPT_CHECK_STATUS

Message Meaning: Autoscript check status

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

32553 - LOG_ID_AUTOSCRIPT_STOP_REACH_LIMIT

Message ID: 32553

Message Description: LOG_ID_AUTOSCRIPT_STOP_REACH_LIMIT

Message Meaning: Autoscript stop due to limit reached

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32554 - LOG_ID_UPD_ADMIN_DB

Message ID: 32554

Message Description: LOG_ID_UPD_ADMIN_DB

Message Meaning: Database updated by admin

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32561 - LOG_ID_ADMIN_LOGOUT_DISCONNECT

Message ID: 32561

Message Description: LOG_ID_ADMIN_LOGOUT_DISCONNECT

Message Meaning: Admin disconnected

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
state	State	string	64
sn	Serial Number	string	64
duration	Duration	uint32	10
reason	Reason	string	256
dstip	Destination IP	ip	39
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32562 - LOG_ID_STORE_CONF_FAIL_SPACE

Message ID: 32562

Message Description: LOG_ID_STORE_CONF_FAIL_SPACE

Message Meaning: Store config failed - not enough flash space

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32564 - LOG_ID_RESTORE_CONF_FAIL

Message ID: 32564

Message Description: LOG_ID_RESTORE_CONF_FAIL

Message Meaning: Configuration failed to restore

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32565 - LOG_ID_RESTORE_CONF_BY_MGMT

Message ID: 32565

Message Description: LOG_ID_RESTORE_CONF_BY_MGMT

Message Meaning: Configuration restored from management station

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32566 - LOG_ID_RESTORE_CONF_BY_SCP

Message ID: 32566

Message Description: LOG_ID_RESTORE_CONF_BY_SCP

Message Meaning: Configuration restored by SCP

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32568 - LOG_ID_DEL_REVISION_DB

Message ID: 32568

Message Description: LOG_ID_DEL_REVISION_DB

Message Meaning: Revision Database deletion

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32569 - LOG_ID_FSW_SWITCH_LOG_EVENT

Message ID: 32569

Message Description: LOG_ID_FSW_SWITCH_LOG_EVENT

Message Meaning: Switch-Controller

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
switchaclid		uint32	10
cert	Certificate	string	36
switchl2capacity		uint32	10
switchl2count		uint32	10
switchtrunk		string	16
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10
switchsysteminterface		string	16
switchphysicalport		string	16
eventtype		string	48
switchtrunkinterface		string	16

Log Field Name	Description	Data Type	Length
vlan		uint32	10
srcmac		string	17
switchinterface		string	16
switchautoip		ip	39
switchmirrorsession		string	16
reason	Reason	string	256
status	Status	string	23
srcip		ip	39
sn		string	64
name		string	128
msg		string	4096
action		string	65
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32571 - LOG_ID_RESTORE_CONF_FAIL_WARNING

Message ID: 32571

Message Description: LOG_ID_RESTORE_CONF_FAIL_WARNING

Message Meaning: Configuration failed to restore warning

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

32601 - LOG_ID_FGT_SWITCH_LOG_DISCOVER

Message ID: 32601

Message Description: LOG_ID_FGT_SWITCH_LOG_DISCOVER

Message Meaning: Switch-Controller discovered

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64

Log Field Name	Description	Data Type	Length
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32602 - LOG_ID_FGT_SWITCH_LOG_AUTH

Message ID: 32602

Message Description: LOG_ID_FGT_SWITCH_LOG_AUTH

Message Meaning: Switch-Controller authorized

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32

Log Field Name	Description	Data Type	Length
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32603 - LOG_ID_FGT_SWITCH_LOG_DEAUTH

Message ID: 32603

Message Description: LOG_ID_FGT_SWITCH_LOG_DEAUTH

Message Meaning: Switch-Controller deauthorized

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10

Log Field Name	Description	Data Type	Length
time		string	8
date		string	10

32604 - LOG_ID_FGT_SWITCH_LOG_DELETE

Message ID: 32604

Message Description: LOG_ID_FGT_SWITCH_LOG_DELETE

Message Meaning: Switch-Controller deleted

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32605 - LOG_ID_FGT_SWITCH_LOG_TUNNEL_UP

Message ID: 32605

Message Description: LOG_ID_FGT_SWITCH_LOG_TUNNEL_UP

Message Meaning: Switch-Controller Tunnel Up

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32606 - LOG_ID_FGT_SWITCH_LOG_TUNNEL_DOWN

Message ID: 32606

Message Description: LOG_ID_FGT_SWITCH_LOG_TUNNEL_DOWN

Message Meaning: Switch-Controller Tunnel Down

Type: Event

Category: switch-controller

Severity: Warning

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32607 - LOG_ID_FGT_SWITCH_PUSH_IMAGE

Message ID: 32607

Message Description: LOG_ID_FGT_SWITCH_PUSH_IMAGE

Message Meaning: Image push to FortiSwitch

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256

Log Field Name	Description	Data Type	Length
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32608 - LOG_ID_FGT_SWITCH_STAGE_IMAGE

Message ID: 32608

Message Description: LOG_ID_FGT_SWITCH_STAGE_IMAGE

Message Meaning: Image stage to FortiSwitch

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16

Log Field Name	Description	Data Type	Length
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32609 - LOG_ID_FGT_SWITCH_DISABLE_DISCOVERY

Message ID: 32609

Message Description: LOG_ID_FGT_SWITCH_DISABLE_DISCOVERY

Message Meaning: Disable FortiSwitch Discovery

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32610 - LOG_ID_FGT_SWITCH_LOG_WARNING

Message ID: 32610

Message Description: LOG_ID_FGT_SWITCH_LOG_WARNING

Message Meaning: Switch-Controller warning

Type: Event

Category: switch-controller

Severity: Warning

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32611 - LOG_ID_FGT_SWITCH_EXPORT_POOL

Message ID: 32611

Message Description: LOG_ID_FGT_SWITCH_EXPORT_POOL

Message Meaning: Export port to pool

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32612 - LOG_ID_FGT_SWITCH_EXPORT_VDOM

Message ID: 32612

Message Description: LOG_ID_FGT_SWITCH_EXPORT_VDOM

Message Meaning: Export port to vdom

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256

Log Field Name	Description	Data Type	Length
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32613 - LOG_ID_FGT_SWITCH_REQUEST_PORT

Message ID: 32613

Message Description: LOG_ID_FGT_SWITCH_REQUEST_PORT

Message Meaning: Request port from pool

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20

Log Field Name	Description	Data Type	Length
type		string	16
logid		string	10
time		string	8
date		string	10

32614 - LOG_ID_FGT_SWITCH_RETURN_PORT

Message ID: 32614

Message Description: LOG_ID_FGT_SWITCH_RETURN_PORT

Message Meaning: Return port to pool

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32615 - LOG_ID_FGT_SWITCH_MAC_ADD

Message ID: 32615

Message Description: LOG_ID_FGT_SWITCH_MAC_ADD

Message Meaning: FortiSwitch MAC add

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32616 - LOG_ID_FGT_SWITCH_MAC_DEL

Message ID: 32616

Message Description: LOG_ID_FGT_SWITCH_MAC_DEL

Message Meaning: FortiSwitch MAC delete

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32617 - LOG_ID_FGT_SWITCH_MAC_MOVE

Message ID: 32617

Message Description: LOG_ID_FGT_SWITCH_MAC_MOVE

Message Meaning: FortiSwitch MAC move

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256

Log Field Name	Description	Data Type	Length
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32618 - LOG_ID_FGT_SWITCH_EXPORT_POOL_UNDO

Message ID: 32618

Message Description: LOG_ID_FGT_SWITCH_EXPORT_POOL_UNDO

Message Meaning: Revert export port to pool

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16

Log Field Name	Description	Data Type	Length
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32619 - LOG_ID_FGT_SWITCH_EXPORT_VDOM_UNDO

Message ID: 32619

Message Description: LOG_ID_FGT_SWITCH_EXPORT_VDOM_UNDO

Message Meaning: Revert export port to vdom

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32620 - LOG_ID_FGT_SWITCH_GROUP_ADD_MEMBER

Message ID: 32620

Message Description: LOG_ID_FGT_SWITCH_GROUP_ADD_MEMBER

Message Meaning: Add switch as member to switch group

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32621 - LOG_ID_FGT_SWITCH_GROUP_DEL_MEMBER

Message ID: 32621

Message Description: LOG_ID_FGT_SWITCH_GROUP_DEL_MEMBER

Message Meaning: Delete switch as member from switch group

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32622 - LOG_ID_FGT_SWITCH_FORTILINK_CONNECTED

Message ID: 32622

Message Description: LOG_ID_FGT_SWITCH_FORTILINK_CONNECTED

Message Meaning: Switch connected via Fortilink

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
field	NTP date-time field	string	32
sn		string	64
name		string	128
msg		string	4096

Log Field Name	Description	Data Type	Length
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32623 - LOG_ID_FGT_SWITCH_LOCATION_CHANGE

Message ID: 32623

Message Description: LOG_ID_FGT_SWITCH_LOCATION_CHANGE

Message Meaning: Fortilink Switch location change

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32624 - LOG_ID_FGT_SWITCH_NEW_PEER_DETECT

Message ID: 32624

Message Description: LOG_ID_FGT_SWITCH_NEW_PEER_DETECT

Message Meaning: Fortilink Switch new peer detected

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16

Log Field Name	Description	Data Type	Length
logid		string	10
time		string	8
date		string	10

32625 - LOG_ID_FGT_SWITCH_IMG_VERIFICATION

Message ID: 32625

Message Description: LOG_ID_FGT_SWITCH_IMG_VERIFICATION

Message Meaning: Fortilink Switch image verification

Type: Event

Category: switch-controller

Severity: Information

Log Field Name	Description	Data Type	Length
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32693 - LOG_ID_FGT_SWITCH_GROUP_SWC

Message ID: 32693

Message Description: LOG_ID_FGT_SWITCH_GROUP_SWC

Message Meaning: FortiSwitch switch controller

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32694 - LOG_ID_FGT_SWITCH_GROUP_POE

Message ID: 32694

Message Description: LOG_ID_FGT_SWITCH_GROUP_POE

Message Meaning: FortiSwitch PoE

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32695 - LOG_ID_FGT_SWITCH_GROUP_LINK

Message ID: 32695

Message Description: LOG_ID_FGT_SWITCH_GROUP_LINK

Message Meaning: FortiSwitch link

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32696 - LOG_ID_FGT_SWITCH_GROUP_STP

Message ID: 32696

Message Description: LOG_ID_FGT_SWITCH_GROUP_STP

Message Meaning: FortiSwitch spanning Tree

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096

Log Field Name	Description	Data Type	Length
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32697 - LOG_ID_FGT_SWITCH_GROUP_SWITCH

Message ID: 32697

Message Description: LOG_ID_FGT_SWITCH_GROUP_SWITCH

Message Meaning: FortiSwitch switch

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256

Log Field Name	Description	Data Type	Length
cfgpath		string	128
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32698 - LOG_ID_FGT_SWITCH_GROUP_ROUTER

Message ID: 32698

Message Description: LOG_ID_FGT_SWITCH_GROUP_ROUTER

Message Meaning: FortiSwitch router

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128

Log Field Name	Description	Data Type	Length
cfgtid		uint32	10
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32699 - LOG_ID_FGT_SWITCH_GROUP_SYSTEM

Message ID: 32699

Message Description: LOG_ID_FGT_SWITCH_GROUP_SYSTEM

Message Meaning: FortiSwitch system

Type: Event

Category: switch-controller

Severity: Critical

Log Field Name	Description	Data Type	Length
cfgattr		string	4096
cfgobj		string	256
cfgpath		string	128
cfgtid		uint32	10

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128
msg		string	4096
ui		string	64
user		string	256
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

32701 - LOG_ID_FGT_INTF_IP_CONFLICT

Message ID: 32701

Message Description: LOG_ID_FGT_INTF_IP_CONFLICT

Message Meaning: Detected IP conflicts on FGT interfaces.

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34415 - LOG_ID_NP6_IPSEC_ENGINE_BUSY

Message ID: 34415

Message Description: LOG_ID_NP6_IPSEC_ENGINE_BUSY

Message Meaning: NP6 IPsec engine is busy

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34416 - LOG_ID_NP6_IPSEC_ENGINE_POSSIBLY_LOCKUP

Message ID: 34416

Message Description: LOG_ID_NP6_IPSEC_ENGINE_POSSIBLY_LOCKUP

Message Meaning: NP6 IPsec engine is possibly locked up

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34417 - LOG_ID_NP6_IPSEC_ENGINE_LOCKUP

Message ID: 34417

Message Description: LOG_ID_NP6_IPSEC_ENGINE_LOCKUP

Message Meaning: NP6 IPsec engine is locked up

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34418 - LOG_ID_NP6_HPE_PACKET_DROP

Message ID: 34418

Message Description: LOG_ID_NP6_HPE_PACKET_DROP

Message Meaning: NP6 HPE is dropping packets

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

34419 - LOG_ID_NP6_HPE_PACKET_FLOOD

Message ID: 34419

Message Description: LOG_ID_NP6_HPE_PACKET_FLOOD

Message Meaning: NP6 HPE under a packets flood

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34420 - LOG_ID_NP6XLITE_HPE_PACKET_DROP

Message ID: 34420

Message Description: LOG_ID_NP6XLITE_HPE_PACKET_DROP

Message Meaning: NP6XLITE HPE is dropping packets

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34421 - LOG_ID_NP6XLITE_HPE_PACKET_FLOOD

Message ID: 34421

Message Description: LOG_ID_NP6XLITE_HPE_PACKET_FLOOD

Message Meaning: NP6XLITE HPE under a packets flood

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34428 - LOG_ID_NP7_HPE_PACKET_DROP

Message ID: 34428

Message Description: LOG_ID_NP7_HPE_PACKET_DROP

Message Meaning: NPU HPE is dropping packets

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

34430 - LOG_ID_NP7_HPE_PACKET_FLOOD

Message ID: 34430

Message Description: LOG_ID_NP7_HPE_PACKET_FLOOD

Message Meaning: NPU HPE under packet flood

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35001 - LOG_ID_HA_SYNC_VIRDB

Message ID: 35001

Message Description: LOG_ID_HA_SYNC_VIRDB

Message Meaning: HA secondary synchronized Virus database

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35002 - LOG_ID_HA_SYNC_ETDB

Message ID: 35002

Message Description: LOG_ID_HA_SYNC_ETDB

Message Meaning: HA secondary synchronized Extended database

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35003 - LOG_ID_HA_SYNC_EXDB

Message ID: 35003

Message Description: LOG_ID_HA_SYNC_EXDB

Message Meaning: HA secondary synchronized Extreme database

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35004 - LOG_ID_HA_SYNC_FLDB

Message ID: 35004

Message Description: LOG_ID_HA_SYNC_FLDB

Message Meaning: HA secondary synchronized FLDB

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35005 - LOG_ID_HA_SYNC_IPS

Message ID: 35005

Message Description: LOG_ID_HA_SYNC_IPS

Message Meaning: HA secondary synchronized IDS package

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35007 - LOG_ID_HA_SYNC_AV

Message ID: 35007

Message Description: LOG_ID_HA_SYNC_AV

Message Meaning: HA secondary synchronized AntiVirus package

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35009 - LOG_ID_HA_SYNC_CID

Message ID: 35009

Message Description: LOG_ID_HA_SYNC_CID

Message Meaning: HA secondary synchronized CID package

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35011 - LOG_ID_HA_SYNC_FAIL

Message ID: 35011

Message Description: LOG_ID_HA_SYNC_FAIL

Message Meaning: HA secondary synchronization failed

Type: Event

Category: ha

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

35012 - LOG_ID_CONF_SYNC_FAIL

Message ID: 35012

Message Description: LOG_ID_CONF_SYNC_FAIL

Message Meaning: Secondary sync failed

Type: Event

Category: ha

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35013 - LOG_ID_HA_FAILOVER_FAIL

Message ID: 35013

Message Description: LOG_ID_HA_FAILOVER_FAIL

Message Meaning: HA failover failed

Type: Event

Category: ha

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35014 - LOG_ID_HA_RESET_UPTIME

Message ID: 35014

Message Description: LOG_ID_HA_RESET_UPTIME

Message Meaning: HA reset uptime

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35015 - LOG_ID_HA_CLEAR_HISTORY

Message ID: 35015

Message Description: LOG_ID_HA_CLEAR_HISTORY

Message Meaning: HA clear history

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
user	User name of authenticated user	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35016 - LOG_ID_HA_FAILOVER_SUCCESS

Message ID: 35016

Message Description: LOG_ID_HA_FAILOVER_SUCCESS

Message Meaning: HA failover success

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35051 - LOG_ID_PCP_MAPPING_CREATE

Message ID: 35051

Message Description: LOG_ID_PCP_MAPPING_CREATE

Message Meaning: Create PCP mapping

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35052 - LOG_ID_PCP_MAPPING_DELETE

Message ID: 35052

Message Description: LOG_ID_PCP_MAPPING_DELETE

Message Meaning: Delete PCP mapping

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36
proto	Protocol Number	uint8	3
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

35053 - LOG_ID_PCP_MAPPING_RENEW

Message ID: 35053

Message Description: LOG_ID_PCP_MAPPING_RENEW

Message Meaning: Renew PCP mapping

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
poolname	IP Pool Name	string	36
proto	Protocol Number	uint8	3
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

36881 - LOG_ID_EVENT_SYSTEM_CFG_REVERT

Message ID: 36881

Message Description: LOG_ID_EVENT_SYSTEM_CFG_REVERT

Message Meaning: Configuration reverted due to timeout

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

36882 - LOG_ID_EVENT_SYSTEM_CFG_MANUALLY_SAVED

Message ID: 36882

Message Description: LOG_ID_EVENT_SYSTEM_CFG_MANUALLY_SAVED

Message Meaning: Configuration manually saved

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

36883 - LOG_ID_EVENT_SYSTEM_CLEAR_ACTIVE_SESSION

Message ID: 36883

Message Description: LOG_ID_EVENT_SYSTEM_CLEAR_ACTIVE_SESSION

Message Meaning: Clear active sessions

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
method	Method	string	64
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37120 - MESGID_NEG_GENERIC_P1_NOTIF

Message ID: 37120

Message Description: MESGID_NEG_GENERIC_P1_NOTIF

Message Meaning: Negotiate IPsec phase 1

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
advpnsc		uint8	3
fctuid		string	32
peer_notif	IPsec VPN Peer Notification	string	25
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64

Log Field Name	Description	Data Type	Length
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37121 - MESGID_NEG_GENERIC_P1_ERROR

Message ID: 37121

Message Description: MESGID_NEG_GENERIC_P1_ERROR

Message Meaning: Negotiate IPsec phase 1

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
advpnsc		uint8	3

Log Field Name	Description	Data Type	Length
fctuid		string	32
peer_notif	IPsec VPN Peer Notification	string	25
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37122 - MESGID_NEG_GENERIC_P2_NOTIF

Message ID: 37122

Message Description: MESGID_NEG_GENERIC_P2_NOTIF

Message Meaning: Negotiate IPsec phase 2

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
espauth	IPsec Phase2 ESP message authentication code	string	17
esptransform	IPsec Phase2 ESP encryption method	string	21
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37123 - MESGID_NEG_GENERIC_P2_ERROR

Message ID: 37123

Message Description: MESGID_NEG_GENERIC_P2_ERROR

Message Meaning: Negotiate IPsec phase 2

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
espauth	IPsec Phase2 ESP message authentication code	string	17
esptransform	IPsec Phase2 ESP encryption method	string	21
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256

Log Field Name	Description	Data Type	Length
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37124 - MESGID_NEG_I_P1_ERROR

Message ID: 37124

Message Description: MESGID_NEG_I_P1_ERROR

Message Meaning: IPsec phase 1 error

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
advpnsc		uint8	3
fctuid		string	32
peer_notif	IPsec VPN Peer Notification	string	25
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37125 - MESGID_NEG_I_P2_ERROR

Message ID: 37125

Message Description: MESGID_NEG_I_P2_ERROR

Message Meaning: IPsec phase 2 error

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37126 - MESGID_NEG_NO_STATE_ERROR

Message ID: 37126

Message Description: MESGID_NEG_NO_STATE_ERROR

Message Meaning: IPsec no state error

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
advpnsc		uint8	3
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37127 - MESGID_NEG_PROGRESS_P1_NOTIF

Message ID: 37127

Message Description: MESGID_NEG_PROGRESS_P1_NOTIF

Message Meaning: Progress IPsec phase 1

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
stage		uint8	3
mode	IPsec VPN ID protection mode	string	32
version	Version	string	64
dir	Direction	string	8
exch	Type of IKE messages exchanged	string	14
init		string	6

Log Field Name	Description	Data Type	Length
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

37128 - MESGID_NEG_PROGRESS_P1_ERROR

Message ID: 37128

Message Description: MESGID_NEG_PROGRESS_P1_ERROR

Message Meaning: Progress IPsec phase 1

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
stage		uint8	3
mode	IPsec VPN ID protection mode	string	32
version	Version	string	64
dir	Direction	string	8
exch	Type of IKE messages exchanged	string	14
init		string	6
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32

Log Field Name	Description	Data Type	Length
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37129 - MESGID_NEG_PROGRESS_P2_NOTIF

Message ID: 37129

Message Description: MESGID_NEG_PROGRESS_P2_NOTIF

Message Meaning: Progress IPsec phase 2

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
stage		uint8	3
mode	IPsec VPN ID protection mode	string	32

Log Field Name	Description	Data Type	Length
version	Version	string	64
dir	Direction	string	8
exch	Type of IKE messages exchanged	string	14
init		string	6
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37130 - MESGID_NEG_PROGRESS_P2_ERROR

Message ID: 37130

Message Description: MESGID_NEG_PROGRESS_P2_ERROR

Message Meaning: Progress IPsec phase 2

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
stage		uint8	3
mode	IPsec VPN ID protection mode	string	32
version	Version	string	64
dir	Direction	string	8
exch	Type of IKE messages exchanged	string	14
init		string	6
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
result	IPsec VPN negotiation result	string	31
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256

Log Field Name	Description	Data Type	Length
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37131 - MESGID_ESP_ERROR

Message ID: 37131

Message Description: MESGID_ESP_ERROR

Message Meaning: IPsec ESP

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
seq	Sequence	string	512
spi	Security Parameter Index	string	16
error_num	Error Number	string	53
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

37132 - MESGID_ESP_CRITICAL

Message ID: 37132

Message Description: MESGID_ESP_CRITICAL

Message Meaning: IPsec ESP

Type: Event

Category: vpn

Severity: Critical

Log Field Name	Description	Data Type	Length
seq	Sequence	string	512
spi	Security Parameter Index	string	16
error_num	Error Number	string	53
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37133 - MESGID_INSTALL_SA

Message ID: 37133

Message Description: MESGID_INSTALL_SA

Message Meaning: IPsec SA installed

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
out_spi	Out SPI	string	16
in_spi	SPI for incoming traffic	string	16
role	IPsec peer role, initator or responder	string	9
advpnsc		uint8	3
fctuid		string	32
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128

Log Field Name	Description	Data Type	Length
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37134 - MESGID_DELETE_P1_SA

Message ID: 37134

Message Description: MESGID_DELETE_P1_SA

Message Meaning: IPsec phase 1 SA deleted

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
advpnsc		uint8	3
fctuid		string	32
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37135 - MESGID_DELETE_P2_SA

Message ID: 37135

Message Description: MESGID_DELETE_P2_SA

Message Meaning: IPsec phase 2 SA deleted

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
out_spi	Out SPI	string	16
in_spi	SPI for incoming traffic	string	16
advpnsc		uint8	3
fctuid		string	32
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37136 - MESGID_DPD_FAILURE

Message ID: 37136

Message Description: MESGID_DPD_FAILURE

Message Meaning: IPsec DPD failed

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37137 - MESGID_CONN_FAILURE

Message ID: 37137

Message Description: MESGID_CONN_FAILURE

Message Meaning: IPsec connection failed

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
advpnsc		uint8	3
fctuid		string	32
status	Status	string	23
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64

Log Field Name	Description	Data Type	Length
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37138 - MESGID_CONN_UPDOWN

Message ID: 37138

Message Description: MESGID_CONN_UPDOWN

Message Meaning: IPsec connection status changed

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
nextstat	Time interval in seconds for the next statistics	uint32	10
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10
advpnsc		uint8	3
fctuid		string	32
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37139 - MESGID_P2_UPDOWN

Message ID: 37139

Message Description: MESGID_P2_UPDOWN

Message Meaning: IPsec phase 2 status changed

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
phase2_name	Phase 2 Name	string	128
advpnsc		uint8	3
fctuid		string	32
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37141 - MESGID_CONN_STATS

Message ID: 37141

Message Description: MESGID_CONN_STATS

Message Meaning: IPsec tunnel statistics

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
nextstat	Time interval in seconds for the next statistics	uint32	10
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10
advpnsc		uint8	3
fctuid		string	32

Log Field Name	Description	Data Type	Length
vpntunnel	IPsec VPN Tunnel Name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
xauthgroup	IPsec VPN Xauth user group name	string	128
xauthuser	IPsec VPN Xauth user name	string	256
useralt		string	256
cookies	Cookie	string	64
srccountry		string	64
outintf	IPsec VPN binding interface	string	32
locport	Local Port	uint16	5
remport	Remote Port	uint16	5
locip	IPsec VPN local gateway IP address	ip	39
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37889 - MESGID_VC_DELETE

Message ID: 37889

Message Description: MESGID_VC_DELETE

Message Meaning: Virtual cluster deleted

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37890 - MESGID_VC_MOVE_VDOM

Message ID: 37890

Message Description: MESGID_VC_MOVE_VDOM

Message Meaning: Virtual cluster VDOM moved

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
vdname	Virtual Domain Name	string	32
to_vcluster	Destination virtual cluster number	uint32	10
from_vcluster	Source virtual cluster number	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37891 - MESGID_VC_ADD_VDOM

Message ID: 37891

Message Description: MESGID_VC_ADD_VDOM

Message Meaning: Virtual cluster VDOM added

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
vdname	Virtual Domain Name	string	32
to_vcluster	Destination virtual cluster number	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37892 - MESGID_VC_MOVE_MEMB_STATE

Message ID: 37892

Message Description: MESGID_VC_MOVE_MEMB_STATE

Message Meaning: Virtual cluster member state moved

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
hostname		string	128
vcluster_member	Virtual cluster member	uint32	10
vcluster_state	Virtual cluster member state	string	7
ha_role	The HA role in the cluster	string	9
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37893 - MESGID_VC_DETECT_MEMB_DEAD

Message ID: 37893

Message Description: MESGID_VC_DETECT_MEMB_DEAD

Message Meaning: Virtual cluster member dead

Type: Event

Category: ha

Severity: Critical

Log Field Name	Description	Data Type	Length
ha_group	HA Group Number - can be 0 - 255	uint16	4
sn	Serial Number	string	64
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37894 - MESGID_VC_DETECT_MEMB_JOIN

Message ID: 37894

Message Description: MESGID_VC_DETECT_MEMB_JOIN

Message Meaning: Virtual cluster member joined

Type: Event

Category: ha

Severity: Critical

Log Field Name	Description	Data Type	Length
ha_group	HA Group Number - can be 0 - 255	uint16	4
sn	Serial Number	string	64
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37895 - MESGID_VC_ADD_HADEV

Message ID: 37895

Message Description: MESGID_VC_ADD_HADEV

Message Meaning: Virtual cluster added HA device interface

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37896 - MESGID_VC_DEL_HADEV

Message ID: 37896

Message Description: MESGID_VC_DEL_HADEV

Message Meaning: Virtual cluster deleted HA device interface

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
vcluster	Virtual cluster	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37897 - MESGID_HADEV_READY

Message ID: 37897

Message Description: MESGID_HADEV_READY

Message Meaning: HA device interface ready

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37898 - MESGID_HADEV_FAIL

Message ID: 37898

Message Description: MESGID_HADEV_FAIL

Message Meaning: HA device interface failed

Type: Event

Category: ha

Severity: Warning

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37899 - MESGID_HADEV_PEERINFO

Message ID: 37899

Message Description: MESGID_HADEV_PEERINFO

Message Meaning: HA device interface peer information

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37900 - MESGID_HBDEV_DELETE

Message ID: 37900

Message Description: MESGID_HBDEV_DELETE

Message Meaning: Heartbeat device interface deleted

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37901 - MESGID_HBDEV_DOWN

Message ID: 37901

Message Description: MESGID_HBDEV_DOWN

Message Meaning: Heartbeat device interface down

Type: Event

Category: ha

Severity: Critical

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37902 - MESGID_HBDEV_UP

Message ID: 37902

Message Description: MESGID_HBDEV_UP

Message Meaning: Heartbeat device interface up

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37903 - MESGID_SYNC_STATUS

Message ID: 37903

Message Description: MESGID_SYNC_STATUS

Message Meaning: Synchronization status with primary

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
sync_status	The sync status with the primary	string	11
sync_type	The sync type with the primary	string	14
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37904 - MESGID_HA_ACTIVITY

Message ID: 37904

Message Description: MESGID_HA_ACTIVITY

Message Meaning: Device set as HA primary

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
activity	HA activity message	string	128
ha_group	HA Group Number - can be 0 - 255	uint16	4
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37907 - MESGID_VLAN_HB_UP

Message ID: 37907

Message Description: MESGID_VLAN_HB_UP

Message Meaning: VLAN heartbeat started

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37908 - MESGID_VLAN_HB_DOWN

Message ID: 37908

Message Description: MESGID_VLAN_HB_DOWN

Message Meaning: VLAN heartbeat lost

Type: Event

Category: ha

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37909 - MESGID_VLAN_HB_DOWN_SUM

Message ID: 37909

Message Description: MESGID_VLAN_HB_DOWN_SUM

Message Meaning: VLAN heartbeat lost summary

Type: Event

Category: ha

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37910 - MESGID_HB_PACKET_LOST

Message ID: 37910

Message Description: MESGID_HB_PACKET_LOST

Message Meaning: Heartbeat packet lost

Type: Event

Category: ha

Severity: Critical

Log Field Name	Description	Data Type	Length
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37911 - MESGID_HA_ACTIVITY_INFO

Message ID: 37911

Message Description: MESGID_HA_ACTIVITY_INFO

Message Meaning: Device set as HA master information

Type: Event

Category: ha

Severity: Information

Log Field Name	Description	Data Type	Length
ha-prio	HA Priority	uint8	3
ip		ip	39
activity	HA activity message	string	128
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37912 - MESGID_FGSP_MEMBER_JOIN

Message ID: 37912

Message Description: MESGID_FGSP_MEMBER_JOIN

Message Meaning: FGSP member joined

Type: Event

Category: ha

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

37913 - MESGID_FGSP_MEMBER_LEAVE

Message ID: 37913

Message Description: MESGID_FGSP_MEMBER_LEAVE

Message Meaning: FGSP member left

Type: Event

Category: ha

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38010 - LOG_ID_FIPS_ENCRY_FAIL

Message ID: 38010

Message Description: LOG_ID_FIPS_ENCRY_FAIL

Message Meaning: FIPS CC encryption failed

Type: Event

Category: user

Severity: Alert

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38011 - LOG_ID_FIPS_DECRY_FAIL

Message ID: 38011

Message Description: LOG_ID_FIPS_DECRY_FAIL

Message Meaning: FIPS CC decryption failed

Type: Event

Category: user

Severity: Alert

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38012 - LOG_ID_ENTROPY_TOKEN

Message ID: 38012

Message Description: LOG_ID_ENTROPY_TOKEN

Message Meaning: Seeding from entropy source

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38031 - LOG_ID_FSSO_LOGON

Message ID: 38031

Message Description: LOG_ID_FSSO_LOGON

Message Meaning: FSSO logon successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
server	AD server FQDN or IP	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38032 - LOG_ID_FSSO_LOGOFF

Message ID: 38032

Message Description: LOG_ID_FSSO_LOGOFF

Message Meaning: FSSO logout successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
server	AD server FQDN or IP	string	64
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38033 - LOG_ID_FSSO_SVR_STATUS

Message ID: 38033

Message Description: LOG_ID_FSSO_SVR_STATUS

Message Meaning: FSSO Active Directory server authentication status

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38403 - LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE

Message ID: 38403

Message Description: LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE

Message Meaning: Insufficient system resource notification

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38404 - LOGID_EVENT_NOTIF_HOSTNAME_ERROR

Message ID: 38404

Message Description: LOGID_EVENT_NOTIF_HOSTNAME_ERROR

Message Meaning: FortiGuard hostname unresolvable

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
hostname	Hostname	string	128
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38405 - LOGID_NOTIF_CODE_SENDTO_SMS_PHONE

Message ID: 38405

Message Description: LOGID_NOTIF_CODE_SENDTO_SMS_PHONE

Message Meaning: Guest user account login information sent to phone

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38406 - LOGID_NOTIF_CODE_SENDTO_SMS_TO

Message ID: 38406

Message Description: LOGID_NOTIF_CODE_SENDTO_SMS_TO

Message Meaning: Guest user account login information sent as SMS

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38407 - LOGID_NOTIF_CODE_SENDTO_EMAIL

Message ID: 38407

Message Description: LOGID_NOTIF_CODE_SENDTO_EMAIL

Message Meaning: Guest user account login information sent to email

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38408 - LOGID_EVENT_OFTP_SSL_CONNECTED

Message ID: 38408

Message Description: LOGID_EVENT_OFTP_SSL_CONNECTED

Message Meaning: SSL connection established

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38409 - LOGID_EVENT_OFTP_SSL_DISCONNECTED

Message ID: 38409

Message Description: LOGID_EVENT_OFTP_SSL_DISCONNECTED

Message Meaning: SSL connection closed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38410 - LOGID_EVENT_OFTP_SSL_FAILED

Message ID: 38410

Message Description: LOGID_EVENT_OFTP_SSL_FAILED

Message Meaning: SSL connection failed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38411 - LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO

Message ID: 38411

Message Description: LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO

Message Meaning: Two-factor authentication code sent

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38412 - LOGID_EVENT_TOKEN_CODE_SENDTO

Message ID: 38412

Message Description: LOGID_EVENT_TOKEN_CODE_SENDTO

Message Meaning: Token activation code sent

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38656 - LOGID_EVENT_RAD_RPT_PROTO_ERROR

Message ID: 38656

Message Description: LOGID_EVENT_RAD_RPT_PROTO_ERROR

Message Meaning: RADIUS protocol error summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38657 - LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND

Message ID: 38657

Message Description: LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND

Message Meaning: RADIUS profile not found summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38658 - LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND

Message ID: 38658

Message Description: LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND

Message Meaning: RADIUS profile CTX not found summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38659 - LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED

Message ID: 38659

Message Description: LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED

Message Meaning: RADIUS accounting stop message missing summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38660 - LOGID_EVENT_RAD_RPT_ACCT_EVENT

Message ID: 38660

Message Description: LOGID_EVENT_RAD_RPT_ACCT_EVENT

Message Meaning: RADIUS accounting event summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38661 - LOGID_EVENT_RAD_RPT_OTHER

Message ID: 38661

Message Description: LOGID_EVENT_RAD_RPT_OTHER

Message Meaning: RADIUS endpoint block event or other event summary

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration	uint32	10
count	Number of Packets	uint32	10
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38662 - LOGID_EVENT_RAD_STAT_PROTO_ERROR

Message ID: 38662

Message Description: LOGID_EVENT_RAD_STAT_PROTO_ERROR

Message Meaning: RADIUS accounting protocol error

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38663 - LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND

Message ID: 38663

Message Description: LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND

Message Meaning: RADIUS accounting profile not found

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38665 - LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED

Message ID: 38665

Message Description: LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED

Message Meaning: RADIUS accounting stop message missing

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

38666 - LOGID_EVENT_RAD_STAT_ACCT_EVENT

Message ID: 38666

Message Description: LOGID_EVENT_RAD_STAT_ACCT_EVENT

Message Meaning: RADIUS accounting event

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38667 - LOGID_EVENT_RAD_STAT_OTHER

Message ID: 38667

Message Description: LOGID_EVENT_RAD_STAT_OTHER

Message Meaning: RADIUS other accounting event

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
count	Number of Packets	uint32	10
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

38668 - LOGID_EVENT_RAD_STAT_EP_BLK

Message ID: 38668

Message Description: LOGID_EVENT_RAD_STAT_EP_BLK

Message Meaning: RADIUS endpoint block event

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
acct_stat	Accounting state (RADIUS)	string	14
rsso_key	RADIUS SSO attribute value	string	64
carrier_ep	The FortiOS Carrier end-point identification	string	64
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39424 - LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP

Message ID: 39424

Message Description: LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP

Message Meaning: SSL VPN tunnel up

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39425 - LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN

Message ID: 39425

Message Description: LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN

Message Meaning: SSL VPN tunnel down

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39426 - LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL

Message ID: 39426

Message Description: LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL

Message Meaning: SSL VPN login fail

Type: Event

Category: vpn

Severity: Alert

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39936 - LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_STATS

Message ID: 39936

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_STATS

Message Meaning: SSL VPN statistics

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
nextstat	Time interval in seconds for the next statistics	uint32	10
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39937 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY

Message ID: 39937

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY

Message Meaning: SSL VPN deny

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39938 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS

Message ID: 39938

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS

Message Meaning: SSL VPN pass

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39939 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT

Message ID: 39939

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT

Message Meaning: SSL VPN timeout

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39940 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE

Message ID: 39940

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE

Message Meaning: SSL VPN close

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39941 - LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY

Message ID: 39941

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY

Message Meaning: SSL VPN system busy

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39942 - LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK

Message ID: 39942

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK

Message Meaning: SSL VPN certificate OK

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39943 - LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON

Message ID: 39943

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON

Message Meaning: SSL VPN new connection

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39944 - LOG_ID_EVENT_SSL_VPN_SESSION_ALERT

Message ID: 39944

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_ALERT

Message Meaning: SSL VPN alert

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
desc	Description	string	128
dst_host	Destination Host	string	64
reason	Reason	string	256
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39945 - LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL

Message ID: 39945

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL

Message Meaning: SSL VPN exit fail

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39946 - LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR

Message ID: 39946

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR

Message Meaning: SSL VPN exit error

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39947 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP

Message ID: 39947

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP

Message Meaning: SSL VPN tunnel up

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39948 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN

Message ID: 39948

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN

Message Meaning: SSL VPN tunnel down

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39949 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS

Message ID: 39949

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS

Message Meaning: SSL VPN statistics

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
nextstat	Time interval in seconds for the next statistics	uint32	10
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
duration	Duration	uint32	10
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39950 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UNKNOWNTAG

Message ID: 39950

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UNKNOWNTAG

Message Meaning: SSL VPN unknown tag

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39951 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR

Message ID: 39951

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR

Message Meaning: SSL VPN tunnel error

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39952 - LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_MODE

Message ID: 39952

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_MODE

Message Meaning: SSL VPN enter conserve mode

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

39953 - LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_MODE

Message ID: 39953

Message Description: LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_MODE

Message Meaning: SSL VPN leave conserve mode

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
dst_host	Destination Host	string	64
reason	Reason	string	256
fctuid		string	32
srccountry		string	64
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40001 - LOG_ID_PPTP_TUNNEL_UP

Message ID: 40001

Message Description: LOG_ID_PPTP_TUNNEL_UP

Message Meaning: PPTP tunnel up

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40002 - LOG_ID_PPTP_TUNNEL_DOWN

Message ID: 40002

Message Description: LOG_ID_PPTP_TUNNEL_DOWN

Message Meaning: PPTP tunnel down

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40003 - LOG_ID_PPTP_TUNNEL_STAT

Message ID: 40003

Message Description: LOG_ID_PPTP_TUNNEL_STAT

Message Meaning: PPTP tunnel status

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40014 - LOG_ID_PPTP_REACH_MAX_CON

Message ID: 40014

Message Description: LOG_ID_PPTP_REACH_MAX_CON

Message Meaning: PPTP client connection limit reached

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40017 - LOG_ID_L2TPD_CLIENT_CON_FAIL

Message ID: 40017

Message Description: LOG_ID_L2TPD_CLIENT_CON_FAIL

Message Meaning: L2TP client connection failed

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40019 - LOG_ID_L2TPD_CLIENT_DISCON

Message ID: 40019

Message Description: LOG_ID_L2TPD_CLIENT_DISCON

Message Meaning: L2TP client disconnected

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40021 - LOG_ID_PPTP_NOT_CONIG

Message ID: 40021

Message Description: LOG_ID_PPTP_NOT_CONIG

Message Meaning: PPTP not configured in VDOM

Type: Event

Category: vpn

Severity: Debug

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40022 - LOG_ID_PPTP_NO_IP_AVAIL

Message ID: 40022

Message Description: LOG_ID_PPTP_NO_IP_AVAIL

Message Meaning: PPTP IP addresses unavailable

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40024 - LOG_ID_PPTP_OUT_MEM

Message ID: 40024

Message Description: LOG_ID_PPTP_OUT_MEM

Message Meaning: PPTP config list insufficient memory

Type: Event

Category: vpn

Severity: Warning

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40034 - LOG_ID_PPTP_START

Message ID: 40034

Message Description: LOG_ID_PPTP_START

Message Meaning: PPTP daemon started

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40035 - LOG_ID_PPTP_START_FAIL

Message ID: 40035

Message Description: LOG_ID_PPTP_START_FAIL

Message Meaning: PPTP daemon failed to start

Type: Event

Category: vpn

Severity: Error

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40036 - LOG_ID_PPTP_EXIT

Message ID: 40036

Message Description: LOG_ID_PPTP_EXIT

Message Meaning: PPTP daemon exited

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40037 - LOG_ID_PPTPD_SVR_DISCON

Message ID: 40037

Message Description: LOG_ID_PPTPD_SVR_DISCON

Message Meaning: PPTP daemon disconnected

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40038 - LOG_ID_PPTPD_CLIENT_CON

Message ID: 40038

Message Description: LOG_ID_PPTPD_CLIENT_CON

Message Meaning: PPTP client connected

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40039 - LOG_ID_PPTPD_CLIENT_DISCON

Message ID: 40039

Message Description: LOG_ID_PPTPD_CLIENT_DISCON

Message Meaning: PPTP client disconnected

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40101 - LOG_ID_L2TP_TUNNEL_UP

Message ID: 40101

Message Description: LOG_ID_L2TP_TUNNEL_UP

Message Meaning: L2TP tunnel up

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40102 - LOG_ID_L2TP_TUNNEL_DOWN

Message ID: 40102

Message Description: LOG_ID_L2TP_TUNNEL_DOWN

Message Meaning: L2TP tunnel down

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40103 - LOG_ID_L2TP_TUNNEL_STAT

Message ID: 40103

Message Description: LOG_ID_L2TP_TUNNEL_STAT

Message Meaning: L2TP tunnel status

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
group	User group Name	string	512
user	User name of authenticated user	string	256
tunnelip	IPsec VPN tunnel IP address	ip	39

Log Field Name	Description	Data Type	Length
remip	IPsec VPN remote gateway IP address	ip	39
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40114 - LOG_ID_L2TPD_START

Message ID: 40114

Message Description: LOG_ID_L2TPD_START

Message Meaning: L2TP daemon started

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40115 - LOG_ID_L2TPD_EXIT

Message ID: 40115

Message Description: LOG_ID_L2TPD_EXIT

Message Meaning: L2TP daemon exited

Type: Event

Category: vpn

Severity: Notice

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40118 - LOG_ID_L2TPD_CLIENT_CON

Message ID: 40118

Message Description: LOG_ID_L2TPD_CLIENT_CON

Message Meaning: L2TP client connected

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40704 - LOG_ID_EVENT_SYS_PERF

Message ID: 40704

Message Description: LOG_ID_EVENT_SYS_PERF

Message Meaning: System performance statistics

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
waninfo		string	512
sysuptime		uint32	10
freediskstorage		uint32	10
fazlograte	FortiAnalyzer Logging Rate	uint64	20
disklograte	Disk Log Rate	uint64	20
setuprate	Session Setup Rate	uint64	20
bandwidth	Bandwidth	string	42
disk	Disk Usage	uint8	3
totalsession	Total Number of Sessions	uint32	10
mem	Memory Usage	uint8	3
cpu	CPU Usage	uint8	3
sn	Serial Number	string	64
name	Display Name of the Connection	string	128
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

This log message is only sent to remote FortiAnalyzer and memory, but not to disk.

40705 - LOG_ID_EVENT_SYS_CPU_USAGE

Message ID: 40705

Message Description: LOG_ID_EVENT_SYS_CPU_USAGE

Message Meaning: CPU usage statistics

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
cpu	CPU Usage	uint8	3
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40706 - LOG_ID_EVENT_SYS_BROKEN_SYMBOLIC_LINK

Message ID: 40706

Message Description: LOG_ID_EVENT_SYS_BROKEN_SYMBOLIC_LINK

Message Meaning: Delete broken symbolic link

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40707 - LOG_ID_EVENT_SYS_CPU_USAGE_SINGLE_CORE

Message ID: 40707

Message Description: LOG_ID_EVENT_SYS_CPU_USAGE_SINGLE_CORE

Message Meaning: CPU single core usage statistics

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
core		uint8	3
cpu	CPU Usage	uint8	3
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

40960 - LOGID_EVENT_WEBPROXY_FWD_SRV_ERROR

Message ID: 40960

Message Description: LOGID_EVENT_WEBPROXY_FWD_SRV_ERROR

Message Meaning: Web proxy forward server error

Type: Event

Category: webproxy

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
port	Port Number	uint16	5
fqdn	Fully Qualified Domain Name	string	256
ip		ip	39
addr_type		string	4
fwserver_name		string	32
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

40961 - LOGID_EVENT_ICAP_REMOTE_SRV_STAT

Message ID: 40961

Message Description: LOGID_EVENT_ICAP_REMOTE_SRV_STAT

Message Meaning: Icap remote server stat

Type: Event

Category: webproxy

Severity: Notice

Log Field Name	Description	Data Type	Length
serveraddr		string	80
servername		string	32
msg	Log Message	string	4096
port	Port Number	uint16	5
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41000 - LOG_ID_UPD_FGT_SUCC

Message ID: 41000

Message Description: LOG_ID_UPD_FGT_SUCC

Message Meaning: FortiGate update succeeded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41001 - LOG_ID_UPD_FGT_FAIL

Message ID: 41001

Message Description: LOG_ID_UPD_FGT_FAIL

Message Meaning: FortiGate update failed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41002 - LOG_ID_UPD_SRC_VIS

Message ID: 41002

Message Description: LOG_ID_UPD_SRC_VIS

Message Meaning: Source visibility signature package updated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41006 - LOG_ID_UPD_FSA_VIRDB

Message ID: 41006

Message Description: LOG_ID_UPD_FSA_VIRDB

Message Meaning: FortiSandbox AV database updated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
version	Version	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41007 - LOG_ID_UPD_MANUAL_LICENSE_SUCC

Message ID: 41007

Message Description: LOG_ID_UPD_MANUAL_LICENSE_SUCC

Message Meaning: FortiGate Manual License update

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41008 - LOG_ID_UPD_MANUAL_LICENSE_FAIL

Message ID: 41008

Message Description: LOG_ID_UPD_MANUAL_LICENSE_FAIL

Message Meaning: FortiGate Manual License is invalid

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41009 - LOG_ID_UPD_DB_SIGN_INVALID

Message ID: 41009

Message Description: LOG_ID_UPD_DB_SIGN_INVALID

Message Meaning: FortiGate database signature invalid

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

41011 - LOG_ID_UPD_DB_UNSIGNED_INSTALLED

Message ID: 41011

Message Description: LOG_ID_UPD_DB_UNSIGNED_INSTALLED

Message Meaning: FortiGate database without signature installed

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41984 - LOG_ID_EVENT_VPN_CERT_LOAD

Message ID: 41984

Message Description: LOG_ID_EVENT_VPN_CERT_LOAD

Message Meaning: Certificate loaded

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41985 - LOG_ID_EVENT_VPN_CERT_REMOVAL

Message ID: 41985

Message Description: LOG_ID_EVENT_VPN_CERT_REMOVAL

Message Meaning: Certificate removed

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41986 - LOG_ID_EVENT_VPN_CERT_REGEN

Message ID: 41986

Message Description: LOG_ID_EVENT_VPN_CERT_REGEN

Message Meaning: Certificate regenerated

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41987 - LOG_ID_EVENT_VPN_CERT_UPDATE

Message ID: 41987

Message Description: LOG_ID_EVENT_VPN_CERT_UPDATE

Message Meaning: Certificate updated

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
reason	Reason	string	256
status	Status	string	23
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41988 - LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE

Message ID: 41988

Message Description: LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE

Message Meaning: SSL setting changed

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
msg	Log Message	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41989 - LOG_ID_EVENT_VPN_CERT_ERR

Message ID: 41989

Message Description: LOG_ID_EVENT_VPN_CERT_ERR

Message Meaning: Certificate error

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

41990 - LOG_ID_EVENT_VPN_CERT_UPDATE_FAILED

Message ID: 41990

Message Description: LOG_ID_EVENT_VPN_CERT_UPDATE_FAILED

Message Meaning: Certificate update failed

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
reason	Reason	string	256
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41991 - LOG_ID_EVENT_VPN_CERT_EXPORT

Message ID: 41991

Message Description: LOG_ID_EVENT_VPN_CERT_EXPORT

Message Meaning: Certificate exported

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

41992 - LOG_ID_EVENT_VPN_CERT_CRL_EXPIRED

Message ID: 41992

Message Description: LOG_ID_EVENT_VPN_CERT_CRL_EXPIRED

Message Meaning: CRL certificate file is expired

Type: Event

Category: vpn

Severity: Information

Log Field Name	Description	Data Type	Length
method	Method	string	64
cert-type	Certification type	string	6
name	Display Name of the Connection	string	128
status	Status	string	23
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43008 - LOG_ID_EVENT_AUTH_SUCCESS

Message ID: 43008

Message Description: LOG_ID_EVENT_AUTH_SUCCESS

Message Meaning: Authentication success

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512

Log Field Name	Description	Data Type	Length
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43009 - LOG_ID_EVENT_AUTH_FAILED

Message ID: 43009

Message Description: LOG_ID_EVENT_AUTH_FAILED

Message Meaning: Authentication failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43010 - LOG_ID_EVENT_AUTH_LOCKOUT

Message ID: 43010

Message Description: LOG_ID_EVENT_AUTH_LOCKOUT

Message Meaning: Authentication lockout

Type: Event

Category: user

Severity: Warning

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43011 - LOG_ID_EVENT_AUTH_TIME_OUT

Message ID: 43011

Message Description: LOG_ID_EVENT_AUTH_TIME_OUT

Message Meaning: Authentication timed out

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43014 - LOG_ID_EVENT_AUTH_FSAE_LOGON

Message ID: 43014

Message Description: LOG_ID_EVENT_AUTH_FSAE_LOGON

Message Meaning: FSSO logon authentication status

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43015 - LOG_ID_EVENT_AUTH_FSAE_LOGOFF

Message ID: 43015

Message Description: LOG_ID_EVENT_AUTH_FSAE_LOGOFF

Message Meaning: FSSO log off authentication status

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43016 - LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS

Message ID: 43016

Message Description: LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS

Message Meaning: NTLM authentication successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
adgroup	AD Group Name of FSSO user	string	128
group	User group Name	string	512
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43017 - LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL

Message ID: 43017

Message Description: LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL

Message Meaning: NTLM authentication failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
adgroup	AD Group Name of FSSO user	string	128
group	User group Name	string	512
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43018 - LOG_ID_EVENT_AUTH_FGOVRD_FAIL

Message ID: 43018

Message Description: LOG_ID_EVENT_AUTH_FGOVRD_FAIL

Message Meaning: FortiGuard override failed

Type: Event

Category: user

Severity: Warning

Log Field Name	Description	Data Type	Length
initiator	Original login user name for Fortiguard override	string	64
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43020 - LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS

Message ID: 43020

Message Description: LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS

Message Meaning: FortiGuard override successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
oldwprof	Old Web Filter Profile	string	64
expiry	FortiGuard override expiry timestamp	string	64
scope	FortiGuard Override Scope	string	16
initiator	Original login user name for Fortiguard override	string	64
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43025 - LOG_ID_EVENT_AUTH_PROXY_SUCCESS

Message ID: 43025

Message Description: LOG_ID_EVENT_AUTH_PROXY_SUCCESS

Message Meaning: Explicit proxy authentication successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43026 - LOG_ID_EVENT_AUTH_PROXY_FAILED

Message ID: 43026

Message Description: LOG_ID_EVENT_AUTH_PROXY_FAILED

Message Meaning: Explicit proxy authentication failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43027 - LOG_ID_EVENT_AUTH_PROXY_TIME_OUT

Message ID: 43027

Message Description: LOG_ID_EVENT_AUTH_PROXY_TIME_OUT

Message Meaning: Explicit proxy authentication timed out

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43028 - LOG_ID_EVENT_AUTH_PROXY_GROUP_INFO_FAILED

Message ID: 43028

Message Description: LOG_ID_EVENT_AUTH_PROXY_GROUP_INFO_FAILED

Message Meaning: Explicit proxy user group query failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43029 - LOG_ID_EVENT_AUTH_WARNING_SUCCESS

Message ID: 43029

Message Description: LOG_ID_EVENT_AUTH_WARNING_SUCCESS

Message Meaning: FortiGuard authentication override successful

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
category	Log category	uint32	10
oldwprof	Old Web Filter Profile	string	64
expiry	FortiGuard override expiry timestamp	string	64
scope	FortiGuard Override Scope	string	16
initiator	Original login user name for Fortiguard override	string	64
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43030 - LOG_ID_EVENT_AUTH_WARNING_TBL_FULL

Message ID: 43030

Message Description: LOG_ID_EVENT_AUTH_WARNING_TBL_FULL

Message Meaning: FortiGuard authentication override failed

Type: Event

Category: user

Severity: Warning

Log Field Name	Description	Data Type	Length
initiator	Original login user name for Fortiguard override	string	64
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43032 - LOG_ID_EVENT_AUTH_PROXY_USER_LIMIT_REACHED

Message ID: 43032

Message Description: LOG_ID_EVENT_AUTH_PROXY_USER_LIMIT_REACHED

Message Meaning: Explicit proxy authentication user limit reached

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43033 - LOG_ID_EVENT_AUTH_PROXY_MULTIPLE_LOGIN

Message ID: 43033

Message Description: LOG_ID_EVENT_AUTH_PROXY_MULTIPLE_LOGIN

Message Meaning: Explicit proxy authentication user concurrent check failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authid		string	36
group	User group Name	string	512
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43034 - LOG_ID_EVENT_AUTH_PROXY_NO_RESP

Message ID: 43034

Message Description: LOG_ID_EVENT_AUTH_PROXY_NO_RESP

Message Meaning: Explicit proxy authentication no response

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
agent	SNMP agent	string	1024
url	URL	string	512
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43037 - LOG_ID_EVENT_AUTH_IPV4_FLUSH

Message ID: 43037

Message Description: LOG_ID_EVENT_AUTH_IPV4_FLUSH

Message Meaning: Authentication IPv4 logon flush

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43038 - LOG_ID_EVENT_AUTH_IPV6_FLUSH

Message ID: 43038

Message Description: LOG_ID_EVENT_AUTH_IPV6_FLUSH

Message Meaning: Authentication IPv6 logon flush

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43039 - LOG_ID_EVENT_AUTH_LOGON

Message ID: 43039

Message Description: LOG_ID_EVENT_AUTH_LOGON

Message Meaning: Authentication logon

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43040 - LOG_ID_EVENT_AUTH_LOGOUT

Message ID: 43040

Message Description: LOG_ID_EVENT_AUTH_LOGOUT

Message Meaning: Authentication logout

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43041 - LOG_ID_EVENT_AUTH_DISCLAIMER_ACCEPT

Message ID: 43041

Message Description: LOG_ID_EVENT_AUTH_DISCLAIMER_ACCEPT

Message Meaning: Disclaimer accepted

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43042 - LOG_ID_EVENT_AUTH_DISCLAIMER_DECLINE

Message ID: 43042

Message Description: LOG_ID_EVENT_AUTH_DISCLAIMER_DECLINE

Message Meaning: Disclaimer declined

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43043 - LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_SUCCESS

Message ID: 43043

Message Description: LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_SUCCESS

Message Meaning: Email collecting succeeded

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43044 - LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_FAIL

Message ID: 43044

Message Description: LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_FAIL

Message Meaning: Email collecting failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
group	User group Name	string	512
interface	Interface	string	32
policyid	Policy ID	uint32	10
dstip	Destination IP	ip	39
reason	Reason	string	256
srcip	Source IP	ip	39
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
authproto	The protocol that initiated the authentication	string	512
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43045 - LOG_ID_EVENT_AUTH_8021X_SUCCESS

Message ID: 43045

Message Description: LOG_ID_EVENT_AUTH_8021X_SUCCESS

Message Meaning: 802.1x authentication succeeded

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
interface	Interface	string	32
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43046 - LOG_ID_EVENT_AUTH_8021X_FAIL

Message ID: 43046

Message Description: LOG_ID_EVENT_AUTH_8021X_FAIL

Message Meaning: 802.1x authentication failed

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
interface	Interface	string	32
reason	Reason	string	256
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43050 - LOG_ID_EVENT_AUTH_FSAE_CONNECT

Message ID: 43050

Message Description: LOG_ID_EVENT_AUTH_FSAE_CONNECT

Message Meaning: FSSO server connected

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43051 - LOG_ID_EVENT_AUTH_FSAE_DISCONNECT

Message ID: 43051

Message Description: LOG_ID_EVENT_AUTH_FSAE_DISCONNECT

Message Meaning: FSSO server disconnected

Type: Event

Category: user

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43520 - LOG_ID_EVENT_WIRELESS_SYS

Message ID: 43520

Message Description: LOG_ID_EVENT_WIRELESS_SYS

Message Meaning: Wireless system activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43521 - LOG_ID_EVENT_WIRELESS_ROGUE

Message ID: 43521

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE

Message Meaning: Rogue AP activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43522 - LOG_ID_EVENT_WIRELESS_WTP

Message ID: 43522

Message Description: LOG_ID_EVENT_WIRELESS_WTP

Message Meaning: Physical AP activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43524 - LOG_ID_EVENT_WIRELESS_STA

Message ID: 43524

Message Description: LOG_ID_EVENT_WIRELESS_STA

Message Meaning: Wireless client activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43525 - LOG_ID_EVENT_WIRELESS_ONWIRE

Message ID: 43525

Message Description: LOG_ID_EVENT_WIRELESS_ONWIRE

Message Meaning: Rogue AP on wire

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43526 - LOG_ID_EVENT_WIRELESS_WTPR

Message ID: 43526

Message Description: LOG_ID_EVENT_WIRELESS_WTPR

Message Meaning: Physical AP radio activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43527 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG

Message ID: 43527

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_CFG

Message Meaning: Rogue AP status configured

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43528 - LOG_ID_EVENT_WIRELESS_WTPR_ERROR

Message ID: 43528

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_ERROR

Message Meaning: Physical AP radio error activity

Type: Event

Category: wireless

Severity: Error

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43529 - LOG_ID_EVENT_WIRELESS_CLB

Message ID: 43529

Message Description: LOG_ID_EVENT_WIRELESS_CLB

Message Meaning: Wireless client load balancing

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stacount	The count of wifi stations	uint32	10
stamac	The MAC address of wifi station	string	17
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43530 - LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE

Message ID: 43530

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE

Message Meaning: Wireless bridge intrusion detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43531 - LOG_ID_EVENT_WIRELESS_WIDS_BR_DEAUTH

Message ID: 43531

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_BR_DEAUTH

Message Meaning: Wireless broadcasting deauthentication detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43532 - LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP

Message ID: 43532

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP

Message Meaning: Wireless null SSID probe response detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43533 - LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI

Message ID: 43533

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI

Message Meaning: Wireless invalid MAC OUI detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
invalidmac	Detected MAC address with invalid OUI	string	17
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10

Log Field Name	Description	Data Type	Length
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43534 - LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR

Message ID: 43534

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR

Message Meaning: Wireless long duration attack detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration of the last threatening packed captured from TA	uint32	10
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512

Log Field Name	Description	Data Type	Length
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43535 - LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV

Message ID: 43535

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV

Message Meaning: Wireless Weak WEP IV detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
weakwepiv	Weak Wep Initiation Vector	string	8
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43542 - LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD

Message ID: 43542

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD

Message Meaning: Wireless EAPOL packet flooding detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
eapolcnt	The count of EAPOL packets	uint32	10
eapoltype	The packet type of EAPOL	string	16
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43544 - LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD

Message ID: 43544

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD

Message Meaning: Wireless management flooding detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mgmtcnt	The number of unauthorized client flooding managemet frames	uint32	10
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43546 - LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH

Message ID: 43546

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH

Message Meaning: Wireless spoofed deauthentication detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43548 - LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP

Message ID: 43548

Message Description: LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP

Message Meaning: Wireless Asleap attack detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
encrypt	The packet is encrypted or not	uint8	3
seq	Sequence	string	512
ds	Direction with distribution system	string	8
frametype	Frame Type	string	32
rssi	The value of Received signal strength indicator	uint8	3
threattype	WIDS threat type	string	64
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
age	Time in seconds - time passed since last seen	uint32	10

Log Field Name	Description	Data Type	Length
live	Time in seconds	uint32	10
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43550 - LOG_ID_EVENT_WIRELESS_STA_LOCATE

Message ID: 43550

Message Description: LOG_ID_EVENT_WIRELESS_STA_LOCATE

Message Meaning: Wireless station presence detection

Type: Event

Category: wireless

Severity: Information

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17

Log Field Name	Description	Data Type	Length
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
radioband	The operating radio band	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43551 - LOG_ID_EVENT_WIRELESS_WTP_JOIN

Message ID: 43551

Message Description: LOG_ID_EVENT_WIRELESS_WTP_JOIN

Message Meaning: Physical AP join

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43552 - LOG_ID_EVENT_WIRELESS_WTP_LEAVE

Message ID: 43552

Message Description: LOG_ID_EVENT_WIRELESS_WTP_LEAVE

Message Meaning: Physical AP leave

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43553 - LOG_ID_EVENT_WIRELESS_WTP_FAIL

Message ID: 43553

Message Description: LOG_ID_EVENT_WIRELESS_WTP_FAIL

Message Meaning: Physical AP fail

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43554 - LOG_ID_EVENT_WIRELESS_WTP_UPDATE

Message ID: 43554

Message Description: LOG_ID_EVENT_WIRELESS_WTP_UPDATE

Message Meaning: Physical AP update

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43555 - LOG_ID_EVENT_WIRELESS_WTP_RESET

Message ID: 43555

Message Description: LOG_ID_EVENT_WIRELESS_WTP_RESET

Message Meaning: Physical AP reset

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43556 - LOG_ID_EVENT_WIRELESS_WTP_KICK

Message ID: 43556

Message Description: LOG_ID_EVENT_WIRELESS_WTP_KICK

Message Meaning: Physical AP kick

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43557 - LOG_ID_EVENT_WIRELESS_WTP_ADD_FAILURE

Message ID: 43557

Message Description: LOG_ID_EVENT_WIRELESS_WTP_ADD_FAILURE

Message Meaning: Physical AP add failure

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43558 - LOG_ID_EVENT_WIRELESS_WTP_CFG_ERR

Message ID: 43558

Message Description: LOG_ID_EVENT_WIRELESS_WTP_CFG_ERR

Message Meaning: Physical AP config error

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43559 - LOG_ID_EVENT_WIRELESS_WTP_SN_MISMATCH

Message ID: 43559

Message Description: LOG_ID_EVENT_WIRELESS_WTP_SN_MISMATCH

Message Meaning: Physical AP SN mismatch

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43560 - LOG_ID_EVENT_WIRELESS_SYS_AC_RESTARTED

Message ID: 43560

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_RESTARTED

Message Meaning: Wireless system restarted

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43561 - LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_UP

Message ID: 43561

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_UP

Message Meaning: Wireless system hostapd up

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43562 - LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_DOWN

Message ID: 43562

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_DOWN

Message Meaning: Wireless system hostapd down

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43563 - LOG_ID_EVENT_WIRELESS_ROGUE_DETECT

Message ID: 43563

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_DETECT

Message Meaning: Rogue AP detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43564 - LOG_ID_EVENT_WIRELESS_ROGUE_OFFAIR

Message ID: 43564

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_OFFAIR

Message Meaning: Rogue AP off air

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43565 - LOG_ID_EVENT_WIRELESS_ROGUE_ONAIR

Message ID: 43565

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_ONAIR

Message Meaning: Rogue AP on air

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43566 - LOG_ID_EVENT_WIRELESS_ROGUE_OFFWIRE

Message ID: 43566

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_OFFWIRE

Message Meaning: Rogue AP off wire

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43567 - LOG_ID_EVENT_WIRELESS_FAKEAP_DETECT

Message ID: 43567

Message Description: LOG_ID_EVENT_WIRELESS_FAKEAP_DETECT

Message Meaning: Fake AP detected

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43568 - LOG_ID_EVENT_WIRELESS_FAKEAP_ONAIR

Message ID: 43568

Message Description: LOG_ID_EVENT_WIRELESS_FAKEAP_ONAIR

Message Meaning: Fake AP on air

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43569 - LOG_ID_EVENT_WIRELESS_ROGUE_SUPPRESSED

Message ID: 43569

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_SUPPRESSED

Message Meaning: Rogue AP suppressed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43570 - LOG_ID_EVENT_WIRELESS_ROGUE_UNSUPPRESSED

Message ID: 43570

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_UNSUPPRESSED

Message Meaning: Rogue AP unsuppressed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3

Log Field Name	Description	Data Type	Length
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43571 - LOG_ID_EVENT_WIRELESS_ROGUE_DETECT_CHG

Message ID: 43571

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_DETECT_CHG

Message Meaning: Rogue AP change detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3

Log Field Name	Description	Data Type	Length
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43572 - LOG_ID_EVENT_WIRELESS_STA_ASSO

Message ID: 43572

Message Description: LOG_ID_EVENT_WIRELESS_STA_ASSO

Message Meaning: Wireless client associated

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43573 - LOG_ID_EVENT_WIRELESS_STA_AUTH

Message ID: 43573

Message Description: LOG_ID_EVENT_WIRELESS_STA_AUTH

Message Meaning: Wireless client authenticated

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4

Log Field Name	Description	Data Type	Length
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43574 - LOG_ID_EVENT_WIRELESS_STA_DASS

Message ID: 43574

Message Description: LOG_ID_EVENT_WIRELESS_STA_DASS

Message Meaning: Wireless client disassociated

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
mpsk	Multiple pre-shared keys	string	33

Log Field Name	Description	Data Type	Length
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43575 - LOG_ID_EVENT_WIRELESS_STA_DAUT

Message ID: 43575

Message Description: LOG_ID_EVENT_WIRELESS_STA_DAUT

Message Meaning: Wireless client deauthenticated

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43576 - LOG_ID_EVENT_WIRELESS_STA_IDLE

Message ID: 43576

Message Description: LOG_ID_EVENT_WIRELESS_STA_IDLE

Message Meaning: Wireless client idle

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43577 - LOG_ID_EVENT_WIRELESS_STA_DENY

Message ID: 43577

Message Description: LOG_ID_EVENT_WIRELESS_STA_DENY

Message Meaning: Wireless client denied

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32

Log Field Name	Description	Data Type	Length
snprev		string	36
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43578 - LOG_ID_EVENT_WIRELESS_STA_KICK

Message ID: 43578

Message Description: LOG_ID_EVENT_WIRELESS_STA_KICK

Message Meaning: Wireless client kicked

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43579 - LOG_ID_EVENT_WIRELESS_STA_IP

Message ID: 43579

Message Description: LOG_ID_EVENT_WIRELESS_STA_IP

Message Meaning: Wireless client IP assigned

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43580 - LOG_ID_EVENT_WIRELESS_STA_LEAVE_WTP

Message ID: 43580

Message Description: LOG_ID_EVENT_WIRELESS_STA_LEAVE_WTP

Message Meaning: Wireless client left WTP

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43581 - LOG_ID_EVENT_WIRELESS_STA_WTP_DISCONN

Message ID: 43581

Message Description: LOG_ID_EVENT_WIRELESS_STA_WTP_DISCONN

Message Meaning: Wireless client WTP disconnected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43582 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_UNCLASSIFIED

Message ID: 43582

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_CFG_UNCLASSIFIED

Message Meaning: Rogue AP status configured as unclassified

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43583 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ACCEPTED

Message ID: 43583

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ACCEPTED

Message Meaning: Rogue AP status configured as accepted

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43584 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ROGUE

Message ID: 43584

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ROGUE

Message Meaning: Rogue AP status configured as rogue

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43585 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_SUPPRESSED

Message ID: 43585

Message Description: LOG_ID_EVENT_WIRELESS_ROGUE_CFG_SUPPRESSED

Message Meaning: Rogue AP status configured as suppressed

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43586 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_CHAN

Message ID: 43586

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DARRP_CHAN

Message Meaning: Physical AP radio DARRP channel change

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43587 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_START

Message ID: 43587

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DARRP_START

Message Meaning: Physical AP radio DARRP start

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43588 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_CHAN

Message ID: 43588

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_OPER_CHAN

Message Meaning: Physical AP radio operation channel change

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43589 - LOG_ID_EVENT_WIRELESS_WTPR_RADAR

Message ID: 43589

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_RADAR

Message Meaning: Physical AP radio radar detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43590 - LOG_ID_EVENT_WIRELESS_WTPR_NOL

Message ID: 43590

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_NOL

Message Meaning: Physical AP radio channel removed from NOL

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4

Log Field Name	Description	Data Type	Length
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43591 - LOG_ID_EVENT_WIRELESS_WTPR_COUNTRY_CFG_SUCCESS

Message ID: 43591

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_COUNTRY_CFG_SUCCESS

Message Meaning: Physical AP radio country config success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43592 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_COUNTRY

Message ID: 43592

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_OPER_COUNTRY

Message Meaning: Physical AP radio operation country

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43593 - LOG_ID_EVENT_WIRELESS_WTPR_CFG_TXPOWER

Message ID: 43593

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_CFG_TXPOWER

Message Meaning: Physical AP radio config TX power

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43594 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_TXPOWER

Message ID: 43594

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_OPER_TXPOWER

Message Meaning: Physical AP radio operation TX power

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43595 - LOG_ID_EVENT_WIRELESS_CLB_DENY

Message ID: 43595

Message Description: LOG_ID_EVENT_WIRELESS_CLB_DENY

Message Meaning: Wireless client load balancing denied

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stacount	The count of wifi stations	uint32	10
stamac	The MAC address of wifi station	string	17
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43596 - LOG_ID_EVENT_WIRELESS_CLB_RETRY

Message ID: 43596

Message Description: LOG_ID_EVENT_WIRELESS_CLB_RETRY

Message Meaning: Wireless client load balancing retry

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stacount	The count of wifi stations	uint32	10
stamac	The MAC address of wifi station	string	17
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43597 - LOG_ID_EVENT_WIRELESS_WTP_ADD

Message ID: 43597

Message Description: LOG_ID_EVENT_WIRELESS_WTP_ADD

Message Meaning: Physical AP add

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43598 - LOG_ID_EVENT_WIRELESS_WTP_ADD_XSS

Message ID: 43598

Message Description: LOG_ID_EVENT_WIRELESS_WTP_ADD_XSS

Message Meaning: Physical AP add XSS

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43599 - LOG_ID_EVENT_WIRELESS_WTP_DEL

Message ID: 43599

Message Description: LOG_ID_EVENT_WIRELESS_WTP_DEL

Message Meaning: Physical AP delete

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43600 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_STOP

Message ID: 43600

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DARRP_STOP

Message Meaning: Physical AP radio DARRP stop

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43601 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON

Message ID: 43601

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON

Message Meaning: Wireless station sign on

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43602 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_SUCCESS

Message ID: 43602

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_SUCCESS

Message Meaning: Wireless station sign on success

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43603 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_FAILURE

Message ID: 43603

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_FAILURE

Message Meaning: Wireless station sign on failed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43604 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_REQUEST

Message ID: 43604

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_REQUEST

Message Meaning: Captive-portal VAP e-mail collect request sent

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43605 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_SUCCESS

Message ID: 43605

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_SUCCESS

Message Meaning: Captive-portal VAP e-mail collect success

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43606 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_FAILURE

Message ID: 43606

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_FAILURE

Message Meaning: Captive-portal VAP e-mail collect failed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43607 - LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_CHECK

Message ID: 43607

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_CHECK

Message Meaning: Captive-portal VAP disclaimer agreed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43608 - LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_DECLINE

Message ID: 43608

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_DECLINE

Message Meaning: Captive-portal VAP disclaimer declined

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43609 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_START

Message ID: 43609

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_START

Message Meaning: DARRP optimization start

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43610 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_STOP

Message ID: 43610

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_STOP

Message Meaning: DARRP optimization stop

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43611 - LOG_ID_EVENT_WIRELESS_SYS_AC_UP

Message ID: 43611

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_UP

Message Meaning: Wireless controller start

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43612 - LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED

Message ID: 43612

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED

Message Meaning: Wireless controller configuration loaded

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43613 - LOG_ID_EVENT_WIRELESS_WTP_ERR

Message ID: 43613

Message Description: LOG_ID_EVENT_WIRELESS_WTP_ERR

Message Meaning: Physical AP error

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43614 - LOG_ID_EVENT_WIRELESS_DHCP_STAVATION

Message ID: 43614

Message Description: LOG_ID_EVENT_WIRELESS_DHCP_STAVATION

Message Meaning: DHCP Starvation detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
vapmode	Virtual Access Point mode	string	17
xid		uint32	10
client_addr	Client address	string	17
source_mac	The source MAC address of wifi station	string	17
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43615 - LOG_ID_EVENT_WIRELESS_SYS_AC_IPSEC_FAIL

Message ID: 43615

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_IPSEC_FAIL

Message Meaning: Wireless controller IPsec setup failed

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43616 - LOG_ID_EVENT_WIRELESS_WTPR_NOL_ADD

Message ID: 43616

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_NOL_ADD

Message Meaning: Physical AP radio NOL added

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4

Log Field Name	Description	Data Type	Length
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43618 - LOG_ID_EVENT_WIRELESS_WTP_IMAGE_RC_SUCCESS

Message ID: 43618

Message Description: LOG_ID_EVENT_WIRELESS_WTP_IMAGE_RC_SUCCESS

Message Meaning: Physical AP image receive success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43619 - LOG_ID_EVENT_WIRELESS_OFFENDINGAP_DETECT

Message ID: 43619

Message Description: LOG_ID_EVENT_WIRELESS_OFFENDINGAP_DETECT

Message Meaning: Offending AP detected

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43620 - LOG_ID_EVENT_WIRELESS_OFFENDINGAP_ONAIR

Message ID: 43620

Message Description: LOG_ID_EVENT_WIRELESS_OFFENDINGAP_ONAIR

Message Meaning: Offending AP on air

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
snclosest	SN of the AP closest to the rogue AP	string	36
stacount	The count of wifi stations	uint32	10
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
sndetected	SN of the AP which detected the rogue AP	string	36
apscan	The name of AP to detect rogue ap	string	36
stamac	The MAC address of wifi station	string	17
detectionmethod	Detection Method	string	21
onwire	The rogue ap is onwire or not	string	3
age	Time in seconds - time passed since last seen	uint32	10
live	Time in seconds	uint32	10
noise	WiFi signal noise level	int8	4
signal	The signal value of SSID or client	int8	4

Log Field Name	Description	Data Type	Length
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
manuf	Manufacturer name	string	20
channel	Channel	uint8	3
radioband	The operating radio band	string	64
rate	WiFi band width rate	uint16	6
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43621 - LOG_ID_EVENT_WIRELESS_WTP_DATA_CHAN_CHG

Message ID: 43621

Message Description: LOG_ID_EVENT_WIRELESS_WTP_DATA_CHAN_CHG

Message Meaning: Wireless wtp data channel changed

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43622 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_PROBE

Message ID: 43622

Message Description: LOG_ID_EVENT_WIRELESS_WTP_VLAN_PROBE

Message Meaning: WTP is probing vlan

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43623 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_MISSING

Message ID: 43623

Message Description: LOG_ID_EVENT_WIRELESS_WTP_VLAN_MISSING

Message Meaning: VLAN not detected

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36

Log Field Name	Description	Data Type	Length
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43624 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_DETECTED

Message ID: 43624

Message Description: LOG_ID_EVENT_WIRELESS_WTP_VLAN_DETECTED

Message Meaning: VLAN detected

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36

Log Field Name	Description	Data Type	Length
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43625 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_SUCCESS

Message ID: 43625

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_SUCCESS

Message Meaning: Wireless station CMCC sign on success

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43626 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_FAILURE

Message ID: 43626

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_FAILURE

Message Meaning: Wireless station CMCC sign on failed

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43627 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_TIMEOUT

Message ID: 43627

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_TIMEOUT

Message Meaning: Wireless station CMCC sign on timeout

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43628 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_MAC_AUTH_SUCCESS

Message ID: 43628

Message Description: LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_MAC_AUTH_SUCCESS

Message Meaning: Wireless station CMCC MAC auth success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43629 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_FAILURE

Message ID: 43629

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_FAILURE

Message Meaning: Wireless client RADIUS authentication failure

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43630 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_SUCCESS

Message ID: 43630

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_SUCCESS

Message Meaning: Wireless client RADIUS authentication success

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43631 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_NO_RESP

Message ID: 43631

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_NO_RESP

Message Meaning: Wireless client RADIUS authentication server not responding

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43632 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_FAILURE

Message ID: 43632

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_FAILURE

Message Meaning: Wireless client RADIUS MAC authentication failure

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43633 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_SUCCESS

Message ID: 43633

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_SUCCESS

Message Meaning: Wireless client RADIUS MAC authentication success

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43634 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_NO_RESP

Message ID: 43634

Message Description: LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_NO_RESP

Message Meaning: Wireless client RADIUS MAC authentication server not responding

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43635 - LOG_ID_EVENT_WIRELESS_STA_OKC_NO_MATCH

Message ID: 43635

Message Description: LOG_ID_EVENT_WIRELESS_STA_OKC_NO_MATCH

Message Meaning: Wireless client authenticates through OKC failed with no match

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43636 - LOG_ID_EVENT_WIRELESS_STA_OKC_LOCAL_MATCH

Message ID: 43636

Message Description: LOG_ID_EVENT_WIRELESS_STA_OKC_LOCAL_MATCH

Message Meaning: Wireless client authenticates through local OKC success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43637 - LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AC_MATCH

Message ID: 43637

Message Description: LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AC_MATCH

Message Meaning: Wireless client authenticates through inter AC OKC success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43638 - LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AP_MATCH

Message ID: 43638

Message Description: LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AP_MATCH

Message Meaning: Wireless client authenticates through inter AP OKC success

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43639 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_ACTION_REQ

Message ID: 43639

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_ACTION_REQ

Message Meaning: Wireless client sent invalid FT action request

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43640 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_AUTH_REQ

Message ID: 43640

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_AUTH_REQ

Message Meaning: Wireless client sent invalid FT auth request

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43641 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_REASSOC_REQ

Message ID: 43641

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_REASSOC_REQ

Message Meaning: Wireless client sent invalid FT reassociation request

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43642 - LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_REQ

Message ID: 43642

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_REQ

Message Meaning: Wireless client sent FT action reqeust

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40

Log Field Name	Description	Data Type	Length
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43643 - LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_RESP

Message ID: 43643

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_RESP

Message Meaning: FT action response was sent to wireless client

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43644 - LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_REQ

Message ID: 43644

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_REQ

Message Meaning: Wireless client sent FT auth request

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43645 - LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_RESP

Message ID: 43645

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_RESP

Message Meaning: FT auth response was sent to wireless client

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43646 - LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_REQ

Message ID: 43646

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_REQ

Message Meaning: Wireless client sent FT reassociation request

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40

Log Field Name	Description	Data Type	Length
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43647 - LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_RESP

Message ID: 43647

Message Description: LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_RESP

Message Meaning: FT reassociation response was sent to wireless client

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43648 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SECOND_MSG

Message ID: 43648

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SECOND_MSG

Message Meaning: Wireless client 4 way handshake failed with invalid 2/4 message

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43649 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_FOURTH_MSG

Message ID: 43649

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_FOURTH_MSG

Message Meaning: Wireless client 4 way handshake failed with invalid 4/4 message

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43650 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_MSG

Message ID: 43650

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_MSG

Message Meaning: AP sent 1/4 message of 4 way handshake to wireless client

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43651 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_MSG

Message ID: 43651

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_MSG

Message Meaning: Wireless client sent 2/4 message of 4 way handshake

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43652 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_THIRD_MSG

Message ID: 43652

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_THIRD_MSG

Message Meaning: AP sent 3/4 message of 4 way handshake to wireless client

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43653 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FOURTH_MSG

Message ID: 43653

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FOURTH_MSG

Message Meaning: Wireless client sent 4/4 message of 4 way handshake

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43654 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_GROUP_MSG

Message ID: 43654

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_GROUP_MSG

Message Meaning: AP sent 1/2 message of group key handshake to wireless client

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43655 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_GROUP_MSG

Message ID: 43655

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_GROUP_MSG

Message Meaning: Wireless client sent 2/2 message of group key handshake

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43656 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_MAX_STA_CNT

Message ID: 43656

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_MAX_STA_CNT

Message Meaning: Max sta count limit for the PSK was reached

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43657 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_FAIL

Message ID: 43657

Message Description: LOG_ID_EVENT_WIRELESS_STA_ASSOC_FAIL

Message Meaning: Wireless station association failed

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43658 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_RESP

Message ID: 43658

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_RESP

Message Meaning: Wireless station DHCP process failed with no server response

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43659 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DIFF_OFFER

Message ID: 43659

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_DIFF_OFFER

Message Meaning: Another DHCP server sent DHCP offer to wireless station

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43660 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_ACK

Message ID: 43660

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_ACK

Message Meaning: No DHCP ACK from server

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17

Log Field Name	Description	Data Type	Length
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43661 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NAK

Message ID: 43661

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_NAK

Message Meaning: DHCP server sent DHCP NAK

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43662 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DUP_IP

Message ID: 43662

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_DUP_IP

Message Meaning: IP offered has been used by another wireless station

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32

Log Field Name	Description	Data Type	Length
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43663 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DISCOVER

Message ID: 43663

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_DISCOVER

Message Meaning: Wireless station sent DHCP DISCOVER

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43664 - LOG_ID_EVENT_WIRELESS_STA_DHCP_OFFER

Message ID: 43664

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_OFFER

Message Meaning: DHCP server sent DHCP OFFER

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43665 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DECLINE

Message ID: 43665

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_DECLINE

Message Meaning: Wireless station sent DHCP DECLINE

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43666 - LOG_ID_EVENT_WIRELESS_STA_DHCP_REQUEST

Message ID: 43666

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_REQUEST

Message Meaning: Wireless station sent DHCP REQUEST

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43667 - LOG_ID_EVENT_WIRELESS_STA_DHCP_ACK

Message ID: 43667

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_ACK

Message Meaning: DHCP server sent DHCP ACK

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43668 - LOG_ID_EVENT_WIRELESS_STA_DHCP_RELEASE

Message ID: 43668

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_RELEASE

Message Meaning: Wireless station sent DHCP RELEASE

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43669 - LOG_ID_EVENT_WIRELESS_STA_DHCP_INFORM

Message ID: 43669

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_INFORM

Message Meaning: Wireless station sent DHCP INFORM

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43670 - LOG_ID_EVENT_WIRELESS_STA_DHCP_SELF_ASSIGNED

Message ID: 43670

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_SELF_ASSIGNED

Message Meaning: Wireless station is using self-assigned IP

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43671 - LOG_ID_EVENT_WIRELESS_STA_DNS_NO_RESP

Message ID: 43671

Message Description: LOG_ID_EVENT_WIRELESS_STA_DNS_NO_RESP

Message Meaning: Wireless station DNS process failed with no server response

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43672 - LOG_ID_EVENT_WIRELESS_STA_DNS_SERVER_FAILURE

Message ID: 43672

Message Description: LOG_ID_EVENT_WIRELESS_STA_DNS_SERVER_FAILURE

Message Meaning: Wireless station DNS process failed due to server failure

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43673 - LOG_ID_EVENT_WIRELESS_STA_DNS_NO_DOMAIN

Message ID: 43673

Message Description: LOG_ID_EVENT_WIRELESS_STA_DNS_NO_DOMAIN

Message Meaning: Wireless station DNS process failed due to non-existing domain

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43674 - LOG_ID_EVENT_WIRELESS_STA_WPA_KRACK_FT_REASSOC

Message ID: 43674

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_KRACK_FT_REASSOC

Message Meaning: Wireless station WPA key reinstallation attack on FT reassociation

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43675 - LOG_ID_EVENT_WIRELESS_STA_AUTH_REQ

Message ID: 43675

Message Description: LOG_ID_EVENT_WIRELESS_STA_AUTH_REQ

Message Meaning: Authentication request from wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36

Log Field Name	Description	Data Type	Length
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43676 - LOG_ID_EVENT_WIRELESS_STA_AUTH_RESP

Message ID: 43676

Message Description: LOG_ID_EVENT_WIRELESS_STA_AUTH_RESP

Message Meaning: Authentication response to wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43677 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_REQ

Message ID: 43677

Message Description: LOG_ID_EVENT_WIRELESS_STA_ASSOC_REQ

Message Meaning: Association request from wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43678 - LOG_ID_EVENT_WIRELESS_STA_REASSOC_REQ

Message ID: 43678

Message Description: LOG_ID_EVENT_WIRELESS_STA_REASSOC_REQ

Message Meaning: Reassociation request from wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17

Log Field Name	Description	Data Type	Length
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43679 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_RESP

Message ID: 43679

Message Description: LOG_ID_EVENT_WIRELESS_STA_ASSOC_RESP

Message Meaning: Association response to wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43680 - LOG_ID_EVENT_WIRELESS_STA_REASSOC_RESP

Message ID: 43680

Message Description: LOG_ID_EVENT_WIRELESS_STA_REASSOC_RESP

Message Meaning: Reassociation response to wireless station

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43681 - LOG_ID_EVENT_WIRELESS_STA_PROBE_REQ

Message ID: 43681

Message Description: LOG_ID_EVENT_WIRELESS_STA_PROBE_REQ

Message Meaning: Probe request from wireless station

Type: Event

Category: wireless

Severity: Information

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43682 - LOG_ID_EVENT_WIRELESS_STA_PROBE_RESP

Message ID: 43682

Message Description: LOG_ID_EVENT_WIRELESS_STA_PROBE_RESP

Message Meaning: Probe response to wireless station

Type: Event

Category: wireless

Severity: Information

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43683 - LOG_ID_EVENT_WIRELESS_BLE_DEV_LOCATE

Message ID: 43683

Message Description: LOG_ID_EVENT_WIRELESS_BLE_DEV_LOCATE

Message Meaning: Wireless ble dev detection

Type: Event

Category: wireless

Severity: Information

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43684 - LOG_ID_EVENT_WIRELESS_ADDRGRP_DUPLICATE_MAC

Message ID: 43684

Message Description: LOG_ID_EVENT_WIRELESS_ADDRGRP_DUPLICATE_MAC

Message Meaning: Wireless addrgrp duplicate mac

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
addrgrp		string	36
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43685 - LOG_ID_EVENT_WIRELESS_ADDRGRP_ADDR_APPLY

Message ID: 43685

Message Description: LOG_ID_EVENT_WIRELESS_ADDRGRP_ADDR_APPLY

Message Meaning: Wireless addrgrp address apply

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
addrgrp		string	36
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43686 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SCHEDULE

Message ID: 43686

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SCHEDULE

Message Meaning: PSK is out of any valid schedules

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43687 - LOG_ID_EVENT_WIRELESS_STA_WL_BRIDGE_TRAFFIC_STATS

Message ID: 43687

Message Description: LOG_ID_EVENT_WIRELESS_STA_WL_BRIDGE_TRAFFIC_STATS

Message Meaning: Traffic stats for station with bridge wlan

Type: Event

Category: wireless

Severity: Information

Log Field Name	Description	Data Type	Length
nextstat	Time interval in seconds for the next statistics	uint32	10
rcvdbyte	Received Bytes	uint64	20
sentbyte	Bytes Sent	uint64	20
snr		int8	4
srcip	Source IP	ip	39
user	User name of authenticated user	string	256
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43688 - LOG_ID_EVENT_WIRELESS_APCFG_RECEIVE

Message ID: 43688

Message Description: LOG_ID_EVENT_WIRELESS_APCFG_RECEIVE

Message Meaning: FortiAP receives the apcfg

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43689 - LOG_ID_EVENT_WIRELESS_APCFG_VALIDATING

Message ID: 43689

Message Description: LOG_ID_EVENT_WIRELESS_APCFG_VALIDATING

Message Meaning: FortiAP is validating the apcfg

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

43690 - LOG_ID_EVENT_WIRELESS_APCFG_APPLY

Message ID: 43690

Message Description: LOG_ID_EVENT_WIRELESS_APCFG_APPLY

Message Meaning: FortiAP applies the apcfg

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43691 - LOG_ID_EVENT_WIRELESS_APCFG_REJECT

Message ID: 43691

Message Description: LOG_ID_EVENT_WIRELESS_APCFG_REJECT

Message Meaning: FortiAP rejects the apcfg

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43692 - LOG_ID_EVENT_WIRELESS_WTPR_ANTENNA_DEFECT_DETECT

Message ID: 43692

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_ANTENNA_DEFECT_DETECT

Message Meaning: Defect antenna detection

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43693 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_REQ

Message ID: 43693

Message Description: LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_REQ

Message Meaning: AP sent WNM action BSTM request

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43694 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_ACCEPT

Message ID: 43694

Message Description: LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_ACCEPT

Message Meaning: Wireless client sent WNM action BSTM response accept

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43695 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_REJECT

Message ID: 43695

Message Description: LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_REJECT

Message Meaning: Wireless client sent WNM action BSTM response reject

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43696 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_START

Message ID: 43696

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DRMA_START

Message Meaning: Physical AP radio DRMA start

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43697 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_STOP

Message ID: 43697

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DRMA_STOP

Message Meaning: Physical AP radio DRMA stop

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43698 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_MODE

Message ID: 43698

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_DRMA_MODE

Message Meaning: Physical AP radio DRMA mode

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43699 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_SOLICIT

Message ID: 43699

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_SOLICIT

Message Meaning: Wireless station sent DHCP6 SOLICIT

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43700 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_ADVERTISE

Message ID: 43700

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_ADVERTISE

Message Meaning: DHCP6 server sent DHCP6 ADVERTISE

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43701 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_REQUEST

Message ID: 43701

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_REQUEST

Message Meaning: Wireless station sent DHCP6 REQUEST

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43702 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_CONFIRM

Message ID: 43702

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_CONFIRM

Message Meaning: Wireless station sent DHCP6 CONFIRM

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43703 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RENEW

Message ID: 43703

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_RENEW

Message Meaning: Wireless station sent DHCP6 RENEW

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32

Log Field Name	Description	Data Type	Length
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43704 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_REPLY

Message ID: 43704

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_REPLY

Message Meaning: DHCP6 server sent DHCP6 REPLY

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43705 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RELEASE

Message ID: 43705

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_RELEASE

Message Meaning: Wireless station sent DHCP6 RELEASE

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43706 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RECONFIGURE

Message ID: 43706

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP6_RECONFIGURE

Message Meaning: DHCP6 server sent DHCP6 RECONFIGURE

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mac	MAC Address	string	17
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43707 - LOG_ID_EVENT_WIRELESS_WTPR_SSID_UP

Message ID: 43707

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_SSID_UP

Message Meaning: Physical AP radio ssid up

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43708 - LOG_ID_EVENT_WIRELESS_WTPR_SSID_DOWN

Message ID: 43708

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_SSID_DOWN

Message Meaning: Physical AP radio ssid down

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43709 - LOG_ID_EVENT_WIRELESS_STA_DHCP_ENFORCEMENT

Message ID: 43709

Message Description: LOG_ID_EVENT_WIRELESS_STA_DHCP_ENFORCEMENT

Message Meaning: Wireless client denied by DHCP enforcement for using static IP address

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
server	AD server FQDN or IP	string	64
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43710 - LOG_ID_EVENT_WIRELESS_SAM_IPERF

Message ID: 43710

Message Description: LOG_ID_EVENT_WIRELESS_SAM_IPERF

Message Meaning: SAM iperf test result

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43711 - LOG_ID_EVENT_WIRELESS_SAM_PING

Message ID: 43711

Message Description: LOG_ID_EVENT_WIRELESS_SAM_PING

Message Meaning: SAM ping test result

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
bssid	Basic service set ID	string	17

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43712 - LOG_ID_EVENT_WIRELESS_SAM_AUTH_FAILED

Message ID: 43712

Message Description: LOG_ID_EVENT_WIRELESS_SAM_AUTH_FAILED

Message Meaning: AP as station failed in SAM authentication

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
security	Security	string	40
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43713 - LOG_ID_EVENT_WIRELESS_SAM_CWP_AUTH_FAILED

Message ID: 43713

Message Description: LOG_ID_EVENT_WIRELESS_SAM_CWP_AUTH_FAILED

Message Meaning: AP as station failed in SAM CWP authentication

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
bssid	Basic service set ID	string	17
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43714 - LOG_ID_EVENT_WIRELESS_WTP_PARTIAL_PASSWD

Message ID: 43714

Message Description: LOG_ID_EVENT_WIRELESS_WTP_PARTIAL_PASSWD

Message Meaning: AP received partial login password

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
snmeshparent	SN of the mesh parent	string	36
meshmode	Mesh mode	string	19
ip		ip	39
profile	Profile Name	string	64
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43715 - LOG_ID_EVENT_WIRELESS_WTPR_BSS_COLOR_COLLISION

Message ID: 43715

Message Description: LOG_ID_EVENT_WIRELESS_WTPR_BSS_COLOR_COLLISION

Message Meaning: AP radio BSS color collision detected.

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
operdrmamode		string	10
slctdrmamode		string	10
opertxpower	The value of operating tx power	uint32	10
cfgtxpower	Config TX power	uint32	10
opercountry	The name of operating country on a AP	string	4
configcountry	Config Country	string	4
bandwidth	Bandwidth	string	42
radioid	The operating radio ID	uint8	3
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43716 - LOG_ID_EVENT_WIRELESS_ADDRGRP_MAX_FW_ADDR

Message ID: 43716

Message Description: LOG_ID_EVENT_WIRELESS_ADDRGRP_MAX_FW_ADDR

Message Meaning: Wireless addrgrp reached firewal address maximum number

Type: Event

Category: wireless

Severity: Warning

Log Field Name	Description	Data Type	Length
addrgrp		string	36
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43717 - LOG_ID_EVENT_WIRELESS_STA_L3R_REHOME

Message ID: 43717

Message Description: LOG_ID_EVENT_WIRELESS_STA_L3R_REHOME

Message Meaning: Wireless client layer3 roaming rehome

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
mpsk	Multiple pre-shared keys	string	33
snr		int8	4

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64
group	User group Name	string	512
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
radioband	The operating radio band	string	64
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43719 - LOG_ID_EVENT_WIRELESS_STA_PROBE_LOW_RSSI

Message ID: 43719

Message Description: LOG_ID_EVENT_WIRELESS_STA_PROBE_LOW_RSSI

Message Meaning: Probe request from wireless station failed due to low rssi

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43720 - LOG_ID_EVENT_WIRELESS_FIPS

Message ID: 43720

Message Description: LOG_ID_EVENT_WIRELESS_FIPS

Message Meaning: Physical AP FIPS activity

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
ip		ip	39
ap	Access Point	string	36
sn	Serial Number	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43721 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_EXT_MPSK_RESULT

Message ID: 43721

Message Description: LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_EXT_MPSK_RESULT

Message Meaning: External MPSK authentication result

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
remotewtptime	The time of AP when client trying to connect	string	32
snprev		string	36
snr		int8	4
authserver	Remote Authentication server	string	64
user	User name of authenticated user	string	256
radioid	The operating radio ID	uint8	3
vap	Virtual Access Point	string	36
reason	Reason	string	256
ap	Access Point	string	36
sn	Serial Number	string	64
stamac	The MAC address of wifi station	string	17
signal	The signal value of SSID or client	int8	4
encryption	The encryption type of detected rogue AP	string	12
security	Security	string	40
channel	Channel	uint8	3
ssid	WiFi Service Set ID	string	33
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43723 - LOG_ID_EVENT_WIRELESS_SYS_AC_DOWN

Message ID: 43723

Message Description: LOG_ID_EVENT_WIRELESS_SYS_AC_DOWN

Message Meaning: Wireless controller down

Type: Event

Category: wireless

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43776 - LOG_ID_EVENT_NAC_QUARANTINE

Message ID: 43776

Message Description: LOG_ID_EVENT_NAC_QUARANTINE

Message Meaning: NAC quarantine

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
admin	Administrator	string	64
banned_rule	NAC quarantine Banned Rule Name	string	80
banned_src	NAC quarantine Banned Source IP	string	16
policyid	Policy ID	uint32	10
group	User group Name	string	512
dst_int	Destination Interface	string	64
src_int	Source Interface	string	64
profile	Profile Name	string	64
duration	Duration	uint32	10
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
proto	Protocol Number	uint8	3
service	Name of Service	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43777 - LOG_ID_EVENT_NAC_ANOMALY_QUARANTINE

Message ID: 43777

Message Description: LOG_ID_EVENT_NAC_ANOMALY_QUARANTINE

Message Meaning: NAC anomaly quarantine

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
admin	Administrator	string	64
banned_rule	NAC quarantine Banned Rule Name	string	80
banned_src	NAC quarantine Banned Source IP	string	16
policyid	Policy ID	uint32	10
group	User group Name	string	512
dst_int	Destination Interface	string	64
src_int	Source Interface	string	64
profile	Profile Name	string	64
duration	Duration	uint32	10
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
proto	Protocol Number	uint8	3
service	Name of Service	string	64
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43778 - LOG_ID_EVENT_NAC_QUARANTINE_EXPIRY

Message ID: 43778

Message Description: LOG_ID_EVENT_NAC_QUARANTINE_EXPIRY

Message Meaning: NAC quarantine expiry

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
duration	Duration	uint32	10
srcip	Source IP	ip	39
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43800 - LOG_ID_EVENT_ELBC_BLADE_JOIN

Message ID: 43800

Message Description: LOG_ID_EVENT_ELBC_BLADE_JOIN

Message Meaning: Blade ready to process traffic

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43801 - LOG_ID_EVENT_ELBC_BLADE_LEAVE

Message ID: 43801

Message Description: LOG_ID_EVENT_ELBC_BLADE_LEAVE

Message Meaning: Blade not ready to process traffic

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43802 - LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND

Message ID: 43802

Message Description: LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND

Message Meaning: Primary blade found

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43803 - LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST

Message ID: 43803

Message Description: LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST

Message Meaning: Primary blade lost

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43804 - LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE

Message ID: 43804

Message Description: LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE

Message Meaning: Primary blade changed

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
newchassisid	New Chassis ID	uint8	3
newslot	New Slot Number	uint8	3
oldchassisid	Original Chassis Number	uint8	3
oldslot	Original Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43805 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND

Message ID: 43805

Message Description: LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND

Message Meaning: ELBC channel active

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
newchannel	New Channel Number	uint8	3
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43806 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST

Message ID: 43806

Message Description: LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST

Message Meaning: ELBC channel inactive

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
oldchannel	Original Channel Number	uint8	3
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43807 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE

Message ID: 43807

Message Description: LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE

Message Meaning: ELBC channel failover

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
oldchannel	Original Channel Number	uint8	3
newchannel	New Channel Number	uint8	3
chassisid	Chassis ID	uint8	3
slot	Slot Number	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43808 - LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE

Message ID: 43808

Message Description: LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE

Message Meaning: ELBC chassis active

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

43809 - LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE

Message ID: 43809

Message Description: LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE

Message Meaning: ELBC chassis inactive

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
chassisid	Chassis ID	uint8	3
informationsource	Information Source	string	4096
msg	Log Message	string	4096
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44544 - LOGID_EVENT_CONFIG_PATH

Message ID: 44544

Message Description: LOGID_EVENT_CONFIG_PATH

Message Meaning: Path configured

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
cfgpath	Configuration path	string	128
cfgtid	Config transaction id	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44545 - LOGID_EVENT_CONFIG_OBJ

Message ID: 44545

Message Description: LOGID_EVENT_CONFIG_OBJ

Message Meaning: Object configured

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
cfgobj	Configuration object	string	256
cfgpath	Configuration path	string	128
cfgtid	Config transaction id	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

44546 - LOGID_EVENT_CONFIG_ATTR

Message ID: 44546

Message Description: LOGID_EVENT_CONFIG_ATTR

Message Meaning: Attribute configured

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
cfgattr	Configuration attribute	string	4096
cfgpath	Configuration path	string	128
cfgtid	Config transaction id	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44547 - LOGID_EVENT_CONFIG_OBJATTR

Message ID: 44547

Message Description: LOGID_EVENT_CONFIG_OBJATTR

Message Meaning: Object attribute configured

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
cfgattr	Configuration attribute	string	4096
cfgobj	Configuration object	string	256
cfgpath	Configuration path	string	128
cfgtid	Config transaction id	uint32	10
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44548 - LOGID_EVENT_CONFIG_EXEC

Message ID: 44548

Message Description: LOGID_EVENT_CONFIG_EXEC

Message Meaning: Action performed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44555 - LOGID_EVENT_CMDB_DEADLOCK_DETECTED

Message ID: 44555

Message Description: LOGID_EVENT_CMDB_DEADLOCK_DETECTED

Message Meaning: CMDB lock deadlock is detected.

Type: Event

Category: system

Severity: Critical

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

44559 - LOGID_EVENT_INSTALL_IPROPE

Message ID: 44559

Message Description: LOGID_EVENT_INSTALL_IPROPE

Message Meaning: Firewall policy installation

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45071 - LOG_ID_FCC_VULN_SCAN

Message ID: 45071

Message Description: LOG_ID_FCC_VULN_SCAN

Message Meaning: FortiClient Vulnerability Scan

Type: Event

Category: endpoint

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
vendorurl		string	256
cveid	CVE ID	string	720
severity	Severity	string	10
vulncat	Vulnerability Category	string	32
vulnname	Vulnerability name	string	128
vulnid	Vulnerability ID	uint32	10
devtype	Device type	string	32
srcmac	Source MAC address	string	17
srcname	Source name	string	64
srcip	Source IP	ip	39
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
scantime		uint64	20
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

45101 - LOG_ID_EC_REG_SUCCEED

Message ID: 45101

Message Description: LOG_ID_EC_REG_SUCCEED

Message Meaning: FortiClient registered

Type: Event

Category: endpoint

Severity: Notice

Log Field Name	Description	Data Type	Length
duration	Duration of the last threatening packed captured from TA	uint32	10
srcport	Source port	uint16	5
msg	Log Message	string	4096
srcip	Source IP	ip	39
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45114 - LOG_ID_EC_REG_QUARANTINE

Message ID: 45114

Message Description: LOG_ID_EC_REG_QUARANTINE

Message Meaning: FortiClient endpoint quarantined

Type: Event

Category: endpoint

Severity: Notice

Log Field Name	Description	Data Type	Length
ip	Source IP	ip	39
hostname	Hostname	string	128
fctemssn		string	16
msg	Log Message	string	4096
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45115 - LOG_ID_EC_REG_UNQUARANTINE

Message ID: 45115

Message Description: LOG_ID_EC_REG_UNQUARANTINE

Message Meaning: FortiClient endpoint quarantine removed

Type: Event

Category: endpoint

Severity: Notice

Log Field Name	Description	Data Type	Length
ip	Source IP	ip	39
hostname	Hostname	string	128
fctemssn		string	16
msg	Log Message	string	4096
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45121 - LOG_ID_EC_EMS_WS_NOTIFICATION

Message ID: 45121

Message Description: LOG_ID_EC_EMS_WS_NOTIFICATION

Message Meaning: EMS WebSocket notification

Type: Event

Category: endpoint

Severity: Notice

Log Field Name	Description	Data Type	Length
fctemsname		string	36
fctemssn		string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45122 - LOG_ID_EC_EMS_REST_API_ERROR

Message ID: 45122

Message Description: LOG_ID_EC_EMS_REST_API_ERROR

Message Meaning: EMS REST API error

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
httpcode		uint16	3
url	URL	string	512
fctemsname		string	36
fctemssn		string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45123 - LOG_ID_EC_EMS_WS_CONN_ERROR

Message ID: 45123

Message Description: LOG_ID_EC_EMS_WS_CONN_ERROR

Message Meaning: EMS WebSocket connection error

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
wscode		uint16	4
url	URL	string	512
fctemsname		string	36
fctemssn		string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45124 - LOG_ID_EC_VPND_CONNECT

Message ID: 45124

Message Description: LOG_ID_EC_VPND_CONNECT

Message Meaning: FortiClient VPN connected

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
intf	Interface	string	16
sn	Serial Number	string	64
ip	Source IP	ip	39
msg	Log Message	string	4096
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45125 - LOG_ID_EC_VPND_DISCONNECT

Message ID: 45125

Message Description: LOG_ID_EC_VPND_DISCONNECT

Message Meaning: FortiClient VPN disconnected

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
intf	Interface	string	16
sn	Serial Number	string	64
ip	Source IP	ip	39
msg	Log Message	string	4096
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45126 - LOG_ID_EC_CLOUD_ENTITLEMENT_LOST

Message ID: 45126

Message Description: LOG_ID_EC_CLOUD_ENTITLEMENT_LOST

Message Meaning: EMS Cloud entitlement lost and connection dropped

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45128 - LOG_ID_EC_EMS_REST_API_NEW_SUCCESS

Message ID: 45128

Message Description: LOG_ID_EC_EMS_REST_API_NEW_SUCCESS

Message Meaning: EMS REST API recovered from an error

Type: Event

Category: endpoint

Severity: Information

Log Field Name	Description	Data Type	Length
httpcode		uint16	3
url	URL	string	512
fctemsname		string	36
fctemssn		string	16
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45129 - LOG_ID_EC_EMS_EMS_VERIFY

Message ID: 45129

Message Description: LOG_ID_EC_EMS_EMS_VERIFY

Message Meaning: FCEMS entry has been verified

Type: Event

Category: endpoint

Severity: Information

Log Field Name	Description	Data Type	Length
fctemsname		string	36
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45130 - LOG_ID_EC_EMS_EMS_VERIFY_FAILED

Message ID: 45130

Message Description: LOG_ID_EC_EMS_EMS_VERIFY_FAILED

Message Meaning: FCEMS entry has failed to be verified

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
fctemsname		string	36
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45131 - LOG_ID_EC_EMS_EMS_UNVERIFY

Message ID: 45131

Message Description: LOG_ID_EC_EMS_EMS_UNVERIFY

Message Meaning: FCEMS entry has been unverified

Type: Event

Category: endpoint

Severity: Information

Log Field Name	Description	Data Type	Length
fctemsname		string	36
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45132 - LOG_ID_EC_EMS_UPGRADE_FAIL

Message ID: 45132

Message Description: LOG_ID_EC_EMS_UPGRADE_FAIL

Message Meaning: EMS entry could not be upgraded

Type: Event

Category: endpoint

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

45133 - LOG_ID_EC_SHM_MISSING_QUERY

Message ID: 45133

Message Description: LOG_ID_EC_SHM_MISSING_QUERY

Message Meaning: FCEMS shared memory missing query statistics

Type: Event

Category: endpoint

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46000 - LOG_ID_VIP_REAL_SVR_ENA

Message ID: 46000

Message Description: LOG_ID_VIP_REAL_SVR_ENA

Message Meaning: VIP real server enabled

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80

Log Field Name	Description	Data Type	Length
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46001 - LOG_ID_VIP_REAL_SVR_DISA

Message ID: 46001

Message Description: LOG_ID_VIP_REAL_SVR_DISA

Message Meaning: VIP real server disabled

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46002 - LOG_ID_VIP_REAL_SVR_UP

Message ID: 46002

Message Description: LOG_ID_VIP_REAL_SVR_UP

Message Meaning: VIP real server up

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46003 - LOG_ID_VIP_REAL_SVR_DOWN

Message ID: 46003

Message Description: LOG_ID_VIP_REAL_SVR_DOWN

Message Meaning: VIP real server down

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46004 - LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN

Message ID: 46004

Message Description: LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN

Message Meaning: VIP real server entered hold-down

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46005 - LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN

Message ID: 46005

Message Description: LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN

Message Meaning: VIP real server health check failed during hold-down

Type: Event

Category: system

Severity: Alert

Log Field Name	Description	Data Type	Length
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46006 - LOG_ID_VIP_REAL_SVR_FAIL

Message ID: 46006

Message Description: LOG_ID_VIP_REAL_SVR_FAIL

Message Meaning: VIP real server health check failed

Type: Event

Category: system

Severity: Debug

Log Field Name	Description	Data Type	Length
monitor-type	Health Monitor Name	string	32
monitor-name	Health Monitor Type	string	35
vip	Virtual IP	string	80
port	Port Number	uint16	5
server	Server IP Address	string	64
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46400 - LOG_ID_EVENT_EXT_SYS

Message ID: 46400

Message Description: LOG_ID_EVENT_EXT_SYS

Message Meaning: FortiExtender system activity

Type: Event

Category: fortiextender

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46401 - LOG_ID_EVENT_EXT_LOCAL

Message ID: 46401

Message Description: LOG_ID_EVENT_EXT_LOCAL

Message Meaning: FortiExtender controller activity

Type: Event

Category: fortiextender

Severity: Notice

Log Field Name	Description	Data Type	Length
action		string	65
ip		ip	39
sn	Serial Number	string	64
version		string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46402 - LOG_ID_EVENT_EXT_LOCAL_ERROR

Message ID: 46402

Message Description: LOG_ID_EVENT_EXT_LOCAL_ERROR

Message Meaning: FortiExtender controller activity error

Type: Event

Category: fortiextender

Severity: Error

Log Field Name	Description	Data Type	Length
action		string	65
ip		ip	39
sn	Serial Number	string	64
version		string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

46403 - LOG_ID_EVENT_EXT_REMOTE_EMERG

Message ID: 46403

Message Description: LOG_ID_EVENT_EXT_REMOTE_EMERG

Message Meaning: Remote FortiExtender emergency activity

Type: Event

Category: fortiextender

Severity: Emergency

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46404 - LOG_ID_EVENT_EXT_REMOTE_ALERT

Message ID: 46404

Message Description: LOG_ID_EVENT_EXT_REMOTE_ALERT

Message Meaning: Remote FortiExtender alert activity

Type: Event

Category: fortiextender

Severity: Alert

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46405 - LOG_ID_EVENT_EXT_REMOTE_CRITICAL

Message ID: 46405

Message Description: LOG_ID_EVENT_EXT_REMOTE_CRITICAL

Message Meaning: Remote FortiExtender critical activity

Type: Event

Category: fortiextender

Severity: Critical

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46406 - LOG_ID_EVENT_EXT_REMOTE_ERROR

Message ID: 46406

Message Description: LOG_ID_EVENT_EXT_REMOTE_ERROR

Message Meaning: Remote FortiExtender error activity

Type: Event

Category: fortiextender

Severity: Error

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46407 - LOG_ID_EVENT_EXT_REMOTE_WARNING

Message ID: 46407

Message Description: LOG_ID_EVENT_EXT_REMOTE_WARNING

Message Meaning: Remote FortiExtender warning activity

Type: Event

Category: fortiextender

Severity: Warning

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46408 - LOG_ID_EVENT_EXT_REMOTE_NOTIF

Message ID: 46408

Message Description: LOG_ID_EVENT_EXT_REMOTE_NOTIF

Message Meaning: Remote FortiExtender notify activity

Type: Event

Category: fortiextender

Severity: Notice

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46409 - LOG_ID_EVENT_EXT_REMOTE_INFO

Message ID: 46409

Message Description: LOG_ID_EVENT_EXT_REMOTE_INFO

Message Meaning: Remote FortiExtender info activity

Type: Event

Category: fortiextender

Severity: Information

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46410 - LOG_ID_EVENT_EXT_REMOTE_DEBUG

Message ID: 46410

Message Description: LOG_ID_EVENT_EXT_REMOTE_DEBUG

Message Meaning: Remote FortiExtender debug activity

Type: Event

Category: fortiextender

Severity: Debug

Log Field Name	Description	Data Type	Length
ip		ip	39
sn	Serial Number	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46501 - LOG_ID_INTERNAL_LTE_MODEM_DETECTION

Message ID: 46501

Message Description: LOG_ID_INTERNAL_LTE_MODEM_DETECTION

Message Meaning: LTE modem detection

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46502 - LOG_ID_INTERNAL_LTE_MODEM_GPSD

Message ID: 46502

Message Description: LOG_ID_INTERNAL_LTE_MODEM_GPSD

Message Meaning: LTE modem GPS daemon started or stopped

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46503 - LOG_ID_INTERNAL_LTE_MODEM_GPS_LOC_ACQUISITION

Message ID: 46503

Message Description: LOG_ID_INTERNAL_LTE_MODEM_GPS_LOC_ACQUISITION

Message Meaning: LTE modem GPS location acquisition

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46504 - LOG_ID_INTERNAL_LTE_MODEM_BILLD

Message ID: 46504

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLD

Message Meaning: LTE modem billing daemon started or stopped

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46505 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_PURGED

Message ID: 46505

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLING_PURGED

Message Meaning: LTE billing data purged

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46507 - LOG_ID_INTERNAL_LTE_MODEM_FW_UPGRADE

Message ID: 46507

Message Description: LOG_ID_INTERNAL_LTE_MODEM_FW_UPGRADE

Message Meaning: LTE modem firmware upgrade event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46508 - LOG_ID_INTERNAL_LTE_MODEM_QDL_DETECTION

Message ID: 46508

Message Description: LOG_ID_INTERNAL_LTE_MODEM_QDL_DETECTION

Message Meaning: LTE modem QDL device detection event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46509 - LOG_ID_INTERNAL_LTE_MODEM_REBOOT

Message ID: 46509

Message Description: LOG_ID_INTERNAL_LTE_MODEM_REBOOT

Message Meaning: LTE modem reboot event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46510 - LOG_ID_INTERNAL_LTE_MODEM_OP_MODE

Message ID: 46510

Message Description: LOG_ID_INTERNAL_LTE_MODEM_OP_MODE

Message Meaning: LTE modem operation mode

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46511 - LOG_ID_INTERNAL_LTE_MODEM_POWER_ON_OFF

Message ID: 46511

Message Description: LOG_ID_INTERNAL_LTE_MODEM_POWER_ON_OFF

Message Meaning: LTE modem powered on or powered off

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46512 - LOG_ID_INTERNAL_LTE_MODEM_SIM_STATE

Message ID: 46512

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_STATE

Message Meaning: LTE modem SIM card state event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46513 - LOG_ID_INTERNAL_LTE_MODEM_LINK_CONNECTION

Message ID: 46513

Message Description: LOG_ID_INTERNAL_LTE_MODEM_LINK_CONNECTION

Message Meaning: LTE modem data link connection event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46514 - LOG_ID_INTERNAL_LTE_MODEM_MANUAL_HANDOVER

Message ID: 46514

Message Description: LOG_ID_INTERNAL_LTE_MODEM_MANUAL_HANDOVER

Message Meaning: LTE modem manual handover event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46515 - LOG_ID_INTERNAL_LTE_MODEM_IP_ADDR

Message ID: 46515

Message Description: LOG_ID_INTERNAL_LTE_MODEM_IP_ADDR

Message Meaning: LTE modem ip address event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46516 - LOG_ID_INTERNAL_LTE_MODEM_BEARER_TECH_CHANGE

Message ID: 46516

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BEARER_TECH_CHANGE

Message Meaning: LTE modem bearer event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46517 - LOG_ID_INTERNAL_LTE_MODEM_WRONG_PIN

Message ID: 46517

Message Description: LOG_ID_INTERNAL_LTE_MODEM_WRONG_PIN

Message Meaning: LTE unlock SIM PIN failed.

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46518 - LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH

Message ID: 46518

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH

Message Meaning: LTE modem active SIM card switch event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46519 - LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_CONNECTION_STATE

Message ID: 46519

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_CONNECTION_STATE

Message Meaning: LTE modem active SIM card switched: modem disconnection detected

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46520 - LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_LINK_MONITOR

Message ID: 46520

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_LINK_MONITOR

Message Meaning: LTE modem active SIM card switched: link monitor probe failure detected

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46521 - LOG_ID_INTERNAL_LTE_MODEM_SIM_FLIP

Message ID: 46521

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_FLIP

Message Meaning: LTE modem active SIM card slot flipped back and forth in short time

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46522 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_ALERT

Message ID: 46522

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_ALERT

Message Meaning: LTE billing data usage reached configured threshold

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46523 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_TIME_REFRESH

Message ID: 46523

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLING_TIME_REFRESH

Message Meaning: LTE billing time passed, refresh billing date counter

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46524 - LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_DATA_PLAN

Message ID: 46524

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_DATA_PLAN

Message Meaning: LTE modem active SIM card switched: data plan reached

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46525 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_STOP_NETWORK

Message ID: 46525

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLING_STOP_NETWORK

Message Meaning: LTE modem stop network due to data plan reached

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46526 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_PLAN_OVER

Message ID: 46526

Message Description: LOG_ID_INTERNAL_LTE_MODEM_BILLING_DATA_PLAN_OVER

Message Meaning: LTE billing data usage reached data limit

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46527 - LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_SIM_STATE

Message ID: 46527

Message Description: LOG_ID_INTERNAL_LTE_MODEM_SIM_SWITCH_SIM_STATE

Message Meaning: LTE modem active SIM card switched: SIM state empty or error

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46600 - LOG_ID_EVENT_AUTOMATION_TRIGGERED

Message ID: 46600

Message Description: LOG_ID_EVENT_AUTOMATION_TRIGGERED

Message Meaning: Automation stitch triggered

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
from	Sender Email Address for Notification	string	128
stitchaction		string	256
trigger	Automation trigger name	string	36
stitch	Automation stitch name	string	36
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46703 - LOG_ID_INTERNAL_5G_MODEM_IPV4_LINK_STATE

Message ID: 46703

Message Description: LOG_ID_INTERNAL_5G_MODEM_IPV4_LINK_STATE

Message Meaning: 5G modem link state changed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
state	State	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46705 - LOG_ID_INTERNAL_5G_MODEM_FW_UPGRADE

Message ID: 46705

Message Description: LOG_ID_INTERNAL_5G_MODEM_FW_UPGRADE

Message Meaning: 5G modem firmware upgrade event

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46708 - LOG_ID_INTERNAL_5G_MODEM_MODE

Message ID: 46708

Message Description: LOG_ID_INTERNAL_5G_MODEM_MODE

Message Meaning: 5G modem changed operation mode

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
mode	Mode	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46709 - LOG_ID_INTERNAL_5G_MODEM_SIM_STATE

Message ID: 46709

Message Description: LOG_ID_INTERNAL_5G_MODEM_SIM_STATE

Message Meaning: 5G modem active sim card state changed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
state	State	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46710 - LOG_ID_INTERNAL_5G_MODEM_SIM_SWITCH

Message ID: 46710

Message Description: LOG_ID_INTERNAL_5G_MODEM_SIM_SWITCH

Message Meaning: 5G modem sim switched

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
simslot		string	4
modem		string	3
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46711 - LOG_ID_INTERNAL_5G_MODEM_AUTO_SIM_SWITCH_REASON

Message ID: 46711

Message Description: LOG_ID_INTERNAL_5G_MODEM_AUTO_SIM_SWITCH_REASON

Message Meaning: 5G modem auto sim switch triggered

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46713 - LOG_ID_INTERNAL_5G_MODEM_SIGNAL_MODE

Message ID: 46713

Message Description: LOG_ID_INTERNAL_5G_MODEM_SIGNAL_MODE

Message Meaning: 5G modem signal mode changed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
modem		string	3
mode	Mode	string	32
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

46900 - LOG_ID_POE_STATUS_REPORT

Message ID: 46900

Message Description: LOG_ID_POE_STATUS_REPORT

Message Meaning: PoE device status reported

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47000 - LOG_ID_MALWARE_LIST_TRUNCATED_ENTER

Message ID: 47000

Message Description: LOG_ID_MALWARE_LIST_TRUNCATED_ENTER

Message Meaning: External blocklist list is truncated

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47001 - LOG_ID_MALWARE_LIST_TRUNCATED_EXIT

Message ID: 47001

Message Description: LOG_ID_MALWARE_LIST_TRUNCATED_EXIT

Message Meaning: External blocklist list is no longer truncated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

47002 - LOG_ID_FILE_HASH_EMS_LIST_TRUNCATED_ENTER

Message ID: 47002

Message Description: LOG_ID_FILE_HASH_EMS_LIST_TRUNCATED_ENTER

Message Meaning: EMS file-hash list is truncated

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47003 - LOG_ID_FILE_HASH_EMS_LIST_TRUNCATED_EXIT

Message ID: 47003

Message Description: LOG_ID_FILE_HASH_EMS_LIST_TRUNCATED_EXIT

Message Meaning: EMS file-hash list is no longer truncated

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47004 - LOG_ID_FILE_HASH_EMS_LIST_LOAD

Message ID: 47004

Message Description: LOG_ID_FILE_HASH_EMS_LIST_LOAD

Message Meaning: EMS file-hash list loaded

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
desc	Description	string	128
reason	Reason	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47203 - LOG_ID_ENTER_BYPASS

Message ID: 47203

Message Description: LOG_ID_ENTER_BYPASS

Message Meaning: Bypass ports pair entered bypass mode

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47204 - LOG_ID_EXIT_BYPASS

Message ID: 47204

Message Description: LOG_ID_EXIT_BYPASS

Message Meaning: Bypass ports pair exited bypass mode

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47301 - LOG_ID_EVENT_REST_API_OK

Message ID: 47301

Message Description: LOG_ID_EVENT_REST_API_OK

Message Meaning: REST API request success

Type: Event

Category: rest-api

Severity: Information

Log Field Name	Description	Data Type	Length
url	URL	string	512

Log Field Name	Description	Data Type	Length
status	Status	string	23
path		string	512
method	Method	string	64
ui	User Interface	string	64
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

47302 - LOG_ID_EVENT_REST_API_ERR

Message ID: 47302

Message Description: LOG_ID_EVENT_REST_API_ERR

Message Meaning: REST API request failed

Type: Event

Category: rest-api

Severity: Error

Log Field Name	Description	Data Type	Length
url	URL	string	512
status	Status	string	23
path		string	512
method	Method	string	64
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

48040 - LOG_ID_WANOPT_TUNNEL_CREATE

Message ID: 48040

Message Description: LOG_ID_WANOPT_TUNNEL_CREATE

Message Meaning: WANOPT Tunnel successfully created

Type: Event

Category: wanopt

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
policyid	Policy ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

48041 - LOG_ID_WANOPT_TUNNEL_CLOSED

Message ID: 48041

Message Description: LOG_ID_WANOPT_TUNNEL_CLOSED

Message Meaning: WANOPT Tunnel closed

Type: Event

Category: wanopt

Severity: Information

Log Field Name	Description	Data Type	Length
wanin		uint64	20
wanout		uint64	20
remotetunnelid		uint32	10
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
policyid	Policy ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
tunnelid	IPsec VPN tunnel ID	uint32	10

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

48101 - LOG_ID_WANOPT_AUTH_FAIL_PSK

Message ID: 48101

Message Description: LOG_ID_WANOPT_AUTH_FAIL_PSK

Message Meaning: WAN Optimization peer PSK authentication failed

Type: Event

Category: wanopt

Severity: Error

Log Field Name	Description	Data Type	Length
host		string	256
authgrp		string	36
serial		uint32	10
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
policyid	Policy ID	uint32	10
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

48102 - LOG_ID_WANOPT_AUTH_FAIL_OTH

Message ID: 48102

Message Description: LOG_ID_WANOPT_AUTH_FAIL_OTH

Message Meaning: WAN Optimization peer authentication failed

Type: Event

Category: wanopt

Severity: Error

Log Field Name	Description	Data Type	Length
peer		string	36
authgrp		string	36
serial		uint32	10
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
policyid	Policy ID	uint32	10
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

48301 - LOG_ID_UNEXP_APP_TYPE

Message ID: 48301

Message Description: LOG_ID_UNEXP_APP_TYPE

Message Meaning: Unexpected application type for WAN Optimization

Type: Event

Category: wanopt

Severity: Critical

Log Field Name	Description	Data Type	Length
app-type		string	64
session_id	Session ID	uint32	10
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
dstip	Destination IP	ip	39
srcport	Source port	uint16	5
srcip	Source IP	ip	39
policyid	Policy ID	uint32	10
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

49002 - LOG_ID_VNP_DPDK_PRIMARY_RESTART

Message ID: 49002

Message Description: LOG_ID_VNP_DPDK_PRIMARY_RESTART

Message Meaning: VNP Primary restarted

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

49004 - LOGID_EVENT_HYPERV_SRIOV_SHOW_UP

Message ID: 49004

Message Description: LOGID_EVENT_HYPERV_SRIOV_SHOW_UP

Message Meaning: Hyper-V SR-IOV VF secondary is hot plugged

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

49005 - LOGID_EVENT_HYPERV_SRIOV_DISAPPEAR

Message ID: 49005

Message Description: LOGID_EVENT_HYPERV_SRIOV_DISAPPEAR

Message Meaning: Hyper-V SR-IOV VF secondary is hot unplugged

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

51000 - LOG_ID_NB_TBL_CHG

Message ID: 51000

Message Description: LOG_ID_NB_TBL_CHG

Message Meaning: Neighbor table changed

Type: Event

Category: router

Severity: Information

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
devintfname	HA device interface name	string	32
src_int	Source Interface	string	64
mac	MAC Address	string	17
service	Name of Service	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

52000 - LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_SUMMARY

Message ID: 52000

Message Description: LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_SUMMARY

Message Meaning: Security Rating summary

Type: Event

Category: security-rating

Severity: Notice

Log Field Name	Description	Data Type	Length
passedcount	Security Rating result passed count	int32	10
lowcount	Security Rating result failed count for low severity	int32	10
mediumcount	Security Rating result failed count for medium severity	int32	10
highcount	Security Rating result failed count for high severity	int32	10
criticalcount	Critical level threat count	int32	10
auditreporttype	Security Rating report type	string	20
auditscore	Security Rating score	string	20
audittime	Security Rating time	uint64	20
auditid	Security Rating ID	uint64	20
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

52001 - LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_CHANGE

Message ID: 52001

Message Description: LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_CHANGE

Message Meaning: Security Rating result change

Type: Event

Category: security-rating

Severity: Notice

Log Field Name	Description	Data Type	Length
passedcount	Security Rating result passed count	int32	10
lowcount	Security Rating result failed count for low severity	int32	10
mediumcount	Security Rating result failed count for medium severity	int32	10
highcount	Security Rating result failed count for high severity	int32	10
criticalcount	Critical level threat count	int32	10
auditreporttype	Security Rating report type	string	20
auditscore	Security Rating score	string	20
audittime	Security Rating time	uint64	20
auditid	Security Rating ID	uint64	20
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53000 - LOG_ID_SDNC_CONNECTED

Message ID: 53000

Message Description: LOG_ID_SDNC_CONNECTED

Message Meaning: Connected to SDN server

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53001 - LOG_ID_SDNC_DISCONNECTED

Message ID: 53001

Message Description: LOG_ID_SDNC_DISCONNECTED

Message Meaning: Disconnected from SDN server

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53002 - LOG_ID_SDNC_SUBSCRIBE

Message ID: 53002

Message Description: LOG_ID_SDNC_SUBSCRIBE

Message Meaning: Dynamic SDN address channel opened

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53003 - LOG_ID_SDNC_UNSUBSCRIBE

Message ID: 53003

Message Description: LOG_ID_SDNC_UNSUBSCRIBE

Message Meaning: Dynamic SDN address channel closed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53010 - LOG_ID_INTERNAL_FDS_FTC

Message ID: 53010

Message Description: LOG_ID_INTERNAL_FDS_FTC

Message Meaning: FortiToken-Cloud data received

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
role	IPsec peer role, initator or responder	string	9
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53050 - LOG_ID_FTC_AUTH_FAILED

Message ID: 53050

Message Description: LOG_ID_FTC_AUTH_FAILED

Message Meaning: FortiToken-Cloud authentication failure

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53200 - LOG_ID_CONNECTOR_OBJECT_ADD

Message ID: 53200

Message Description: LOG_ID_CONNECTOR_OBJECT_ADD

Message Meaning: Dynamic address added

Type: Event

Category: connector

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
netid		string	128
cldobjid		string	128
protocol		string	128
port	Port Number	uint16	5
addr	IP Address	string	80

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
cfgobj	Configuration object	string	256
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53201 - LOG_ID_CONNECTOR_OBJECT_REMOVE

Message ID: 53201

Message Description: LOG_ID_CONNECTOR_OBJECT_REMOVE

Message Meaning: Dynamic address removed

Type: Event

Category: connector

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
netid		string	128
cldobjid		string	128
protocol		string	128
port	Port Number	uint16	5
addr	IP Address	string	80
action	Policy Action	string	65
cfgobj	Configuration object	string	256

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53202 - LOG_ID_CONNECTOR_API_FAILED

Message ID: 53202

Message Description: LOG_ID_CONNECTOR_API_FAILED

Message Meaning: SDN Connector API failed

Type: Event

Category: connector

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
addr	IP Address	string	80
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53203 - LOG_ID_CONNECTOR_OBJECT_UPDATE

Message ID: 53203

Message Description: LOG_ID_CONNECTOR_OBJECT_UPDATE

Message Meaning: Dynamic address updated.

Type: Event

Category: connector

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
addr	IP Address	string	80
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53204 - LOG_ID_CONNECTOR_OBJECT_CANT_ADD

Message ID: 53204

Message Description: LOG_ID_CONNECTOR_OBJECT_CANT_ADD

Message Meaning: Dynamic address can't be added

Type: Event

Category: connector

Severity: Warning

Log Field Name	Description	Data Type	Length
fctemssn		string	16
msg	Log Message	string	4096
addr	IP Address	string	80
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53205 - LOG_ID_CONNECTOR_OBJECT_CANT_REMOVE

Message ID: 53205

Message Description: LOG_ID_CONNECTOR_OBJECT_CANT_REMOVE

Message Meaning: Dynamic address can't be removed

Type: Event

Category: connector

Severity: Warning

Log Field Name	Description	Data Type	Length
fctemssn		string	16
msg	Log Message	string	4096
addr	IP Address	string	80
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53300 - LOG_ID_VNE_PRO_UPDATE_COMPLETED

Message ID: 53300

Message Description: LOG_ID_VNE_PRO_UPDATE_COMPLETED

Message Meaning: VNE provision server update completed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
hostname	Hostname	string	128
server	Server IP Address	string	64
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53301 - LOG_ID_VNE_PRO_UPDATE_FAILED

Message ID: 53301

Message Description: LOG_ID_VNE_PRO_UPDATE_FAILED

Message Meaning: VNE provision server update failed

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
hostname	Hostname	string	128
server	Server IP Address	string	64
error	Error Reason for Log Upload to Forticloud	string	256
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53311 - LOG_ID_NPU_PER_MAPPING_ALLOCATION

Message ID: 53311

Message Description: LOG_ID_NPU_PER_MAPPING_ALLOCATION

Message Meaning: Resource per mapping allocation

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53312 - LOG_ID_NPD_INFO

Message ID: 53312

Message Description: LOG_ID_NPD_INFO

Message Meaning: NPD INFO

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53313 - LOG_ID_NPD_WARNING

Message ID: 53313

Message Description: LOG_ID_NPD_WARNING

Message Meaning: NPD WARNING MSG

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53314 - LOG_ID_NPD_ERROR

Message ID: 53314

Message Description: LOG_ID_NPD_ERROR

Message Meaning: NPD ERROR MSG

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53315 - LOG_ID_LPM_ERROR

Message ID: 53315

Message Description: LOG_ID_LPM_ERROR

Message Meaning: LPM ERROR MSG

Type: Event

Category: system

Severity: Error

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53316 - LOG_ID_LPM_INFO

Message ID: 53316

Message Description: LOG_ID_LPM_INFO

Message Meaning: LPM INFO MSG

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

53320 - LOG_ID_FORTICONVERTER_RESULT_READY

Message ID: 53320

Message Description: LOG_ID_FORTICONVERTER_RESULT_READY

Message Meaning: FortiConverter ticket has a result file ready

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
extension		string	20
filename		string	80
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53321 - LOG_ID_FORTICONVERTER_CONFIG_UPLOADED

Message ID: 53321

Message Description: LOG_ID_FORTICONVERTER_CONFIG_UPLOADED

Message Meaning: Uploaded local config to a FortiConverter ticket

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
ticket		string	40
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53400 - LOG_ID_FMG_TUNNEL_UP

Message ID: 53400

Message Description: LOG_ID_FMG_TUNNEL_UP

Message Meaning: Central Management connectivity is active

Type: Event

Category: system

Severity: Notice

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53401 - LOG_ID_FMG_TUNNEL_DOWN

Message ID: 53401

Message Description: LOG_ID_FMG_TUNNEL_DOWN

Message Meaning: Central Management connectivity is inactive

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
date	Date	string	10

53402 - LOG_ID_FGFM_RECOVERY

Message ID: 53402

Message Description: LOG_ID_FGFM_RECOVERY

Message Meaning: FGFM recovery is triggered

Type: Event

Category: system

Severity: Warning

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
status	Status	string	23
action	Policy Action	string	65
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53406 - LOG_ID_2GB_CSF_UPGRADE

Message ID: 53406

Message Description: LOG_ID_2GB_CSF_UPGRADE

Message Meaning: Security Fabric settings changed during upgrade

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

53407 - LOG_ID_FABRIC_VPN_PSK_SECRET_UPG_SET

Message ID: 53407

Message Description: LOG_ID_FABRIC_VPN_PSK_SECRET_UPG_SET

Message Meaning: Fabric VPN settings changed during upgrade

Type: Event

Category: system

Severity: Information

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logdesc	Log Description	string	4096
tz	Time zone	string	5
eventtime	Event time	uint64	20
vd	Virtual Domain Name	string	32
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Log Subtype	string	20
type	Log Type	string	16
logid	Log ID	string	10
time	Time	string	8
date	Date	string	10

63002 - LOG_ID_CIFS_CONN_FAIL

Message ID: 63002

Message Description: LOG_ID_CIFS_CONN_FAIL

Message Meaning: Unable to connect to the CIFS Domain Controller

Type: Event

Category: cifs-auth-fail

Severity: Warning

Log Field Name	Description	Data Type	Length
msg		string	4096
error		string	256
domainctrlprotocoltype		uint32	5
domainctrlauthtype		uint32	5
domainctrlauthstate		uint32	5
domainctrlusername		string	65
domainctrldomain		string	80
domainctrlname		string	64
domainctrlip		ip	39
profile		string	64
policyid		uint32	10
dst_int		string	64
src_int		string	64
dstport		uint16	5
srcport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
srcip		ip	39
dstintfrole		string	10
srcintfrole		string	10
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

63003 - LOG_ID_CIFS_AUTH_FAIL

Message ID: 63003

Message Description: LOG_ID_CIFS_AUTH_FAIL

Message Meaning: Unable to authenticate with the CIFS Domain Controller

Type: Event

Category: cifs-auth-fail

Severity: Warning

Log Field Name	Description	Data Type	Length
msg		string	4096
error		string	256
domainctrlprotocoltype		uint32	5
domainctrlauthtype		uint32	5
domainctrlauthstate		uint32	5
domainctrlusername		string	65

Log Field Name	Description	Data Type	Length
domainctrldomain		string	80
domainctrlname		string	64
domainctrlip		ip	39
profile		string	64
policyid		uint32	10
dst_int		string	64
src_int		string	64
dstport		uint16	5
srcport		uint16	5
dstip		ip	39
srcip		ip	39
dstintfrole		string	10
srcintfrole		string	10
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

63004 - LOG_ID_CIFS_AUTH_INTERNAL_ERROR

Message ID: 63004

Message Description: LOG_ID_CIFS_AUTH_INTERNAL_ERROR

Message Meaning: An error occurred in processing CIFS authentication

Type: Event

Category: cifs-auth-fail

Severity: Warning

Log Field Name	Description	Data Type	Length
msg		string	4096
error		string	256
domainctrlprotocoltype		uint32	5
domainctrlauthtype		uint32	5
domainctrlauthstate		uint32	5
domainctrlusername		string	65
domainctrldomain		string	80
domainctrlname		string	64
domainctrlip		ip	39
profile		string	64
policyid		uint32	10
dst_int		string	64
src_int		string	64
dstport		uint16	5
srcport		uint16	5
dstip		ip	39
srcip		ip	39
dstintfrole		string	10
srcintfrole		string	10
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

63005 - LOG_ID_CIFS_AUTH_KRB_ERROR

Message ID: 63005

Message Description: LOG_ID_CIFS_AUTH_KRB_ERROR

Message Meaning: An error occurred in processing CIFS authentication.

Type: Event

Category: cifs-auth-fail

Severity: Warning

Log Field Name	Description	Data Type	Length
msg		string	4096
error		string	256
domainctrlprotocoltype		uint32	5
domainctrlauthtype		uint32	5
domainctrlauthstate		uint32	5
domainctrlusername		string	65
domainctrldomain		string	80
domainctrlname		string	64
domainctrlip		ip	39
profile		string	64
policyid		uint32	10
dst_int		string	64
src_int		string	64
dstport		uint16	5
srcport		uint16	5
dstip		ip	39
srcip		ip	39
dstintfrole		string	10
srcintfrole		string	10
logdesc		string	4096
tz		string	5
eventtime		uint64	20
vd		string	32

Log Field Name	Description	Data Type	Length
devid		string	16
level		string	11
subtype		string	20
type		string	16
logid		string	10
time		string	8
date		string	10

FILE-FILTER

64000 - LOG_ID_FILE_FILTER_BLOCK

Message ID: 64000

Message Description: LOG_ID_FILE_FILTER_BLOCK

Message Meaning: File was blocked by file filter

Type: FILE-FILTER

Category: file-filter

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8

Log Field Name	Description	Data Type	Length
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	36
sender		string	128
rulename		string	36
referralurl		string	512
recipient		string	512
rawdata		string	20480
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pathname		string	256
msg		string	512
matchfiletype		string	23
matchfilename		string	256
logid		string	10
level		string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname		string	256
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	23
filesize		uint64	10
filename		string	256
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	512
authserver		string	64
attachment		string	3
agent		string	1024
action		string	20

64001 - LOG_ID_FILE_FILTER_LOG

Message ID: 64001

Message Description: LOG_ID_FILE_FILTER_LOG

Message Meaning: File was detected by file filter

Type: FILE-FILTER

Category: file-filter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	36
sender		string	128
rulename		string	36
referralurl		string	512

Log Field Name	Description	Data Type	Length
recipient		string	512
rawdata		string	20480
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pathname		string	256
msg		string	512
matchfiletype		string	23
matchfilename		string	256
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	23
filesize		uint64	10
filename		string	256
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10

Log Field Name	Description	Data Type	Length
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
cc		string	512
authserver		string	64
attachment		string	3
agent		string	1024
action		string	20

FORTI-SWITCH

56001 - LOG_ID_FSW_FLOW

Message ID: 56001

Message Description: LOG_ID_FSW_FLOW

Message Meaning: (null)

Type: FORTI-SWITCH

Category: fsw-flow

Severity: Information

Log Field Name	Description	Data Type	Length
vd		string	32
tz		string	5
type		string	16
time		string	8
switchid		string	32
subtype		string	20
srcip		ip	39

Log Field Name	Description	Data Type	Length
rcvdpkt		uint32	10
rcvdbyte		uint32	10
proto		uint8	3
logid		string	10
level		string	11
ftlkintf		string	32
eventtime		uint64	20
duration		uint32	10
dstip		ip	39
devid		string	16
date		string	10

GTP

41216 - LOGID_GTP_FORWARD

Message ID: 41216

Message Description: LOGID_GTP_FORWARD

Message Meaning: GTP forward

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
upteid		uint32	10
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
ugsn6		ip	39

Log Field Name	Description	Data Type	Length
u-gsn	User Plane GSN	ip	39
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39

Log Field Name	Description	Data Type	Length
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cgsn6		ip	39
c-gsn	Control Plane GSN	ip	39
apn	Access Point Name	string	128

41217 - LOGID_GTP_DENY

Message ID: 41217

Message Description: LOGID_GTP_DENY

Message Meaning: GTP deny

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
upteid		uint32	10
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
ugsn6		ip	39
u-gsn	User Plane GSN	ip	39

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128

Log Field Name	Description	Data Type	Length
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cgsn6		ip	39
c-gsn	Control Plane GSN	ip	39
apn	Access Point Name	string	128

41218 - LOGID_GTP_RATE_LIMIT

Message ID: 41218

Message Description: LOGID_GTP_RATE_LIMIT

Message Meaning: GTP rate limit

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
upteid		uint32	10
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
ugsn6		ip	39
u-gsn	User Plane GSN	ip	39
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20

Log Field Name	Description	Data Type	Length
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cgsn6		ip	39
c-gsn	Control Plane GSN	ip	39
apn	Access Point Name	string	128

41219 - LOGID_GTP_STATE_INVALID

Message ID: 41219

Message Description: LOGID_GTP_STATE_INVALID

Message Meaning: GTP state invalid

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
upteid		uint32	10
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
ugsn6		ip	39
u-gsn	User Plane GSN	ip	39
tz	Time zone	string	5
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39

Log Field Name	Description	Data Type	Length
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cgsn6		ip	39
c-gsn	Control Plane GSN	ip	39
apn	Access Point Name	string	128

41220 - LOGID_GTP_TUNNEL_LIMIT

Message ID: 41220

Message Description: LOGID_GTP_TUNNEL_LIMIT

Message Meaning: Tunnel limit GTP message. These messages occur only when the maximum number of GTP tunnels is reached. No new tunnels are created when the maximum number is reached

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
upteid		uint32	10
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
ugsn6		ip	39
u-gsn	User Plane GSN	ip	39
tz	Time zone	string	5
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39

Log Field Name	Description	Data Type	Length
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
cgsn6		ip	39
c-gsn	Control Plane GSN	ip	39
apn	Access Point Name	string	128

41221 - LOGID_GTP_TRAFFIC_COUNT

Message ID: 41221

Message Description: LOGID_GTP_TRAFFIC_COUNT

Message Meaning: Statistic summary information when the GTP tunnel is being torn down

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
usgsn6		ip	39
uggsn6		ip	39
u-sgsn-teid	User plane sgsn tunnel endpoint identifier	uint32	10
u-sgsn	User plane sgsn IP address	ip	39
u-pkts	User Plane Packets	uint64	20
u-ggsn-teid	User plane ggsn teid	uint32	10
u-ggsn	User plane ggsn IP address	ip	39
u-bytes	User Plane Data Bytes	uint64	20
duration	Tunnel duration	uint32	10
csgsn6		ip	39
clashtunnelidx		uint32	10

Log Field Name	Description	Data Type	Length
cggsn6		ip	39
c-sgsn-teid	Control Plane SGSN Tunnel Endpoint Identifier	uint32	10
c-sgsn	Control Plane SGSN IP Address	ip	39
c-pkts	Control Plane Packets	uint64	20
c-ggsn-teid	Control Plane GGSN Tunnel Endpoint Identifier	uint32	10
c-ggsn	Control Plane GGSN IP Address	ip	39
c-bytes	Control Plane Data Bytes	uint64	20
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
rai	Routing Area Identifier	string	32
profile	Profile Name	string	64
nsapi	Netscape Server Application Programming Interface	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
logid	Log ID	string	10
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16

Log Field Name	Description	Data Type	Length
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
devid	Device ID	string	16
date	Date	string	10
apn	Access Point Name	string	128

41222 - LOGID_GTP_USER_DATA

Message ID: 41222

Message Description: LOGID_GTP_USER_DATA

Message Meaning: GTP user data

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
user_data	User traffic content inside GTP-U tunnel	string	256
version	Version	uint32	64
vd	Virtual Domain Name	string	32
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
profile	Profile Name	string	64
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
devid	Device ID	string	16
date	Date	string	10
apn	Access Point Name	string	128

41223 - LOGID_GTPV2_FORWARD

Message ID: 41223

Message Description: LOGID_GTPV2_FORWARD

Message Meaning: GTPv2 forward message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpaddr6		ip	39
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10

Log Field Name	Description	Data Type	Length
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25

Log Field Name	Description	Data Type	Length
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
apn	Access Point Name	string	128

41224 - LOGID_GTPV2_DENY

Message ID: 41224

Message Description: LOGID_GTPV2_DENY

Message Meaning: GTPv2 deny message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpaddr6		ip	39
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
apn	Access Point Name	string	128

41225 - LOGID_GTPV2_RATE_LIMIT

Message ID: 41225

Message Description: LOGID_GTPV2_RATE_LIMIT

Message Meaning: GTPv2 rate limit message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpaddr6		ip	39
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
apn	Access Point Name	string	128

41226 - LOGID_GTPV2_STATE_INVALID

Message ID: 41226

Message Description: LOGID_GTPV2_STATE_INVALID

Message Meaning: GTPv2 state invalid message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpaddr6		ip	39
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
version	Version	uint32	64

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128

Log Field Name	Description	Data Type	Length
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
apn	Access Point Name	string	128

41227 - LOGID_GTPV2_TUNNEL_LIMIT

Message ID: 41227

Message Description: LOGID_GTPV2_TUNNEL_LIMIT

Message Meaning: Tunnel limit GTP (version 2) message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpaddr6		ip	39
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10

Log Field Name	Description	Data Type	Length
to6		ip	39
to	To	ip	512
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25

Log Field Name	Description	Data Type	Length
date	Date	string	10
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
apn	Access Point Name	string	128

41228 - LOGID_GTPV2_TRAFFIC_COUNT

Message ID: 41228

Message Description: LOGID_GTPV2_TRAFFIC_COUNT

Message Meaning: Statistic summary information when the GTPv2 tunnel is being torn down

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
cpulteid	control plane uplink teid	uint32	10
cpuladdr6		ip	39
cpuladdr	control plane uplink IP address	ip	39
cpdlteid	control plane downlink tunnel endpoint identifier	uint32	10
cpdlisrteid	control plane ISR downlink tunnel endpoint identifier	uint32	10
cpdlisraddr6		ip	39
cpdlisraddr	Control Plane ISR Downlink IP Address	ip	39
cpdladdr6		ip	39
cpdladdr	Control Plane Downlink IP Address	ip	39
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
u-pkts	User Plane Packets	uint64	20
u-bytes	User Plane Data Bytes	uint64	20
duration	Tunnel duration	uint32	10
clashtunnelidx		uint32	10
c-pkts	Control Plane Packets	uint64	20
c-bytes	Control Plane Data Bytes	uint64	20
version	Version	uint32	64
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
ulimnc		uint16	3
ulimcc		uint16	3
uli	User Location Information	string	120
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
timeoutdelete		uint8	3
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
selection	APN selection, which is one IE in gtp packet	string	14
rat-type	Radio Access Technology type	string	7
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
devid	Device ID	string	16
date	Date	string	10
apn	Access Point Name	string	128

41229 - LOGID_GTPU_FORWARD

Message ID: 41229

Message Description: LOGID_GTPU_FORWARD

Message Meaning: GTPU forward message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
apn	Access Point Name	string	128

41230 - LOGID_GTPU_DENY

Message ID: 41230

Message Description: LOGID_GTPU_DENY

Message Meaning: GTPU deny message

Type: GTP

Category: gtp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
tz	Time zone	string	5
type	Log Type	string	16
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
to6		ip	39
to	To	ip	512
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
profile	Profile Name	string	64
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
headerteid	Tunnel Endpoint ID Header	uint32	10
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
apn	Access Point Name	string	128

41231 - LOGID_PFCP_FORWARD

Message ID: 41231

Message Description: LOGID_PFCP_FORWARD

Message Meaning: PFCP forward message

Type: GTP

Category: pfcp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ufseidaddr		ip	39
ufseid		string	20
tz	Time zone	string	5
type	Log Type	string	16
to6		ip	39
to	To	ip	512
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
profile	Profile Name	string	64
nai		string	128

Log Field Name	Description	Data Type	Length
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
hseid		string	20
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cfseidaddr		ip	39
cfseid		string	20
apn	Access Point Name	string	128

41232 - LOGID_PFCP_DENY

Message ID: 41232

Message Description: LOGID_PFCP_DENY

Message Meaning: PFCP deny message

Type: GTP

Category: pfcp-all

Severity: Information

Log Field Name	Description	Data Type	Length
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ufseidaddr		ip	39
ufseid		string	20
tz	Time zone	string	5
type	Log Type	string	16
to6		ip	39
to	To	ip	512
time	Time	string	8
subtype	Log Subtype	string	20
status	Status	string	23
srcport	Source Port	uint16	5
seqnum	GTP packet sequence number	uint32	10
profile	Profile Name	string	64
nai		string	128
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
msgtypename		string	50
msg-type	Message Type	uint8	3
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
ietype	Malformed GTP IE number	uint8	3
hseid		string	20
from6		ip	39
from	From	ip	128
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39

Log Field Name	Description	Data Type	Length
dtlexp	Detailed Explanation	string	64
dstport	Destination Port	uint16	5
devid	Device ID	string	16
deny_cause	Deny Cause	string	25
date	Date	string	10
cfseidaddr		ip	39
cfseid		string	20
apn	Access Point Name	string	128

41233 - LOGID_PFCP_TRAFFIC_COUNT

Message ID: 41233

Message Description: LOGID_PFCP_TRAFFIC_COUNT

Message Meaning: Statistic summary information when the PFCP session is being torn down

Type: GTP

Category: pfcp-all

Severity: Information

Log Field Name	Description	Data Type	Length
u-pkts	User Plane Packets	uint64	20
u-bytes	User Plane Data Bytes	uint64	20
sessionid		uint32	10
duration	Tunnel duration	uint32	10
c-pkts	Control Plane Packets	uint64	20
c-bytes	Control Plane Data Bytes	uint64	20
version	Version	uint32	64
vd	Virtual Domain Name	string	32
ufseidaddr		ip	39
ufseid		string	20
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
status	Status	string	23
profile	Profile Name	string	64
nai		string	128
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
logid	Log ID	string	10
level	Log Level	string	11
imsi	International mobile subscriber ID	string	16
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
eventtime	Event time line	uint64	20
endusraddress6		ip	39
end-usr-address	End user IP Address	ip	39
devid	Device ID	string	16
date	Date	string	10
cfseidaddr		ip	39
cfseid		string	20
apn	Access Point Name	string	128

ICAP

60000 - LOG_ID_ICAP_SERVER_ERROR

Message ID: 60000

Message Description: LOG_ID_ICAP_SERVER_ERROR

Message Meaning: Traffic blocked as it cannot be forwarded to ICAP Server.

Type: ICAP

Category: icap

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		string	64
violations		string	256
vd		string	32
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srccountry		string	64
sessionid		uint32	10
service		string	5
reason		string	4096
proto		uint8	3
profile		string	64
policytype		string	24
policyid		uint32	10
msg		string	4096
logid		string	10
level		string	11
infection		string	96
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
action		string	17

60001 - LOG_ID_ICAP_INFECTION_BLOCK

Message ID: 60001

Message Description: LOG_ID_ICAP_INFECTION_BLOCK

Message Meaning: Traffic blocked as ICAP server found infection.

Type: ICAP

Category: icap

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		string	64
violations		string	256
vd		string	32
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32

Log Field Name	Description	Data Type	Length
srccountry		string	64
sessionid		uint32	10
service		string	5
reason		string	4096
proto		uint8	3
profile		string	64
policytype		string	24
policyid		uint32	10
msg		string	4096
logid		string	10
level		string	11
infection		string	96
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
action		string	17

60002 - LOG_ID_ICAP_CONN_ERROR

Message ID: 60002

Message Description: LOG_ID_ICAP_CONN_ERROR

Message Meaning: Traffic dropped as ICAP connection is closed.

Type: ICAP

Category: icap

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		string	64
violations		string	256
vd		string	32
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srccountry		string	64
sessionid		uint32	10
service		string	5
reason		string	4096
proto		uint8	3
profile		string	64
policytype		string	24
policyid		uint32	10
msg		string	4096
logid		string	10
level		string	11
infection		string	96
eventtype		string	32
eventtime		uint64	20
dstuuid		string	37
dstport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
action		string	17

IPS

16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP

Message ID: 16384

Message Description: LOGID_ATTCK_SIGNATURE_TCP_UDP

Message Meaning: Attack detected by UDP/TCP signature

Type: IPS

Category: signature

Severity: Alert

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
referralurl		string	512
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11
incidentserialno	Incident serial number	uint32	10
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128

Log Field Name	Description	Data Type	Length
fctuid	FortiClient UID	string	32
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackid	Attack ID	uint32	10
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
agent		string	1024
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

16385 - LOGID_ATTCK_SIGNATURE_ICMP

Message ID: 16385

Message Description: LOGID_ATTCK_SIGNATURE_ICMP

Message Meaning: Attack detected by ICMP signature

Type: IPS

Category: signature

Severity: Alert

Log Field Name	Description	Data Type	Length
icmptype	The type of ICMP message	string	6
icmpid	Source port of the ICMP message	string	8
icmpcode	Destination Port of the ICMP message	string	6
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
rawdataid		string	10

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11
incidentserialno	Incident serial number	uint32	10
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10

Log Field Name	Description	Data Type	Length
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackid	Attack ID	uint32	10
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

16386 - LOGID_ATTCK_SIGNATURE_OTHERS

Message ID: 16386

Message Description: LOGID_ATTCK_SIGNATURE_OTHERS

Message Meaning: Attack detected by other signature

Type: IPS

Category: signature

Severity: Alert

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16

Log Field Name	Description	Data Type	Length
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11
incidentserialno	Incident serial number	uint32	10
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackid	Attack ID	uint32	10
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

16399 - LOGID_ATTACK_MALICIOUS_URL

Message ID: 16399

Message Description: LOGID_ATTACK_MALICIOUS_URL

Message Meaning: Attack detected by a malicious URL

Type: IPS

Category: malicious-url

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
referralurl		string	512
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
agent		string	1024

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

16400 - LOGID_ATTACK_BOTNET_WARNING

Message ID: 16400

Message Description: LOGID_ATTACK_BOTNET_WARNING

Message Meaning: Botnet C&amp;C Communication (warning)

Type: IPS

Category: botnet

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackid	Attack ID	uint32	10
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

16401 - LOGID_ATTACK_BOTNET_NOTIF

Message ID: 16401

Message Description: LOGID_ATTACK_BOTNET_NOTIF

Message Meaning: Botnet C&amp;C Communication (notice)

Type: IPS

Category: botnet

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
user	User name	string	256
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz		string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log Subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	64
srcdomain		string	255
srccountry	Country name for Source IP	string	64
severity	Severity of the attack	string	8
sessionid	Session ID	uint32	10
service	Service name	string	80
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
rawdataid		string	10
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Profile name for IPS	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message for the attack	string	518
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	IPS Event Type	string	32
eventtime	Time when detection occured	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	64
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid	Deivce ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation Level	string	10
craction	Action performed by Threat Weight	uint32	10
authserver	Authentication server for the user	string	64
attackid	Attack ID	uint32	10
attackcontextid	Attack context ID / total	string	10
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attack	Attack Name	string	256
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16

SSH

61000 - LOG_ID_SSH_COMMAND_BLOCK

Message ID: 61000

Message Description: LOG_ID_SSH_COMMAND_BLOCK

Message Meaning: SSH shell command is blocked

Type: SSH

Category: ssh-command

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61001 - LOG_ID_SSH_COMMAND_BLOCK_ALERT

Message ID: 61001

Message Description: LOG_ID_SSH_COMMAND_BLOCK_ALERT

Message Meaning: SSH shell command is blocked

Type: SSH

Category: ssh-command

Severity: Alert

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61002 - LOG_ID_SSH_COMMAND_PASS

Message ID: 61002

Message Description: LOG_ID_SSH_COMMAND_PASS

Message Meaning: SSH shell command is detected

Type: SSH

Category: ssh-command

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61003 - LOG_ID_SSH_COMMAND_PASS_ALERT

Message ID: 61003

Message Description: LOG_ID_SSH_COMMAND_PASS_ALERT

Message Meaning: SSH shell command is detected

Type: SSH

Category: ssh-command

Severity: Alert

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256

Log Field Name	Description	Data Type	Length
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61010 - LOG_ID_SSH_CHANNEL_BLOCK

Message ID: 61010

Message Description: LOG_ID_SSH_CHANNEL_BLOCK

Message Meaning: SSH channel is blocked

Type: SSH

Category: ssh-channel

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61011 - LOG_ID_SSH_CHANNEL_PASS

Message ID: 61011

Message Description: LOG_ID_SSH_CHANNEL_PASS

Message Meaning: SSH channel is detected

Type: SSH

Category: ssh-channel

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15

Log Field Name	Description	Data Type	Length
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61012 - LOG_ID_SSH_HOST_KEY_WARNING

Message ID: 61012

Message Description: LOG_ID_SSH_HOST_KEY_WARNING

Message Meaning: SSH connection is blocked, because host-key is not trust

Type: SSH

Category: ssh-hostkey

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61013 - LOG_ID_SSH_HOST_KEY_NOTIF

Message ID: 61013

Message Description: LOG_ID_SSH_HOST_KEY_NOTIF

Message Meaning: SSH host-key is not trust

Type: SSH

Category: ssh-hostkey

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20

Log Field Name	Description	Data Type	Length
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61014 - LOG_ID_SSH_UNSUPPORT_PROTO_BLOCK

Message ID: 61014

Message Description: LOG_ID_SSH_UNSUPPORT_PROTO_BLOCK

Message Meaning: SSH connection is blocked, because unsupported SSH protocol

Type: SSH

Category: ssh-unsupport-proto

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

61015 - LOG_ID_SSH_UNSUPPORT_PROTO_PASS

Message ID: 61015

Message Description: LOG_ID_SSH_UNSUPPORT_PROTO_PASS

Message Meaning: Unsupported SSH protocol is detected

Type: SSH

Category: ssh-unsupport-proto

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User name for authentication	string	256
unauthusersource	Unauthenticated User Source	string	66
unauthuser	Unauthenticated User	string	66
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity level of shell command	string	8
sessionid	Session ID	uint32	10
proto	Protocol number	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
login	SSH login Name	string	128

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log level	string	11
hostkeystatus		string	15
group	Group name for authentication	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
direction	Direction of session	string	4096
devid	Device ID	string	16
date	Date	string	10
command	Shell command	string	256
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

SSL

62004 - LOG_ID_SSL_EXEMPT_ADDR

Message ID: 62004

Message Description: LOG_ID_SSL_EXEMPT_ADDR

Message Meaning: SSL connection is exempted based on address

Type: SSL

Category: ssl-exempt

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7

Log Field Name	Description	Data Type	Length
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
catdesc		string	64
cat		uint8	3
authalgo		string	7
action		string	20

62006 - LOG_ID_SSL_EXEMPT_ALLOWLIST

Message ID: 62006

Message Description: LOG_ID_SSL_EXEMPT_ALLOWLIST

Message Meaning: SSL connection is exempted based on allowlist

Type: SSL

Category: ssl-exempt

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32

Log Field Name	Description	Data Type	Length
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
catdesc		string	64
cat		uint8	3
authalgo		string	7
action		string	20

62007 - LOG_ID_SSL_EXEMPT_FTGD_CATEGORY

Message ID: 62007

Message Description: LOG_ID_SSL_EXEMPT_FTGD_CATEGORY

Message Meaning: SSL connection is exempted based on FortiGuard category rating

Type: SSL

Category: ssl-exempt

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3

Log Field Name	Description	Data Type	Length
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256

Log Field Name	Description	Data Type	Length
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
catdesc		string	64
cat		uint8	3
authalgo		string	7
action		string	20

62008 - LOG_ID_SSL_EXEMPT_LOCAL_CATEGORY

Message ID: 62008

Message Description: LOG_ID_SSL_EXEMPT_LOCAL_CATEGORY

Message Meaning: SSL connection is exempted based on local category rating

Type: SSL

Category: ssl-exempt

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32

Log Field Name	Description	Data Type	Length
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512

Log Field Name	Description	Data Type	Length
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
catdesc		string	64
cat		uint8	3
authalgo		string	7
action		string	20

62009 - LOG_ID_SSL_EXEMPT_USER_CATEGORY

Message ID: 62009

Message Description: LOG_ID_SSL_EXEMPT_USER_CATEGORY

Message Meaning: SSL connection is exempted based on user category rating

Type: SSL

Category: ssl-exempt

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
catdesc		string	64
cat		uint8	3
authalgo		string	7
action		string	20

62100 - LOG_ID_SSL_NEGOTIATION_INSPECT

Message ID: 62100

Message Description: LOG_ID_SSL_NEGOTIATION_INSPECT

Message Meaning: Continue inspect the SSL connection

Type: SSL

Category: ssl-negotiation

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20
msg		string	512
logid		string	10
level		string	11
kxproto		string	7

Log Field Name	Description	Data Type	Length
kxcurve		string	32
keysize		uint16	4
keyalgo		string	8
issuer		string	64
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40
authalgo		string	7
action		string	20

62101 - LOG_ID_SSL_NEGOTIATION_BLOCK

Message ID: 62101

Message Description: LOG_ID_SSL_NEGOTIATION_BLOCK

Message Meaning: SSL connection is blocked due to its SSL negotiation

Type: SSL

Category: ssl-negotiation

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20

Log Field Name	Description	Data Type	Length
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
keysize		uint16	4
keyalgo		string	8
issuer		string	64
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40
authalgo		string	7
action		string	20

62102 - LOG_ID_SSL_NEGOTIATION_BYPASS

Message ID: 62102

Message Description: LOG_ID_SSL_NEGOTIATION_BYPASS

Message Meaning: SSL connection is bypassed due to its SSL negotiation

Type: SSL

Category: ssl-negotiation

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
keysize		uint16	4
keyalgo		string	8
issuer		string	64
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40

Log Field Name	Description	Data Type	Length
authalgo		string	7
action		string	20

62103 - LOG_ID_SSL_NEGOTIATION_INFO

Message ID: 62103

Message Description: LOG_ID_SSL_NEGOTIATION_INFO

Message Meaning: SSL connection information

Type: SSL

Category: ssl-negotiation

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40

Log Field Name	Description	Data Type	Length
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
keysize		uint16	4
keyalgo		string	8
issuer		string	64
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10

Log Field Name	Description	Data Type	Length
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40
authalgo		string	7
action		string	20

62200 - LOG_ID_SSL_SERVER_CERT_INFO

Message ID: 62200

Message Description: LOG_ID_SSL_SERVER_CERT_INFO

Message Meaning: SSL server certificate information

Type: SSL

Category: ssl-server-cert-info

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5

Log Field Name	Description	Data Type	Length
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
keysize		uint16	4
keyalgo		string	8
issuer		string	64
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40
authalgo		string	7
action		string	20

62220 - LOG_ID_SSL_HANDSHAKE_INFO

Message ID: 62220

Message Description: LOG_ID_SSL_HANDSHAKE_INFO

Message Meaning: SSL handshake information

Type: SSL

Category: ssl-handshake

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5

Log Field Name	Description	Data Type	Length
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sn		string	40
ski		string	64
sessionid		uint32	10
service		string	5
san		string	448
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
notbefore		string	20
notafter		string	20
mitm		string	3
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
keysize		uint16	4

Log Field Name	Description	Data Type	Length
keyalgo		string	8
issuer		string	64
hostname		string	256
handshake		string	11
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cn		string	64
cipher		string	6
certhash		string	40
authalgo		string	7
action		string	20

62300 - LOG_ID_SSL_ANOMALY_CERT_BLOCKLISTED

Message ID: 62300

Message Description: LOG_ID_SSL_ANOMALY_CERT_BLOCKLISTED

Message Meaning: SSL connection is blocked due to the server certificate is blocklisted

Type: SSL

Category: ssl-anomaly

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32

Log Field Name	Description	Data Type	Length
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62301 - LOG_ID_SSL_ANOMALY_CERT_RESIGN_TRUSTED

Message ID: 62301

Message Description: LOG_ID_SSL_ANOMALY_CERT_RESIGN_TRUSTED

Message Meaning: Server certificate has security problem

Type: SSL

Category: ssl-anomaly

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3

Log Field Name	Description	Data Type	Length
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256

Log Field Name	Description	Data Type	Length
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62302 - LOG_ID_SSL_ANOMALY_CERT_RESIGN_UNTRUSTED

Message ID: 62302

Message Description: LOG_ID_SSL_ANOMALY_CERT_RESIGN_UNTRUSTED

Message Meaning: Re-signed server certificate as untrusted due to security problem

Type: SSL

Category: ssl-anomaly

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3

Log Field Name	Description	Data Type	Length
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256

Log Field Name	Description	Data Type	Length
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62303 - LOG_ID_SSL_ANOMALY_CERT_BLOCKED

Message ID: 62303

Message Description: LOG_ID_SSL_ANOMALY_CERT_BLOCKED

Message Meaning: SSL connection is blocked due to server certificate security problem

Type: SSL

Category: ssl-anomaly

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32

Log Field Name	Description	Data Type	Length
user		string	256
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512

Log Field Name	Description	Data Type	Length
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62304 - LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED

Message ID: 62304

Message Description: LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED

Message Meaning: SSL connection is blocked due to server certificate and SNI mismatched

Type: SSL

Category: ssl-anomaly

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62305 - LOG_ID_SSL_ANOMALY_CERT_PROBE_FAILURE_BLOCK

Message ID: 62305

Message Description: LOG_ID_SSL_ANOMALY_CERT_PROBE_FAILURE_BLOCK

Message Meaning: SSL connection is blocked due to unable to retrieve server's certificate

Type: SSL

Category: ssl-anomaly

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62306 - LOG_ID_SSL_ANOMALY_CERT_PROBE_FAILURE_PASS

Message ID: 62306

Message Description: LOG_ID_SSL_ANOMALY_CERT_PROBE_FAILURE_PASS

Message Meaning: SSL connection is bypassed due to unable to retrieve server's certificate

Type: SSL

Category: ssl-anomaly

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62307 - LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED_INFO

Message ID: 62307

Message Description: LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED_INFO

Message Meaning: Server certificate and SNI mismatched

Type: SSL

Category: ssl-anomaly

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62308 - LOG_ID_SSL_ANOMALY_HANDSHAKE_FAILURE

Message ID: 62308

Message Description: LOG_ID_SSL_ANOMALY_HANDSHAKE_FAILURE

Message Meaning: Error occured during SSL handshake.

Type: SSL

Category: ssl-anomaly

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
unauthuser		string	66
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32

Log Field Name	Description	Data Type	Length
eventtime		uint64	20
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

62309 - LOG_ID_SSL_ANOMALY_CERT_INVALID

Message ID: 62309

Message Description: LOG_ID_SSL_ANOMALY_CERT_INVALID

Message Meaning: Server certificate has security problem

Type: SSL

Category: ssl-anomaly

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
unauthusersource		string	66
unauthuser		string	66

Log Field Name	Description	Data Type	Length
tz		string	5
type		string	16
tlsver		string	8
time		string	8
subtype		string	20
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sni		string	256
sessionid		uint32	10
service		string	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
kxproto		string	7
kxcurve		string	32
hostname		string	256
group		string	512
fctuid		string	32
eventtype		string	32
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
eventsubtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
devid		string	16
date		string	10
cipher		string	6
certhash		string	40
certdesc		string	64
authalgo		string	7
action		string	20

Traffic

2 - LOG_ID_TRAFFIC_ALLOW

Message ID: 2

Message Description: LOG_ID_TRAFFIC_ALLOW

Message Meaning: Allowed traffic

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66

Log Field Name	Description	Data Type	Length
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

3 - LOG_ID_TRAFFIC_DENY

Message ID: 3

Message Description: LOG_ID_TRAFFIC_DENY

Message Meaning: Traffic violation

Type: Traffic

Category: forward

Severity: Warning

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14

Log Field Name	Description	Data Type	Length
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10

Log Field Name	Description	Data Type	Length
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20

Log Field Name	Description	Data Type	Length
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

4 - LOG_ID_TRAFFIC_OTHER_START

Message ID: 4

Message Description: LOG_ID_TRAFFIC_OTHER_START

Message Meaning: Traffic other session start

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4

Log Field Name	Description	Data Type	Length
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

5 - LOG_ID_TRAFFIC_OTHER_ICMP_ALLOW

Message ID: 5

Message Description: LOG_ID_TRAFFIC_OTHER_ICMP_ALLOW

Message Meaning: Traffic allowed ICMP

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37

Log Field Name	Description	Data Type	Length
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10

Log Field Name	Description	Data Type	Length
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64

Log Field Name	Description	Data Type	Length
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96

Log Field Name	Description	Data Type	Length
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

6 - LOG_ID_TRAFFIC_OTHER_ICMP_DENY

Message ID: 6

Message Description: LOG_ID_TRAFFIC_OTHER_ICMP_DENY

Message Meaning: Traffic denied ICMP

Type: Traffic

Category: forward

Severity: Warning

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256

Log Field Name	Description	Data Type	Length
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32

Log Field Name	Description	Data Type	Length
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20

Log Field Name	Description	Data Type	Length
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16

Log Field Name	Description	Data Type	Length
accessproxy		string	80
accessctrl		string	80

7 - LOG_ID_TRAFFIC_OTHER_INVALID

Message ID: 7

Message Description: LOG_ID_TRAFFIC_OTHER_INVALID

Message Meaning: Traffic other invalid

Type: Traffic

Category: forward

Severity: Warning

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66

Log Field Name	Description	Data Type	Length
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80

Log Field Name	Description	Data Type	Length
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

8 - LOG_ID_TRAFFIC_WANOPT

Message ID: 8

Message Description: LOG_ID_TRAFFIC_WANOPT

Message Meaning: WAN optimization traffic

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10

Log Field Name	Description	Data Type	Length
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10

Log Field Name	Description	Data Type	Length
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

9 - LOG_ID_TRAFFIC_WEBCACHE

Message ID: 9

Message Description: LOG_ID_TRAFFIC_WEBCACHE

Message Meaning: Web cache traffic

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10

Log Field Name	Description	Data Type	Length
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10

Log Field Name	Description	Data Type	Length
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512

Log Field Name	Description	Data Type	Length
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64

Log Field Name	Description	Data Type	Length
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

10 - LOG_ID_TRAFFIC_EXPLICIT_PROXY

Message ID: 10

Message Description: LOG_ID_TRAFFIC_EXPLICIT_PROXY

Message Meaning: Explicit proxy traffic

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10

Log Field Name	Description	Data Type	Length
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39

Log Field Name	Description	Data Type	Length
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4

Log Field Name	Description	Data Type	Length
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8

Log Field Name	Description	Data Type	Length
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5

Log Field Name	Description	Data Type	Length
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64

Log Field Name	Description	Data Type	Length
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

11 - LOG_ID_TRAFFIC_FAIL_CONN

Message ID: 11

Message Description: LOG_ID_TRAFFIC_FAIL_CONN

Message Meaning: Failed connection attempts

Type: Traffic

Category: forward

Severity: Warning

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9

Log Field Name	Description	Data Type	Length
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36

Log Field Name	Description	Data Type	Length
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66

Log Field Name	Description	Data Type	Length
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

12 - LOG_ID_TRAFFIC_MULTICAST

Message ID: 12

Message Description: LOG_ID_TRAFFIC_MULTICAST

Message Meaning: Multicast traffic

Type: Traffic

Category: multicast

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3

Log Field Name	Description	Data Type	Length
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66

Log Field Name	Description	Data Type	Length
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32

Log Field Name	Description	Data Type	Length
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8

Log Field Name	Description	Data Type	Length
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

13 - LOG_ID_TRAFFIC_END_FORWARD

Message ID: 13

Message Description: LOG_ID_TRAFFIC_END_FORWARD

Message Meaning: Forward traffic

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10

Log Field Name	Description	Data Type	Length
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10

Log Field Name	Description	Data Type	Length
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512

Log Field Name	Description	Data Type	Length
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64

Log Field Name	Description	Data Type	Length
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

14 - LOG_ID_TRAFFIC_END_LOCAL

Message ID: 14

Message Description: LOG_ID_TRAFFIC_END_LOCAL

Message Meaning: Local traffic

Type: Traffic

Category: local

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14

Log Field Name	Description	Data Type	Length
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10

Log Field Name	Description	Data Type	Length
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20

Log Field Name	Description	Data Type	Length
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

15 - LOG_ID_TRAFFIC_START_FORWARD

Message ID: 15

Message Description: LOG_ID_TRAFFIC_START_FORWARD

Message Meaning: Forward traffic session start

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4

Log Field Name	Description	Data Type	Length
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

16 - LOG_ID_TRAFFIC_START_LOCAL

Message ID: 16

Message Description: LOG_ID_TRAFFIC_START_LOCAL

Message Meaning: Local traffic session start

Type: Traffic

Category: local

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37

Log Field Name	Description	Data Type	Length
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10

Log Field Name	Description	Data Type	Length
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64

Log Field Name	Description	Data Type	Length
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96

Log Field Name	Description	Data Type	Length
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

17 - LOG_ID_TRAFFIC_SNIFFER

Message ID: 17

Message Description: LOG_ID_TRAFFIC_SNIFFER

Message Meaning: Sniffer traffic

Type: Traffic

Category: sniffer

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256

Log Field Name	Description	Data Type	Length
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32

Log Field Name	Description	Data Type	Length
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20

Log Field Name	Description	Data Type	Length
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application Name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

19 - LOG_ID_TRAFFIC_BROADCAST

Message ID: 19

Message Description: LOG_ID_TRAFFIC_BROADCAST

Message Meaning: Broadcast traffic

Type: Traffic

Category: multicast

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37

Log Field Name	Description	Data Type	Length
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10

Log Field Name	Description	Data Type	Length
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64

Log Field Name	Description	Data Type	Length
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96

Log Field Name	Description	Data Type	Length
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

20 - LOG_ID_TRAFFIC_STAT

Message ID: 20

Message Description: LOG_ID_TRAFFIC_STAT

Message Meaning: Forward traffic statistics

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256

Log Field Name	Description	Data Type	Length
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32

Log Field Name	Description	Data Type	Length
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20

Log Field Name	Description	Data Type	Length
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16

Log Field Name	Description	Data Type	Length
accessproxy		string	80
accessctrl		string	80

21 - LOG_ID_TRAFFIC_SNIFFER_STAT

Message ID: 21

Message Description: LOG_ID_TRAFFIC_SNIFFER_STAT

Message Meaning: Sniffer traffic statistics

Type: Traffic

Category: sniffer

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66

Log Field Name	Description	Data Type	Length
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80

Log Field Name	Description	Data Type	Length
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application Name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

22 - LOG_ID_TRAFFIC_UTM_CORRELATION

Message ID: 22

Message Description: LOG_ID_TRAFFIC_UTM_CORRELATION

Message Meaning: Forward traffic for UTM correlation

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
countweb	Number of Web Filter logs associated with the session	uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countvpatch		uint32	10
countssl		uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countsctpf		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
counticap		uint32	10
countff		uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countcifs		uint32	10
countcasb		uint32	10
countav	Number of AV logs associated with the session	uint32	10
countapp	Number of App Ctrl logs associated with the session	uint32	10
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10

Log Field Name	Description	Data Type	Length
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10

Log Field Name	Description	Data Type	Length
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

24 - LOG_ID_TRAFFIC_ZTNA

Message ID: 24

Message Description: LOG_ID_TRAFFIC_ZTNA

Message Meaning: ZTNA traffic

Type: Traffic

Category: ztna

Severity: Notice

Log Field Name	Description	Data Type	Length
wanout	WAN outgoing traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanin	WAN incoming traffic in bytes	uint64	20
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlname		string	36
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vrf	Virtual router forwarding	uint8	3
vpntype	The type of the VPN tunnel	string	14
vip		string	64
vd	Virtual domain name	string	32
utmaction	Security action performed by UTM	string	32
user	User name	string	256
url	URL	string	512
unauthusersource	The method used to detect unauthenticated user name	string	66
unauthuser	Unauthenticated user name	string	66
tz	Time zone	string	5
type	Log type	string	16
tunnelid		uint32	10
transport	NAT Source Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
transip	NAT Source IP	ip	39
tranport	NAT Destination Port	uint16	5
tranip	NAT Destination IP	ip	39
trandisp	NAT translation type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
sslaction	Action taken by ssl-ssh-profile	string	26
srcuuid	UUID of the Source Address Object	string	37
srcthreatfeed		string	36
srcswversion		string	66
srcssid	Source SSID	string	33
srcserver	Source server	uint8	3
srcreputation		uint32	10
srcremote		ip	39
srcregion		string	64
srcport	Source protocol port number	uint16	5
srcname	Source name	string	256
srcmacvendor		string	66
srcmac	MAC address associated with the Source IP	string	17
srcip	Source IP address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source interface name	string	32
srcinetsvc	Internet service name for the source	string	64
srchwversion		string	66
srchwvendor		string	66
srcfamily		string	66
srcdomain		string	255
srccountry	Country name for Source IP	string	64
srccity		string	64
snr		int8	4

Log Field Name	Description	Data Type	Length
signal		int8	4
shapingpolicyname		string	36
shapingpolicyid	Shaping Policy ID	uint32	10
shapersentname	Traffic shaper name for sent traffic	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shaperperipname	Traffic shaper name (per IP)	string	36
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
sessionid	Session ID	uint32	10
service	Name of Service	string	80
sentpktdelta		uint32	20
sentpkt	Sent Packets	uint32	10
sentdelta	Delta Sent Bytes	uint64	20
sentbyte	Sent Bytes	uint64	20
saasname		string	80
replysrcintf		string	32
replydstintf		string	32
realserverid		uint32	10
rcvdpktdelta		uint32	20
rcvdpkt	Received Packets	uint32	10
rcvddelta	Delta Received Bytes	uint64	20
rcvdbyte	Received Bytes	uint64	20
radioband	Radio Band	string	64
psrcport		uint16	5
proxyapptype		string	16
proto	Protocol Number	uint8	3
poluuid	UUID of the Firewall Policy	string	37
policytype	Policy type	string	24
policyname	Policy name	string	36

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Firewall Policy ID	uint32	10
pdstport		uint16	5
osname	Name of the device's OS	string	66
msg	Log message	string	512
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
masterdstmac	Destination master MAC address	string	17
logid	Log ID	string	10
level	Log Level	string	11
lanout	LAN outgoing traffic in bytes	uint64	20
lanin	LAN incoming traffic in bytes	uint64	20
identifier		uint16	5
group	User group name	string	512
gatewayid		uint32	10
fwdsrv		string	64
fctuid	FortiClient UID	string	32
eventtime	Epoch time in nanoseconds	uint64	20
emsconnection		string	8
durationdelta		uint32	20
duration	Duration of the session	uint32	10
dstuuid	UUID of the Destination Address Object	string	37
dstuser		string	256
dstunauthusersource		string	66
dstunauthuser		string	66
dstthreatfeed		string	36
dstswversion		string	66
dstssid	Destination SSID	string	33
dstserver	Destination Server	uint8	3
dstreputation		uint32	10
dstregion		string	64

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port Number	uint16	5
dstosname	Destination OS name	string	66
dstname	Destination name	string	256
dstmac	Destination Mac Address	string	17
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstinetsvc	Internet service name for the destination	string	64
dsthwversion		string	66
dsthwvendor		string	66
dstfamily		string	66
dstdevtype	Destination Device Type	string	66
dstcountry	Country name for the destination IP	string	64
dstcity		string	64
dstauthserver		string	64
devtype	Device Type	string	66
devid	Device Serial Number	string	16
date	Date	string	10
crscore	Threat Weight score	uint32	10
crlevel	Threat Weight level	string	10
craction	Action performed by Threat Weight	uint32	10
comment	Customized policy comment	string	1024
clientdevicetags		string	512
clientdeviceowner		string	80
clientdevicemanageable		string	16
clientdeviceid		string	80
clientdeviceems		string	16
clientcert		string	10
channel	WiFi Channel	uint32	10
centralnatid	central-snat-map id	uint32	10

Log Field Name	Description	Data Type	Length
authserver	Remote Authentication server	string	64
apsn	Access Point serial number	string	36
apprisk	Application Risk Level	string	16
applist	Application Control profile (name)	string	64
appid	Application ID	uint32	10
appcat	Application category	string	64
appact	The security action from app control	string	16
app	Application Name	string	96
ap	Access Point name	string	36
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
accessproxy		string	80
accessctrl		string	80

25 - LOG_ID_TRAFFIC_SFLOW

Message ID: 25

Message Description: LOG_ID_TRAFFIC_SFLOW

Message Meaning: Sflow sample

Type: Traffic

Category: forward

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Subtype of the traffic	string	20
logid	Log ID	string	10
level	Log Level	string	11
eventtime	Epoch time in nanoseconds	uint64	20
devid	Device Serial Number	string	16
date	Date	string	10

virtual-patch

64600 - LOG_ID_OT_VPATCH_BLOCK

Message ID: 64600

Message Description: LOG_ID_OT_VPATCH_BLOCK

Message Meaning: Traffic was blocked by OT virtual patch

Type: virtual-patch

Category: ot-vpatch

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39

Log Field Name	Description	Data Type	Length
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
severity		string	8
sessionid		uint32	10
service		string	80
referralurl		string	512
rawdataid		string	10
rawdata		string	20480
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
forwardedfor		string	128
fctuid		string	32
eventtype		string	32

Log Field Name	Description	Data Type	Length
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
authserver		string	64
attackid		uint32	10
attackcontextid		string	10
attackcontext		string	2048
attack		string	256
agent		string	1024
action		string	16

64601 - LOG_ID_OT_VPATCH_LOG

Message ID: 64601

Message Description: LOG_ID_OT_VPATCH_LOG

Message Meaning: Traffic was detected by OT virtual patch

Type: virtual-patch

Category: ot-vpatch

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256

Log Field Name	Description	Data Type	Length
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
severity		string	8
sessionid		uint32	10
service		string	80
referralurl		string	512
rawdataid		string	10
rawdata		string	20480
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
logid		string	10
level		string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname		string	256
group		string	512
forwardedfor		string	128
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
authserver		string	64
attackid		uint32	10
attackcontextid		string	10
attackcontext		string	2048
attack		string	256
agent		string	1024
action		string	16

64610 - LOG_ID_LOCALIN_VPATCH_BLOCK

Message ID: 64610

Message Description: LOG_ID_LOCALIN_VPATCH_BLOCK

Message Meaning: Traffic was blocked by local-in virtual patch

Type: virtual-patch

Category: localin-vpatch

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
severity		string	8
sessionid		uint32	10
service		string	80
referralurl		string	512
rawdataid		string	10
rawdata		string	20480
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10

Log Field Name	Description	Data Type	Length
pdstport		uint16	5
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
forwardedfor		string	128
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
authserver		string	64
attackid		uint32	10
attackcontextid		string	10
attackcontext		string	2048
attack		string	256
agent		string	1024
action		string	16

64611 - LOG_ID_LOCALIN_VPATCH_LOG

Message ID: 64611

Message Description: LOG_ID_LOCALIN_VPATCH_LOG

Message Meaning: Traffic was detected by local-in virtual patch

Type: virtual-patch

Category: localin-vpatch

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	64
srcdomain		string	255
srccountry		string	64
severity		string	8
sessionid		uint32	10
service		string	80
referralurl		string	512
rawdataid		string	10
rawdata		string	20480
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
forwardedfor		string	128
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	64
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
authserver		string	64
attackid		uint32	10
attackcontextid		string	10
attackcontext		string	2048
attack		string	256
agent		string	1024
action		string	16

Virus

8192 - MESGID_INFECT_WARNING

Message ID: 8192

Message Description: MESGID_INFECT_WARNING

Message Meaning: Infected file detected by the FortiGate unit and blocked

Type: Virus

Category: infected

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65

Log Field Name	Description	Data Type	Length
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10

Log Field Name	Description	Data Type	Length
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8193 - MESGID_INFECT_NOTIF

Message ID: 8193

Message Description: MESGID_INFECT_NOTIF

Message Meaning: Infected file detected by the FortiGate unit and it passed

Type: Virus

Category: infected

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64

Log Field Name	Description	Data Type	Length
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8194 - MESGID_INFECT_MIME_WARNING

Message ID: 8194

Message Description: MESGID_INFECT_MIME_WARNING

Message Meaning: MIME header detected to have a virus and blocked

Type: Virus

Category: infected

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5

Log Field Name	Description	Data Type	Length
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128

Log Field Name	Description	Data Type	Length
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10

Log Field Name	Description	Data Type	Length
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8195 - MESGID_INFECT_MIME_NOTIF

Message ID: 8195

Message Description: MESGID_INFECT_MIME_NOTIF

Message Meaning: MIME header infected and passed

Type: Virus

Category: infected

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8200 - MESGID_MIME_FILETYPE_EXE_WARNING

Message ID: 8200

Message Description: MESGID_MIME_FILETYPE_EXE_WARNING

Message Meaning: File is an executable (warning)

Type: Virus

Category: filetype-executable

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
user	Username (authentication)	string	256
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8201 - MESGID_MIME_FILETYPE_EXE_NOTIF

Message ID: 8201

Message Description: MESGID_MIME_FILETYPE_EXE_NOTIF

Message Meaning: File is an executable (notice)

Type: Virus

Category: filetype-executable

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512

Log Field Name	Description	Data Type	Length
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
checksum	The checksum of the scanned file	string	16
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8202 - MESGID_AVQUERY_WARNING

Message ID: 8202

Message Description: MESGID_AVQUERY_WARNING

Message Meaning: File reported infected by Outbreak Prevention (warning)

Type: Virus

Category: outbreak-prevention

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16

Log Field Name	Description	Data Type	Length
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11

Log Field Name	Description	Data Type	Length
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8203 - MESGID_AVQUERY_NOTIF

Message ID: 8203

Message Description: MESGID_AVQUERY_NOTIF

Message Meaning: File reported infected by Outbreak Prevention (notice)

Type: Virus

Category: outbreak-prevention

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46

Log Field Name	Description	Data Type	Length
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8204 - MESGID_MIME_AVQUERY_WARNING

Message ID: 8204

Message Description: MESGID_MIME_AVQUERY_WARNING

Message Meaning: MIME data reported infected by Outbreak Prevention (warning)

Type: Virus

Category: outbreak-prevention

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8205 - MESGID_MIME_AVQUERY_NOTIF

Message ID: 8205

Message Description: MESGID_MIME_AVQUERY_NOTIF

Message Meaning: MIME data reported infected by Outbreak Prevention (notice)

Type: Virus

Category: outbreak-prevention

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8206 - MESGID_AV_EXEMPT_NOTIF

Message ID: 8206

Message Description: MESGID_AV_EXEMPT_NOTIF

Message Meaning: File reported matched AV exempt list (notice)

Type: Virus

Category: exempt-hash

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8207 - MESGID_MIME_AV_EXEMPT_NOTIF

Message ID: 8207

Message Description: MESGID_MIME_AV_EXEMPT_NOTIF

Message Meaning: MIME data reported matched AV exempt list (notice)

Type: Virus

Category: exempt-hash

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16

Log Field Name	Description	Data Type	Length
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11

Log Field Name	Description	Data Type	Length
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8212 - MESGID_MALWARE_LIST_WARNING

Message ID: 8212

Message Description: MESGID_MALWARE_LIST_WARNING

Message Meaning: File reported infected by external malware list (warning)

Type: Virus

Category: malware-list

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46

Log Field Name	Description	Data Type	Length
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8213 - MESGID_MALWARE_LIST_NOTIF

Message ID: 8213

Message Description: MESGID_MALWARE_LIST_NOTIF

Message Meaning: File reported infected by external malware list (notice)

Type: Virus

Category: malware-list

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8214 - MESGID_MIME_MALWARE_LIST_WARNING

Message ID: 8214

Message Description: MESGID_MIME_MALWARE_LIST_WARNING

Message Meaning: MIME data reported infected by external malware list (warning)

Type: Virus

Category: malware-list

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8215 - MESGID_MIME_MALWARE_LIST_NOTIF

Message ID: 8215

Message Description: MESGID_MIME_MALWARE_LIST_NOTIF

Message Meaning: MIME data reported infected by external malware list (notice)

Type: Virus

Category: malware-list

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8216 - MESGID_FILE_HASH_EMS_WARNING

Message ID: 8216

Message Description: MESGID_FILE_HASH_EMS_WARNING

Message Meaning: File reported infected by EMS threat feed (warning)

Type: Virus

Category: ems-threat-feed

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256

Log Field Name	Description	Data Type	Length
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11

Log Field Name	Description	Data Type	Length
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10

Log Field Name	Description	Data Type	Length
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8217 - MESGID_FILE_HASH_EMS_NOTIF

Message ID: 8217

Message Description: MESGID_FILE_HASH_EMS_NOTIF

Message Meaning: File reported infected by EMS threat feed (notice)

Type: Virus

Category: ems-threat-feed

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5

Log Field Name	Description	Data Type	Length
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8218 - MESGID_MIME_FILE_HASH_EMS_WARNING

Message ID: 8218

Message Description: MESGID_MIME_FILE_HASH_EMS_WARNING

Message Meaning: MIME data reported infected by EMS threat feed (warning)

Type: Virus

Category: ems-threat-feed

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32

Log Field Name	Description	Data Type	Length
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8219 - MESGID_MIME_FILE_HASH_EMS_NOTIF

Message ID: 8219

Message Description: MESGID_MIME_FILE_HASH_EMS_NOTIF

Message Meaning: MIME data reported infected by EMS threat feed (notice)

Type: Virus

Category: ems-threat-feed

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512

Log Field Name	Description	Data Type	Length
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8220 - MESGID_ICB_WARNING

Message ID: 8220

Message Description: MESGID_ICB_WARNING

Message Meaning: File reported infected by Inline Block (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5

Log Field Name	Description	Data Type	Length
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256

Log Field Name	Description	Data Type	Length
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8221 - MESGID_ICB_NOTIF

Message ID: 8221

Message Description: MESGID_ICB_NOTIF

Message Meaning: File reported infected by Inline Block (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512

Log Field Name	Description	Data Type	Length
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3

Log Field Name	Description	Data Type	Length
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8222 - MESGID_MIME_ICB_WARNING

Message ID: 8222

Message Description: MESGID_MIME_ICB_WARNING

Message Meaning: MIME data reported infected by Inline Block (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256

Log Field Name	Description	Data Type	Length
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11

Log Field Name	Description	Data Type	Length
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10

Log Field Name	Description	Data Type	Length
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8223 - MESGID_MIME_ICB_NOTIF

Message ID: 8223

Message Description: MESGID_MIME_ICB_NOTIF

Message Meaning: MIME data reported infected by Inline Block (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5

Log Field Name	Description	Data Type	Length
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8224 - MESGID_ICB_TIMEOUT_WARNING

Message ID: 8224

Message Description: MESGID_ICB_TIMEOUT_WARNING

Message Meaning: Inline Block scan timeout (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32

Log Field Name	Description	Data Type	Length
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8225 - MESGID_ICB_TIMEOUT_NOTIF

Message ID: 8225

Message Description: MESGID_ICB_TIMEOUT_NOTIF

Message Meaning: Inline Block scan timeout (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512

Log Field Name	Description	Data Type	Length
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8226 - MESGID_MIME_ICB_TIMEOUT_WARNING

Message ID: 8226

Message Description: MESGID_MIME_ICB_TIMEOUT_WARNING

Message Meaning: MIME data reported Inline Block scan timeout (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5

Log Field Name	Description	Data Type	Length
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256

Log Field Name	Description	Data Type	Length
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8227 - MESGID_MIME_ICB_TIMEOUT_NOTIF

Message ID: 8227

Message Description: MESGID_MIME_ICB_TIMEOUT_NOTIF

Message Meaning: MIME data reported Inline Block scan timeout (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512

Log Field Name	Description	Data Type	Length
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3

Log Field Name	Description	Data Type	Length
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8228 - MESGID_ICB_ERROR_WARNING

Message ID: 8228

Message Description: MESGID_ICB_ERROR_WARNING

Message Meaning: Inline Block scan error (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256

Log Field Name	Description	Data Type	Length
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11

Log Field Name	Description	Data Type	Length
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10

Log Field Name	Description	Data Type	Length
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8229 - MESGID_ICB_ERROR_NOTIF

Message ID: 8229

Message Description: MESGID_ICB_ERROR_NOTIF

Message Meaning: Inline Block scan error (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5

Log Field Name	Description	Data Type	Length
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8230 - MESGID_MIME_ICB_ERROR_WARNING

Message ID: 8230

Message Description: MESGID_MIME_ICB_ERROR_WARNING

Message Meaning: MIME data reported Inline Block scan error (warning)

Type: Virus

Category: inline-block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32

Log Field Name	Description	Data Type	Length
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8231 - MESGID_MIME_ICB_ERROR_NOTIF

Message ID: 8231

Message Description: MESGID_MIME_ICB_ERROR_NOTIF

Message Meaning: MIME data reported Inline Block scan error (notice)

Type: Virus

Category: inline-block

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid		uint32	10
viruscat		string	32
virus		string	128
vd		string	32
user		string	256
url		string	512
unauthusersource		string	66
unauthuser		string	66
tz		string	5
type		string	16
trueclntip		ip	39
to		string	512
time		string	8
subtype		string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid		uint32	10
service		string	5
sender		string	128
referralurl		string	512
ref		string	512

Log Field Name	Description	Data Type	Length
recipient		string	512
rawdata		string	20480
quarskip		string	46
psrcport		uint16	5
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid		uint32	10
pdstport		uint16	5
pathname		string	256
msg		string	4096
logid		string	10
level		string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group		string	512
from		string	128
forwardedfor		string	128
filetype		string	16
filename		string	256
filehashsrc		string	32
filehash		string	64
fctuid		string	32

Log Field Name	Description	Data Type	Length
eventtype		string	32
eventtime		uint64	20
dtype		string	32
dstuuid		string	37
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
dstcountry		string	64
dstauthserver		string	64
direction		string	8
devid		string	16
date		string	10
crscore		uint32	10
crlevel		string	10
craction		uint32	10
contentdisarmed		string	13
checksum		string	16
cdrcontent		string	256
cc		string	512
authserver		string	64
attachment		string	3
analyticssubmit		string	10
analyticscksum		string	64
agent		string	1024
action		string	18

8448 - MESGID_BLOCK_WARNING

Message ID: 8448

Message Description: MESGID_BLOCK_WARNING

Message Meaning: FortiGate unit blocked a file because it contains a virus

Type: Virus

Category: filename

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
quarskip	Quarantine skip explanation	string	46

Log Field Name	Description	Data Type	Length
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
filetype	File type	string	16
filename	File name	string	256
filefilter	The filter used to identify the affected file	string	12
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
checksum	The checksum of the scanned file	string	16
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8450 - MESGID_BLOCK_MIME_WARNING

Message ID: 8450

Message Description: MESGID_BLOCK_MIME_WARNING

Message Meaning: FortiGate unit blocked a file because it contains a virus (MIME)

Type: Virus

Category: mimefragmented

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16

Log Field Name	Description	Data Type	Length
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20

Log Field Name	Description	Data Type	Length
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
filetype	File type	string	16
filename	File name	string	256
filefilter	The filter used to identify the affected file	string	12
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
checksum	The checksum of the scanned file	string	16
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8451 - MESGID_BLOCK_MIME_NOTIF

Message ID: 8451

Message Description: MESGID_BLOCK_MIME_NOTIF

Message Meaning: FortiGate unit blocked a file because it contains a virus (MIME)

Type: Virus

Category: mimefragmented

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5

Log Field Name	Description	Data Type	Length
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
filetype	File type	string	16
filename	File name	string	256
filefilter	The filter used to identify the affected file	string	12
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
checksum	The checksum of the scanned file	string	16
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8452 - MESGID_BLOCK_COMMAND

Message ID: 8452

Message Description: MESGID_BLOCK_COMMAND

Message Meaning: FortiGate unit blocked a virus command

Type: Virus

Category: command-blocked

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
referralurl		string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
fctuid	Forticlient user ID	string	32

Log Field Name	Description	Data Type	Length
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
command		string	16
authserver	Server used to authenticate the involved user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8704 - MESGID_OVERSIZE_WARNING

Message ID: 8704

Message Description: MESGID_OVERSIZE_WARNING

Message Meaning: Defined file size limit was exceeded

Type: Virus

Category: oversize

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37

Log Field Name	Description	Data Type	Length
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8705 - MESGID_OVERSIZE_NOTIF

Message ID: 8705

Message Description: MESGID_OVERSIZE_NOTIF

Message Meaning: File size limit was exceeded

Type: Virus

Category: oversize

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20

Log Field Name	Description	Data Type	Length
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8708 - MESGID_OVERSIZE_STREAM_UNCOMP_WARNING

Message ID: 8708

Message Description: MESGID_OVERSIZE_STREAM_UNCOMP_WARNING

Message Meaning: Stream-based uncompression reached size limit.

Type: Virus

Category: oversize

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8709 - MESGID_OVERSIZE_STREAM_UNCOMP_NOTIF

Message ID: 8709

Message Description: MESGID_OVERSIZE_STREAM_UNCOMP_NOTIF

Message Meaning: Stream-based uncompression reached size limit.

Type: Virus

Category: oversize

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
recipient	Email addresses from the SMTP envelope	string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8720 - MESGID_SWITCH_PROTO_WARNING

Message ID: 8720

Message Description: MESGID_SWITCH_PROTO_WARNING

Message Meaning: Switching protocols request (warning)

Type: Virus

Category: unknown

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
switchproto		string	128
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
referralurl		string	512
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8721 - MESGID_SWITCH_PROTO_NOTIF

Message ID: 8721

Message Description: MESGID_SWITCH_PROTO_NOTIF

Message Meaning: Switching protocols request (notice)

Type: Virus

Category: unknown

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
switchproto		string	128
subtype	Subtype of the virus log	string	20
subservice		string	16
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
referralurl		string	512
psrcport		uint16	5
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
authserver	Server used to authenticate the involved user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8960 - MESGID_SCAN_UNCOMPSIZELIMIT_WARNING

Message ID: 8960

Message Description: MESGID_SCAN_UNCOMPSIZELIMIT_WARNING

Message Meaning: File reached the uncompressed nested limit

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8961 - MESGID_SCAN_UNCOMPSIZELIMIT_NOTIF

Message ID: 8961

Message Description: MESGID_SCAN_UNCOMPSIZELIMIT_NOTIF

Message Meaning: File reached the uncompressed size limit

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480

Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32

Log Field Name	Description	Data Type	Length
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8962 - MESGID_SCAN_ARCHIVE_ENCRYPTED_WARNING

Message ID: 8962

Message Description: MESGID_SCAN_ARCHIVE_ENCRYPTED_WARNING

Message Meaning: Archived file is corrupted

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8963 - MESGID_SCAN_ARCHIVE_ENCRYPTED_NOTIF

Message ID: 8963

Message Description: MESGID_SCAN_ARCHIVE_ENCRYPTED_NOTIF

Message Meaning: Archived file is encrypted

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8964 - MESGID_SCAN_ARCHIVE_CORRUPTED_WARNING

Message ID: 8964

Message Description: MESGID_SCAN_ARCHIVE_CORRUPTED_WARNING

Message Meaning: Corrupted archive (warning)

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8965 - MESGID_SCAN_ARCHIVE_CORRUPTED_NOTIF

Message ID: 8965

Message Description: MESGID_SCAN_ARCHIVE_CORRUPTED_NOTIF

Message Meaning: Corrupted archive (notice)

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16

Log Field Name	Description	Data Type	Length
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11

Log Field Name	Description	Data Type	Length
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8966 - MESGID_SCAN_ARCHIVE_MULTIPART_WARNING

Message ID: 8966

Message Description: MESGID_SCAN_ARCHIVE_MULTIPART_WARNING

Message Meaning: File is a multipart archive or contains multiple files within the archive

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46

Log Field Name	Description	Data Type	Length
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8967 - MESGID_SCAN_ARCHIVE_MULTIPART_NOTIF

Message ID: 8967

Message Description: MESGID_SCAN_ARCHIVE_MULTIPART_NOTIF

Message Meaning: File is a multipart archive or contains multiple files within the archive

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8968 - MESGID_SCAN_ARCHIVE_NESTED_WARNING

Message ID: 8968

Message Description: MESGID_SCAN_ARCHIVE_NESTED_WARNING

Message Meaning: File is a nested archived file

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8969 - MESGID_SCAN_ARCHIVE_NESTED_NOTIF

Message ID: 8969

Message Description: MESGID_SCAN_ARCHIVE_NESTED_NOTIF

Message Meaning: File is an archived type unhandled

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8970 - MESGID_SCAN_ARCHIVE_OVERSIZE_WARNING

Message ID: 8970

Message Description: MESGID_SCAN_ARCHIVE_OVERSIZE_WARNING

Message Meaning: Archived file is oversized

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16

Log Field Name	Description	Data Type	Length
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11

Log Field Name	Description	Data Type	Length
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8971 - MESGID_SCAN_ARCHIVE_OVERSIZE_NOTIF

Message ID: 8971

Message Description: MESGID_SCAN_ARCHIVE_OVERSIZE_NOTIF

Message Meaning: Archived file is oversized

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46

Log Field Name	Description	Data Type	Length
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8972 - MESGID_SCAN_ARCHIVE_UNHANDLED_WARNING

Message ID: 8972

Message Description: MESGID_SCAN_ARCHIVE_UNHANDLED_WARNING

Message Meaning: Unhandled archive (warning)

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8973 - MESGID_SCAN_ARCHIVE_UNHANDLED_NOTIF

Message ID: 8973

Message Description: MESGID_SCAN_ARCHIVE_UNHANDLED_NOTIF

Message Meaning: Unhandled archive (notice)

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8974 - MESGID_SCAN_AV_ENGINE_LOAD_FAILED_ERROR

Message ID: 8974

Message Description: MESGID_SCAN_AV_ENGINE_LOAD_FAILED_ERROR

Message Meaning: AV Engine load failed

Type: Virus

Category: scanerror

Severity: Error

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8975 - MESGID_SCAN_ARCHIVE_PARTIALLYCORRUPTED_WARNING

Message ID: 8975

Message Description: MESGID_SCAN_ARCHIVE_PARTIALLYCORRUPTED_WARNING

Message Meaning: Partially corrupted archive (warning)

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8976 - MESGID_SCAN_ARCHIVE_PARTIALLYCORRUPTED_NOTIF

Message ID: 8976

Message Description: MESGID_SCAN_ARCHIVE_PARTIALLYCORRUPTED_NOTIF

Message Meaning: Partially corrupted archive (notice)

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10

Log Field Name	Description	Data Type	Length
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512

Log Field Name	Description	Data Type	Length
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64

Log Field Name	Description	Data Type	Length
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8979 - MESGID_SCAN_ARCHIVE_TIMEOUT_WARNING

Message ID: 8979

Message Description: MESGID_SCAN_ARCHIVE_TIMEOUT_WARNING

Message Meaning: Archive scan timeout (warning)

Type: Virus

Category: scanerror

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8980 - MESGID_SCAN_ARCHIVE_TIMEOUT_NOTIF

Message ID: 8980

Message Description: MESGID_SCAN_ARCHIVE_TIMEOUT_NOTIF

Message Meaning: Archive scan timeout (notice)

Type: Virus

Category: scanerror

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8981 - MESGID_SCAN_AV_CDR_INTERNAL_ERROR

Message ID: 8981

Message Description: MESGID_SCAN_AV_CDR_INTERNAL_ERROR

Message Meaning: AV CDR engine internal error

Type: Virus

Category: scanerror

Severity: Error

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

8982 - MESGID_SCAN_AV_MAX_MEMORY_REACHED_ERROR

Message ID: 8982

Message Description: MESGID_SCAN_AV_MAX_MEMORY_REACHED_ERROR

Message Meaning: Exceeded max AV memory

Type: Virus

Category: scanerror

Severity: Error

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9233 - MESGID_ANALYTICS_SUBMITTED

Message ID: 9233

Message Description: MESGID_ANALYTICS_SUBMITTED

Message Meaning: File submitted to Sandbox

Type: Virus

Category: analytics

Severity: Information

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480

Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32

Log Field Name	Description	Data Type	Length
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9234 - MESGID_ANALYTICS_INFECT_WARNING

Message ID: 9234

Message Description: MESGID_ANALYTICS_INFECT_WARNING

Message Meaning: File reported infected by FortiSandbox (warning)

Type: Virus

Category: infected

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16

Log Field Name	Description	Data Type	Length
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9235 - MESGID_ANALYTICS_INFECT_NOTIF

Message ID: 9235

Message Description: MESGID_ANALYTICS_INFECT_NOTIF

Message Meaning: File reported infected by FortiSandbox (notice)

Type: Virus

Category: infected

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9236 - MESGID_ANALYTICS_INFECT_MIME_WARNING

Message ID: 9236

Message Description: MESGID_ANALYTICS_INFECT_MIME_WARNING

Message Meaning: File reported infected by FortiSandbox (warning)

Type: Virus

Category: infected

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512

Log Field Name	Description	Data Type	Length
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9237 - MESGID_ANALYTICS_INFECT_MIME_NOTIF

Message ID: 9237

Message Description: MESGID_ANALYTICS_INFECT_MIME_NOTIF

Message Meaning: File reported infected by FortiSandbox (notice)

Type: Virus

Category: infected

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
virusid	Virus ID (unique virus identifier)	uint32	10
viruscat		string	32
virus	Virus Name	string	128
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16

Log Field Name	Description	Data Type	Length
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sharename		string	256
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
referralurl		string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
quarskip	Quarantine skip explanation	string	46
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
pdstport		uint16	5
pathname		string	256
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11

Log Field Name	Description	Data Type	Length
icbverdict		string	5
icbseverity		string	11
icbfiletype		string	10
icbfileid		string	65
icbconfidence		string	6
icbaction		string	7
httpmethod		string	20
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filetype	File type	string	16
filename	File name	string	256
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16

Log Field Name	Description	Data Type	Length
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticssubmit	The flag for analytics submission	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9238 - MESGID_ANALYTICS_FSA_RESULT

Message ID: 9238

Message Description: MESGID_ANALYTICS_FSA_RESULT

Message Meaning: File verdict returned from FortiSandbox

Type: Virus

Category: analytics

Severity: Notice

Log Field Name	Description	Data Type	Length
fsaverdict	FortiSandbox Verdict returned to FortiGate after analysis (clean, low risk, med risk, high risk, malicious)	string	32
vd	VDOM name	string	32
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Subtype of the virus log	string	20
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcdomain		string	255
service	Proxy service which scanned this traffic	string	5
logid	Log ID	string	10
level	Log level	string	11
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dtype	Data type for virus category	string	32
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
devid		string	16
date	Date	string	10
analyticscksum	The checksum of the file submitted for analytics	string	64
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9239 - MESGID_CONTENT_DISARM_NOTIF

Message ID: 9239

Message Description: MESGID_CONTENT_DISARM_NOTIF

Message Meaning: Active content detected by Content Disarm engine

Type: Virus

Category: content-disarm

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
group	Group name (authentication)	string	512
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
eventid		uint32	10
epoch		uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticscksum	The checksum of the file submitted for analytics	string	64
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9240 - MESGID_CONTENT_DISARM_WARNING

Message ID: 9240

Message Description: MESGID_CONTENT_DISARM_WARNING

Message Meaning: File was disarmed by Content Disarm engine

Type: Virus

Category: content-disarm

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
unauthusersource		string	66
unauthuser		string	66
tz	Time Zone	string	5
type	Log type	string	16

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
time	Time	string	8
subtype	Subtype of the virus log	string	20
subservice		string	16
subject		string	256
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
sender	Email address from the SMTP envelope	string	128
recipient	Email addresses from the SMTP envelope	string	512
rawdata		string	20480
psrcport		uint16	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
pdstport		uint16	5
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
group	Group name (authentication)	string	512

Log Field Name	Description	Data Type	Length
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
forwardedfor		string	128
filename	File name	string	256
fctuid	Forticlient user ID	string	32
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
eventid		uint32	10
epoch		uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Message/packets direction	string	8
devid		string	16
date	Date	string	10
crscore	Threat Weight Score	uint32	10
crlevel	Threat Weight Level	string	10
craction	Threat Weight action	uint32	10
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
checksum	The checksum of the scanned file	string	16
cdrcontent		string	256
cc		string	512
authserver	Server used to authenticate the involved user	string	64
attachment		string	3
analyticscksum	The checksum of the file submitted for analytics	string	64

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9241 - LOG_ID_UNKNOWN_CE_BLOCK

Message ID: 9241

Message Description: LOG_ID_UNKNOWN_CE_BLOCK

Message Meaning: Unknown content-encoding detected and blocked

Type: Virus

Category: unknown

Severity: Warning

Log Field Name	Description	Data Type	Length
contentencoding		string	512
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Subtype of the virus log	string	20
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policyid	Policy ID	uint32	10
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
group	Group name (authentication)	string	512
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
devid		string	16
date	Date	string	10
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

9242 - LOG_ID_UNKNOWN_CE_BYPASS

Message ID: 9242

Message Description: LOG_ID_UNKNOWN_CE_BYPASS

Message Meaning: Scan is bypassed due to unknown content-encoding

Type: Virus

Category: unknown

Severity: Notice

Log Field Name	Description	Data Type	Length
contentencoding		string	512

Log Field Name	Description	Data Type	Length
vrf		uint8	3
vd	VDOM name	string	32
user	Username (authentication)	string	256
url	The URL address	string	512
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Subtype of the virus log	string	20
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
sessionid	Session ID	uint32	10
service	Proxy service which scanned this traffic	string	5
proto	Protocol number	uint8	3
profile	The name of the profile that was used to detect and take action	string	64
poluuid		string	37
policyid	Policy ID	uint32	10
msg	Log message	string	4096
logid	Log ID	string	10
level	Log level	string	11
group	Group name (authentication)	string	512
eventtype	Event type of AV	string	32
eventtime	Time when detection occured	uint64	20
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
devid		string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18

VoIP

44032 - LOGID_EVENT_VOIP_SIP

Message ID: 44032

Message Description: LOGID_EVENT_VOIP_SIP

Message Meaning: VoIP SIP

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
logsrc		string	32
to	Destination address	string	512
from	Where call was originated from	string	128
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
dir	Destination Interface	string	16
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
status	Status. Ex: status="blocked" , status= "start"	string	23
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
dst_int	Destination Interface	string	16

Log Field Name	Description	Data Type	Length
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44033 - LOGID_EVENT_VOIP_SIP_BLOCK

Message ID: 44033

Message Description: LOGID_EVENT_VOIP_SIP_BLOCK

Message Meaning: VoIP SIP blocked

Type: VoIP

Category: voip

Severity: Notice

Log Field Name	Description	Data Type	Length
count	Session count	uint32	10
request_name	Name of request. Ex: request_name="INVITE" or "NOTIFY"	string	64
message_type	Message Type. Ex: message_type="request"	string	16
reason	Reason. Ex: reason="unrecognized-form"	string	128
logsrc		string	32
to	Destination address	string	512
from	Where call was originated from	string	128
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
dir	Destination Interface	string	16
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
status	Status. Ex: status="blocked" , status= "start"	string	23
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
dst_int	Destination Interface	string	16
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20

Log Field Name	Description	Data Type	Length
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44034 - LOGID_EVENT_VOIP_SIP_FUZZING

Message ID: 44034

Message Description: LOGID_EVENT_VOIP_SIP_FUZZING

Message Meaning: VoIP SIP fuzzing

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
column	Ex: column=16	uint32	10
line	SIP header line	string	128
malform_data	Malformed header data	uint32	10
malform_desc	Malformed header description	string	47
request_name	Name of request. Ex: request_name="INVITE" or "NOTIFY"	string	64
message_type	Message Type. Ex: message_type="request"	string	16
logsrc		string	32
attack		string	256
attackid		uint32	10
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
dir	Destination Interface	string	16

Log Field Name	Description	Data Type	Length
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
dst_int	Destination Interface	string	16
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44035 - LOGID_EVENT_VOIP_SCCP_REGISTER

Message ID: 44035

Message Description: LOGID_EVENT_VOIP_SCCP_REGISTER

Message Meaning: VoIP SCCP registered

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
phone	Phone	string	64
locip	Local IP	ip	39
status	Status. Ex: status="blocked" , status= "start"	string	23
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44036 - LOGID_EVENT_VOIP_SCCP_UNREGISTER

Message ID: 44036

Message Description: LOGID_EVENT_VOIP_SCCP_UNREGISTER

Message Meaning: VoIP SCCP unregistered

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
phone	Phone	string	64
locip	Local IP	ip	39
reason	Reason. Ex: reason="unrecognized-form"	string	128
status	Status. Ex: status="blocked" , status= "start"	string	23
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44037 - LOGID_EVENT_VOIP_SCCP_CALL_BLOCK

Message ID: 44037

Message Description: LOGID_EVENT_VOIP_SCCP_CALL_BLOCK

Message Meaning: VoIP SCCP call blocked

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
phone	Phone	string	64
locip	Local IP	ip	39
reason	Reason. Ex: reason="unrecognized-form"	string	128
status	Status. Ex: status="blocked" , status= "start"	string	23

Log Field Name	Description	Data Type	Length
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

44038 - LOGID_EVENT_VOIP_SCCP_CALL_INFO

Message ID: 44038

Message Description: LOGID_EVENT_VOIP_SCCP_CALL_INFO

Message Meaning: VoIP SCCP call information

Type: VoIP

Category: voip

Severity: Information

Log Field Name	Description	Data Type	Length
remport	Remote Port	uint16	5
remip	Remote IP	ip	39
locport	Local Port	uint16	5
phone	Phone	string	64
locip	Local IP	ip	39
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
status	Status. Ex: status="blocked" , status= "start"	string	23
action	Action. Eg. block , allow	string	15
kind	Kind of service. Typically it will have value "call"	string	10
voip_proto	SIP/SCCP/MGCP/h323	string	4
profile	Name or number of associated VOIP profile	string	64
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
dst_int	Destination Interface	string	16
src_int	Name of the source interface. Ex: src_int="port1"	string	16
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
dst_port	Destination port	uint16	5
dstip	Destination IP	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
event_id	Unique event ID	uint32	10
epoch	Epoch	uint32	10
session_id	Session ID. Ex: session_id=232	uint32	10
tz	Time zone	string	5
eventtime	Time when event occured	uint64	20
vd	Name of the virtual domain in which the log message was recorded.	string	32

Log Field Name	Description	Data Type	Length
devid	Serial number of the device for the traffic's origin.	string	16
level	Log Level	string	11
subtype	Subtype	string	20
type	Type of log. Ex: type="utm"	string	16
logid	Unique Log ID	string	10
time	Hour clock when the log message was recorded.	string	8
date	Day, month, and year when the log message was recorded.	string	10

WAF

30248 - LOGID_WAF_SIGNATURE_BLOCK

Message ID: 30248

Message Description: LOGID_WAF_SIGNATURE_BLOCK

Message Meaning: Web application firewall blocked application by signature

Type: WAF

Category: waf-signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30249 - LOGID_WAF_SIGNATURE_PASS

Message ID: 30249

Message Description: LOGID_WAF_SIGNATURE_PASS

Message Meaning: Web application firewall passed application by signature

Type: WAF

Category: waf-signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30250 - LOGID_WAF_SIGNATURE_ERASE

Message ID: 30250

Message Description: LOGID_WAF_SIGNATURE_ERASE

Message Meaning: Web application firewall erased application by signature

Type: WAF

Category: waf-signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30251 - LOGID_WAF_CUSTOM_SIGNATURE_BLOCK

Message ID: 30251

Message Description: LOGID_WAF_CUSTOM_SIGNATURE_BLOCK

Message Meaning: Web application firewall blocked application by custom signature

Type: WAF

Category: waf-custom-signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30252 - LOGID_WAF_CUSTOM_SIGNATURE_PASS

Message ID: 30252

Message Description: LOGID_WAF_CUSTOM_SIGNATURE_PASS

Message Meaning: Web application firewall allowed application by custom signature

Type: WAF

Category: waf-custom-signature

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30253 - LOGID_WAF_METHOD_BLOCK

Message ID: 30253

Message Description: LOGID_WAF_METHOD_BLOCK

Message Meaning: Web application firewall blocked application by HTTP method

Type: WAF

Category: waf-http-method

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30255 - LOGID_WAF_ADDRESS_LIST_BLOCK

Message ID: 30255

Message Description: LOGID_WAF_ADDRESS_LIST_BLOCK

Message Meaning: Web application firewall blocked application by address list

Type: WAF

Category: waf-address-list

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30257 - LOGID_WAF_CONSTRAINTS_BLOCK

Message ID: 30257

Message Description: LOGID_WAF_CONSTRAINTS_BLOCK

Message Meaning: Web application firewall blocked application by HTTP constraints

Type: WAF

Category: waf-http-constraint

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3

Log Field Name	Description	Data Type	Length
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30258 - LOGID_WAF_CONSTRAINTS_PASS

Message ID: 30258

Message Description: LOGID_WAF_CONSTRAINTS_PASS

Message Meaning: Web application firewall allowed application by HTTP constraints

Type: WAF

Category: waf-http-constraint

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64

Log Field Name	Description	Data Type	Length
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30259 - LOGID_WAF_URL_ACCESS_PERMIT

Message ID: 30259

Message Description: LOGID_WAF_URL_ACCESS_PERMIT

Message Meaning: Web application firewall allowed application by URL access permit

Type: WAF

Category: waf-url-access

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30260 - LOGID_WAF_URL_ACCESS_BYPASS

Message ID: 30260

Message Description: LOGID_WAF_URL_ACCESS_BYPASS

Message Meaning: Web application firewall allowed application by URL access bypass

Type: WAF

Category: waf-url-access

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20

Log Field Name	Description	Data Type	Length
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

30261 - LOGID_WAF_URL_ACCESS_BLOCK

Message ID: 30261

Message Description: LOGID_WAF_URL_ACCESS_BLOCK

Message Meaning: Web application firewall blocked application by URL access

Type: WAF

Category: waf-url-access

Severity: Warning

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
user	User Name	string	256
url	URL	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time zone	string	5
type	Log Type	string	16
time	Time	string	8
subtype	Log Subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP Address	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
severity	Severity	string	6
sessionid	Session ID	uint32	10
service	Service name	string	5
referralurl		string	512
rawdata	Raw Data	string	20480
ratemethod		string	4096
proto	Protocol	uint8	3
profile	Full profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
name	Method or custom signature name	string	64
msg	Log Message	string	4096
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
group	User Group Name	string	512
fctuid	FortiClient UID	string	32
eventtype	Event Type	string	32
eventtime	Event Time, Time when WAF event detected	uint64	20
eventid	Event ID	uint32	10
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP Address	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction	string	4096
devid	Device ID	string	16
date	Date	string	10
constraint	WAF HTTP protocol restrictions	string	4096
authserver	Authentication Server	string	64
agent	Agent	string	1024
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

Webfilter

12288 - LOG_ID_WEB_CONTENT_BANWORD

Message ID: 12288

Message Description: LOG_ID_WEB_CONTENT_BANWORD

Message Meaning: Web content banned word found

Type: Webfilter

Category: content

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	MMS-only - From/To headers from the email	string	128
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12290 - LOG_ID_WEB_CONTENT_EXEMPTWORD

Message ID: 12290

Message Description: LOG_ID_WEB_CONTENT_EXEMPTWORD

Message Meaning: Web content exempt word found

Type: Webfilter

Category: content

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512

Log Field Name	Description	Data Type	Length
from	MMS-only - From/To headers from the email	string	128
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12292 - LOG_ID_WEB_CONTENT_KEYWORD

Message ID: 12292

Message Description: LOG_ID_WEB_CONTENT_KEYWORD

Message Meaning: Message contained a key word in the profile list

Type: Webfilter

Category: content

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	MMS-only - From/To headers from the email	string	128
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12293 - LOG_ID_WEB_CONTENT_SEARCH

Message ID: 12293

Message Description: LOG_ID_WEB_CONTENT_SEARCH

Message Meaning: Search phrase detected

Type: Webfilter

Category: content

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8
subtype	Log subtype	string	20

Log Field Name	Description	Data Type	Length
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	MMS-only - From/To headers from the email	string	128

Log Field Name	Description	Data Type	Length
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12544 - LOG_ID_URL_FILTER_BLOCK

Message ID: 12544

Message Description: LOG_ID_URL_FILTER_BLOCK

Message Meaning: URL address was blocked because it was found in the URL filter list

Type: Webfilter

Category: urlfilter

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
urlfilterlist	URL filter list	string	64
urlfilteridx	URL filter ID	uint32	10
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10

Log Field Name	Description	Data Type	Length
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12545 - LOG_ID_URL_FILTER_EXEMPT

Message ID: 12545

Message Description: LOG_ID_URL_FILTER_EXEMPT

Message Meaning: URL address was exempted because it was found in the URL filter list

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
urlfilterlist	URL filter list	string	64
urlfilteridx	URL filter ID	uint32	10
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32

Log Field Name	Description	Data Type	Length
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12546 - LOG_ID_URL_FILTER_ALLOW

Message ID: 12546

Message Description: LOG_ID_URL_FILTER_ALLOW

Message Meaning: URL address was allowed because it was found in the URL filter list

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
urlfilterlist	URL filter list	string	64
urlfilteridx	URL filter ID	uint32	10
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64

Log Field Name	Description	Data Type	Length
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12547 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_BLK

Message ID: 12547

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_BLK

Message Meaning: The request contained an invalid domain name

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12548 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_BLK

Message ID: 12548

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_BLK

Message Meaning: HTTP certificate request contained an invalid domain name

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12549 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_PASS

Message ID: 12549

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_PASS

Message Meaning: HTTP request contained an invalid name so the session has been filtered by IP only

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12550 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_PASS

Message ID: 12550

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_PASS

Message Meaning: HTTPS request contained an invalid name so the session has been filtered by IP only

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12551 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_BLK

Message ID: 12551

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_BLK

Message Meaning: Insufficient resources

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12552 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_PASS

Message ID: 12552

Message Description: LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_PASS

Message Meaning: Getting the host name failed

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12553 - LOG_ID_URL_FILTER_INVALID_CERT

Message ID: 12553

Message Description: LOG_ID_URL_FILTER_INVALID_CERT

Message Meaning: Server certificate validation failed

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12554 - LOG_ID_URL_FILTER_INVALID_SESSION

Message ID: 12554

Message Description: LOG_ID_URL_FILTER_INVALID_SESSION

Message Meaning: SSL session blocked because its identification number was unknown

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256

Log Field Name	Description	Data Type	Length
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12555 - LOG_ID_URL_FILTER_SRV_CERT_ERR_BLK

Message ID: 12555

Message Description: LOG_ID_URL_FILTER_SRV_CERT_ERR_BLK

Message Meaning: SSL session blocked

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12556 - LOG_ID_URL_FILTER_SRV_CERT_ERR_PASS

Message ID: 12556

Message Description: LOG_ID_URL_FILTER_SRV_CERT_ERR_PASS

Message Meaning: SSL session ignored

Type: Webfilter

Category: urlfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512

Log Field Name	Description	Data Type	Length
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12557 - LOG_ID_URL_FILTER_FAMS_NOT_ACTIVE

Message ID: 12557

Message Description: LOG_ID_URL_FILTER_FAMS_NOT_ACTIVE

Message Meaning: The FortiGuard Analysis and Management Service is not active. You must enable this service

Type: Webfilter

Category: urlfilter

Severity: Critical

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
devid	Device ID	string	16
date	Date	string	10

12558 - LOG_ID_URL_FILTER_RATING_ERR

Message ID: 12558

Message Description: LOG_ID_URL_FILTER_RATING_ERR

Message Meaning: Rating error occurred

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
urltype	URL filter type	string	8
error	URL rating error message	string	256
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcdomain		string	255
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
hostname	The host name of a URL	string	256
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuser		string	256
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12559 - LOG_ID_URL_FILTER_PASS

Message ID: 12559

Message Description: LOG_ID_URL_FILTER_PASS

Message Meaning: URL passed because it was in the URL filter list

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
urlfilterlist	URL filter list	string	64
urlfilteridx	URL filter ID	uint32	10
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39

Log Field Name	Description	Data Type	Length
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512

Log Field Name	Description	Data Type	Length
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12560 - LOG_ID_URL_WISP_BLOCK

Message ID: 12560

Message Description: LOG_ID_URL_WISP_BLOCK

Message Meaning: URL blocked by Websense service

Type: Webfilter

Category: urlfilter

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12561 - LOG_ID_URL_WISP_REDIR

Message ID: 12561

Message Description: LOG_ID_URL_WISP_REDIR

Message Meaning: URL blocked with redirect message by Websense service

Type: Webfilter

Category: urlfilter

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512

Log Field Name	Description	Data Type	Length
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12562 - LOG_ID_URL_WISP_ALLOW

Message ID: 12562

Message Description: LOG_ID_URL_WISP_ALLOW

Message Meaning: URL allowed by Websense service

Type: Webfilter

Category: urlfilter

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12688 - LOG_ID_WEB_SSL_EXEMPT

Message ID: 12688

Message Description: LOG_ID_WEB_SSL_EXEMPT

Message Meaning: URL address was exempted because it was found in the ssl-exempt

Type: Webfilter

Category: ssl-exempt

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256

Log Field Name	Description	Data Type	Length
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10

Log Field Name	Description	Data Type	Length
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12800 - LOG_ID_WEB_FTGD_ERR

Message ID: 12800

Message Description: LOG_ID_WEB_FTGD_ERR

Message Meaning: Rating error occurred (error)

Type: Webfilter

Category: ftgd_err

Severity: Error

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
error	URL rating error message	string	256

Log Field Name	Description	Data Type	Length
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12801 - LOG_ID_WEB_FTGD_WARNING

Message ID: 12801

Message Description: LOG_ID_WEB_FTGD_WARNING

Message Meaning: Rating error occurred (warning)

Type: Webfilter

Category: ftgd_err

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
error	URL rating error message	string	256
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

12802 - LOG_ID_WEB_FTGD_QUOTA

Message ID: 12802

Message Description: LOG_ID_WEB_FTGD_QUOTA

Message Meaning: Daily FortiGuard quota status

Type: Webfilter

Category: ftgd_quota

Severity: Information

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
user	User name	string	256
tz	Time Zone	string	5
type	Log type	string	16
time	Time	string	8
subtype	Log subtype	string	20
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotaexceeded	Quota has been exceeded	string	3
profile	Web Filter profile name	string	64
logid	Log ID	string	10
level	Log Level	string	11
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuser		string	256
devid	Device ID	string	16
date	Date	string	10
catdesc	Web category description	string	64

13056 - LOG_ID_WEB_FTGD_CAT_BLK

Message ID: 13056

Message Description: LOG_ID_WEB_FTGD_CAT_BLK

Message Meaning: URL belongs to an blocked category within the firewall policy

Type: Webfilter

Category: ftgd_blk

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13057 - LOG_ID_WEB_FTGD_CAT_WARN

Message ID: 13057

Message Description: LOG_ID_WEB_FTGD_CAT_WARN

Message Meaning: URL belongs to a category with warnings enabled

Type: Webfilter

Category: ftgd_blk

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URl	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24

Log Field Name	Description	Data Type	Length
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13312 - LOG_ID_WEB_FTGD_CAT_ALLOW

Message ID: 13312

Message Description: LOG_ID_WEB_FTGD_CAT_ALLOW

Message Meaning: URL belongs to an allowed category within the firewall policy

Type: Webfilter

Category: ftgd_allow

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13315 - LOG_ID_WEB_FTGD_QUOTA_COUNTING

Message ID: 13315

Message Description: LOG_ID_WEB_FTGD_QUOTA_COUNTING

Message Meaning: FortiGuard web filter category quota counting log message

Type: Webfilter

Category: ftgd_quota_counting

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20

Log Field Name	Description	Data Type	Length
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13316 - LOG_ID_WEB_FTGD_QUOTA_EXPIRED

Message ID: 13316

Message Description: LOG_ID_WEB_FTGD_QUOTA_EXPIRED

Message Meaning: FortiGuard web filter category quota expired log message

Type: Webfilter

Category: ftgd_quota_expired

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13317 - LOG_ID_WEB_URL

Message ID: 13317

Message Description: LOG_ID_WEB_URL

Message Meaning: URL has been visited

Type: Webfilter

Category: urlmonitor

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
urlsource	URL source	string	64
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URl	string	512
rcvdbyte	Received Bytes	uint64	20

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13568 - LOG_ID_WEB_SCRIPTFILTER_ACTIVEX

Message ID: 13568

Message Description: LOG_ID_WEB_SCRIPTFILTER_ACTIVEX

Message Meaning: ActiveX script removed

Type: Webfilter

Category: activexfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13573 - LOG_ID_WEB_SCRIPTFILTER_COOKIE

Message ID: 13573

Message Description: LOG_ID_WEB_SCRIPTFILTER_COOKIE

Message Meaning: Cookie removed

Type: Webfilter

Category: cookiefilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64

Log Field Name	Description	Data Type	Length
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13584 - LOG_ID_WEB_SCRIPTFILTER_APPLET

Message ID: 13584

Message Description: LOG_ID_WEB_SCRIPTFILTER_APPLET

Message Meaning: Java applet removed

Type: Webfilter

Category: appletfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13600 - LOG_ID_WEB_SCRIPTFILTER_OTHER

Message ID: 13600

Message Description: LOG_ID_WEB_SCRIPTFILTER_OTHER

Message Meaning: Script entity removed

Type: Webfilter

Category: scriptfilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13601 - LOG_ID_WEB_WF_COOKIE

Message ID: 13601

Message Description: LOG_ID_WEB_WF_COOKIE

Message Meaning: Cookie removed entirely

Type: Webfilter

Category: cookiefilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13602 - LOG_ID_WEB_WF_REFERER

Message ID: 13602

Message Description: LOG_ID_WEB_WF_REFERER

Message Meaning: Referrer removed from request

Type: Webfilter

Category: cookiefilter

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
filtertype	Filter type	string	10
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20

Log Field Name	Description	Data Type	Length
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13603 - LOG_ID_WEB_WF_COMMAND_BLOCK

Message ID: 13603

Message Description: LOG_ID_WEB_WF_COMMAND_BLOCK

Message Meaning: Command blocked

Type: Webfilter

Category: webfilter_command_block

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32

Log Field Name	Description	Data Type	Length
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto		uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13616 - LOG_ID_CONTENT_TYPE_BLOCK

Message ID: 13616

Message Description: LOG_ID_CONTENT_TYPE_BLOCK

Message Meaning: Blocked by HTTP header content type

Type: Webfilter

Category: content

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URl	string	512
rcvdbyte	Received Bytes	uint64	20

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
from	MMS-only - From/To headers from the email	string	128
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13617 - LOG_ID_CONTENT_TYPE_EXEMPT

Message ID: 13617

Message Description: LOG_ID_CONTENT_TYPE_EXEMPT

Message Meaning: Exempted by HTTP header content type

Type: Webfilter

Category: content

Severity: Information

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39

Log Field Name	Description	Data Type	Length
to	MMS-only - From/To headers from the email	string	512
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
keyword	Keyword used for search	string	512
initiator	The initiator user for override	string	64
httpmethod		string	20

Log Field Name	Description	Data Type	Length
hostname	The host name of a URL	string	256
group	User group name	string	512
from	MMS-only - From/To headers from the email	string	128
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
contenttype	Content Type from HTTP header	string	64
banword	Banned word	string	128
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13632 - LOGID_HTTP_HDR_CHG_REQ

Message ID: 13632

Message Description: LOGID_HTTP_HDR_CHG_REQ

Message Meaning: Depends on info in msg field

Type: Webfilter

Category: http_header_change

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
tz	Time Zone	string	5
type	Log type	string	16
transid	Transaction ID	uint32	10
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
referralurl	Referrer URI	string	512
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User group name	string	512
eventtype	Web Filter event type	string	32

Log Field Name	Description	Data Type	Length
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
devid	Device ID	string	16
date	Date	string	10
chgheaders	Change headers	string	20480
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13633 - LOGID_HTTP_HDR_CHG_RESP

Message ID: 13633

Message Description: LOGID_HTTP_HDR_CHG_RESP

Message Meaning: Depends on info in msg field

Type: Webfilter

Category: http_header_change

Severity: Notice

Log Field Name	Description	Data Type	Length
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
type	Log type	string	16
transid	Transaction ID	uint32	10
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
referralurl	Referrer URI	string	512
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policyid	Policy ID	uint32	10
logid	Log ID	string	10
level	Log Level	string	11
httpmethod		string	20
group	User group name	string	512
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstcountry		string	64
dstauthserver		string	64
devid	Device ID	string	16
date	Date	string	10
chgheaders	Change headers	string	20480
authserver	Authentication server for the user	string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13648 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_ALLOW

Message ID: 13648

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_ALLOW

Message Meaning: Antiphishing matched a URL filter rule without blocking the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512

Log Field Name	Description	Data Type	Length
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13649 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_ALLOW

Message ID: 13649

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_ALLOW

Message Meaning: Antiphishing matched a Fortiguard category rule without blocking the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480

Log Field Name	Description	Data Type	Length
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13650 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_ALLOW

Message ID: 13650

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_ALLOW

Message Meaning: Antiphishing reached default action without blocking the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39

Log Field Name	Description	Data Type	Length
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256

Log Field Name	Description	Data Type	Length
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13651 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_BLOCK

Message ID: 13651

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_BLOCK

Message Meaning: Antiphishing matched a URL filter rule and blocked the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13652 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_BLOCK

Message ID: 13652

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_BLOCK

Message Meaning: Antiphishing matched a Fortiguard category rule and blocked the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13653 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_BLOCK

Message ID: 13653

Message Description: LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_BLOCK

Message Meaning: Antiphishing reached default action and blocked the request.

Type: Webfilter

Category: antiphishing

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf	Virtual router forwarding	uint8	3
vd	Virtual domain name	string	32
user	User name	string	256
url	The URL address	string	512
unauthusersource	Unauthenticated user source	string	66
unauthuser	Unauthenticated user	string	66
tz	Time Zone	string	5
type	Log type	string	16
trueclntip	True-Client-IP HTTP header	ip	39
time	Time	string	8
subtype	Log subtype	string	20
srcuuid		string	37
srcport	Source Port	uint16	5
srcip	Source IP	ip	39
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcintf	Source Interface	string	32
srcdomain		string	255
srccountry		string	64
sessionid	Session ID	uint32	10
service	Service name	string	36
sentbyte	Sent Bytes	uint64	20
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
referralurl	Referrer URI	string	512
rcvdbyte	Received Bytes	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	20480
ratemethod		string	6
proto	Protocol number	uint8	3
profile	Web Filter profile name	string	64
poluuid		string	37
policytype		string	24
policymode		string	8
policyid	Policy ID	uint32	10
msg	Log message	string	512
logid	Log ID	string	10
level	Log Level	string	11
initiator	The initiator user for override	string	64
httpmethod		string	20
hostname	The host name of a URL	string	256
group	User group name	string	512
forwardedfor	X-Forwarded-For HTTP header	string	128
fctuid	FortiClient UID	string	32
eventtype	Web Filter event type	string	32
eventtime	Web Filter event time	uint64	20
dstuuid		string	37
dstuser		string	256
dstport	Destination Port	uint16	5
dstip	Destination IP	ip	39
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstintf	Destination Interface	string	32
dstcountry		string	64
dstauthserver		string	64

Log Field Name	Description	Data Type	Length
direction	Direction of the web traffic	string	8
devid	Device ID	string	16
date	Date	string	10
crscore	Client Reputation Score	uint32	10
crlevel	Client Reputation level	string	10
craction	Client Reputation Action	uint32	10
catdesc	Web category description	string	64
cat	Web category ID	uint8	3
authserver	Authentication server for the user	string	64
antiphishrule		string	64
antiphishdc		string	64
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

13664 - LOG_ID_VIDEOFILTER_CATEGORY_BLOCK

Message ID: 13664

Message Description: LOG_ID_VIDEOFILTER_CATEGORY_BLOCK

Message Meaning: Video category is blocked.

Type: Webfilter

Category: videofilter-category

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512

Log Field Name	Description	Data Type	Length
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256

Log Field Name	Description	Data Type	Length
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13665 - LOG_ID_VIDEOFILTER_CATEGORY_MONITOR

Message ID: 13665

Message Description: LOG_ID_VIDEOFILTER_CATEGORY_MONITOR

Message Meaning: Video category is monitored

Type: Webfilter

Category: videofilter-category

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16

Log Field Name	Description	Data Type	Length
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13666 - LOG_ID_VIDEOFILTER_CATEGORY_ALLOW

Message ID: 13666

Message Description: LOG_ID_VIDEOFILTER_CATEGORY_ALLOW

Message Meaning: Video category is allowed

Type: Webfilter

Category: videofilter-category

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13680 - LOG_ID_VIDEOFILTER_CHANNEL_BLOCK

Message ID: 13680

Message Description: LOG_ID_VIDEOFILTER_CHANNEL_BLOCK

Message Meaning: Video channel is blocked.

Type: Webfilter

Category: videofilter-channel

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13681 - LOG_ID_VIDEOFILTER_CHANNEL_MONITOR

Message ID: 13681

Message Description: LOG_ID_VIDEOFILTER_CHANNEL_MONITOR

Message Meaning: Video channel is monitored

Type: Webfilter

Category: videofilter-channel

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256

Log Field Name	Description	Data Type	Length
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13682 - LOG_ID_VIDEOFILTER_CHANNEL_ALLOW

Message ID: 13682

Message Description: LOG_ID_VIDEOFILTER_CHANNEL_ALLOW

Message Meaning: Video channel is allowed

Type: Webfilter

Category: videofilter-channel

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8

Log Field Name	Description	Data Type	Length
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13712 - LOG_ID_VIDEOFILTER_TITLE_BLOCK

Message ID: 13712

Message Description: LOG_ID_VIDEOFILTER_TITLE_BLOCK

Message Meaning: Video title is blocked.

Type: Webfilter

Category: videofilter-title

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13713 - LOG_ID_VIDEOFILTER_TITLE_MONITOR

Message ID: 13713

Message Description: LOG_ID_VIDEOFILTER_TITLE_MONITOR

Message Meaning: Video title is monitored

Type: Webfilter

Category: videofilter-title

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13714 - LOG_ID_VIDEOFILTER_TITLE_ALLOW

Message ID: 13714

Message Description: LOG_ID_VIDEOFILTER_TITLE_ALLOW

Message Meaning: Video title is allowed

Type: Webfilter

Category: videofilter-title

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256

Log Field Name	Description	Data Type	Length
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13728 - LOG_ID_VIDEOFILTER_DESCRIPTION_BLOCK

Message ID: 13728

Message Description: LOG_ID_VIDEOFILTER_DESCRIPTION_BLOCK

Message Meaning: Video description is blocked.

Type: Webfilter

Category: videofilter-description

Severity: Warning

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8

Log Field Name	Description	Data Type	Length
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13729 - LOG_ID_VIDEOFILTER_DESCRIPTION_MONITOR

Message ID: 13729

Message Description: LOG_ID_VIDEOFILTER_DESCRIPTION_MONITOR

Message Meaning: Video description is monitored

Type: Webfilter

Category: videofilter-description

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3

Log Field Name	Description	Data Type	Length
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

13730 - LOG_ID_VIDEOFILTER_DESCRIPTION_ALLOW

Message ID: 13730

Message Description: LOG_ID_VIDEOFILTER_DESCRIPTION_ALLOW

Message Meaning: Video description is allowed

Type: Webfilter

Category: videofilter-description

Severity: Notice

Log Field Name	Description	Data Type	Length
vrf		uint8	3
videotitle		string	512
videoinfosource		string	10
videoid		string	512
videodesc		string	64
videochannelid		string	512
videocategoryname		string	256
videocategoryid		uint32	10
vd		string	32
user		string	256
url		string	512
tz		string	5
type		string	16
time		string	8
subtype		string	20
srcport		uint16	5
srcip		ip	39
srcintfrole		string	10
srcintf		string	32
sessionid		uint32	10
service		string	36
referralurl	Referrer URI	string	512
proto		uint8	3
profile		string	64
poluuid		string	37
policytype		string	24
policyid		uint32	10
msg		string	512
logid		string	10
level		string	11

Log Field Name	Description	Data Type	Length
httpmethod		string	20
hostname		string	256
group		string	512
eventtype		string	32
eventtime		uint64	20
dstuser		string	256
dstport		uint16	5
dstip		ip	39
dstintfrole		string	10
dstintf		string	32
devid		string	16
date		string	10
agent	User agent - eg. agent="Mozilla/5.0"	string	1024
action		string	11

FORTINET®

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.