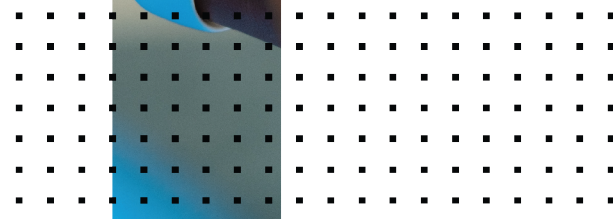
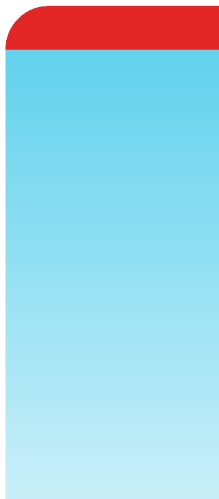


Log Reference

FortiClient 7.0.11



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



January 31, 2024

FortiClient 7.0.11 Log Reference

04-7011-739392-20240131

TABLE OF CONTENTS

Change log	4
Introduction	5
Windows	6
Mandatory fields	6
Log fields by type	7
securityevent	7
systemevent	10
traffic	12
Log message by type	13
securityevent > antiexploit	13
securityevent > antiransomware	14
securityevent > applicationcontrol	15
securityevent > av	15
securityevent > cloudscan	18
securityevent > firewall	18
securityevent > fsso	18
securityevent > ipsecvpn	19
securityevent > removablemediaaccess	23
securityevent > sandboxing	23
securityevent > sslvpn	24
securityevent > vulnerabilityscan	26
securityevent > webfilter	28
systemevent > endpoint	28
systemevent > system	30
systemevent > update	32
traffic > system	33
Linux	35
Mandatory fields	35
Log fields by type	36
securityevent	36
systemevent	38
Log message by type	39
securityevent > av	39
securityevent > vulnerabilityscan	40
systemevent > endpoint	41

Change log

Date	Change Description
2024-01-31	Initial release.

Introduction

This document provides information about all the log messages applicable to FortiClient 7.0.11. The logs are intended for administrators to use as reference for more information about a specific log entry and message that FortiClient generated.

FortiClient has three log types: security event, system event, and traffic. This document contains the following information:

- [Windows on page 6](#): fields that apply to FortiClient (Windows) logs
- [Linux on page 35](#): fields that apply to FortiClient (Linux) logs

Windows

This section contains the following information for FortiClient (Windows):

- [Mandatory fields on page 6](#): fields that are mandatory to all FortiClient (Windows) logs.
- [Log fields by type on page 7](#): fields that only apply to security event logs.
- [Log message by type on page 13](#): lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
site	Multi-tenancy site	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
action	action taken for the infected item	enumeration string	32
activity	activity	enumeration string	64
ae_api	API used of the violation	string	64
ae_reason	reason of the violation	string	64
app	application	string	96
cat	category id	int	20
category	category name	string	260
checksum	file crc32 checksum	int	20
checksum	file SHA256 checksum	string	16
date	date	string	260
default_used	if process is handled by default action	int	20
description	description	string	260
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
detectedpath	detected path(s)	string	260
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
devid	device ID	string	16

Log Field Name	Description	Data Type	Length
domain	domain of user	string	256
emsserial	EMS serial number	string	16
error_code	reason of the failure	int	20
eventtype	type of event	enumeration string	32
failed_reason	reason of the failure	string	260
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
file	file location	string	256
filesize	file size	int	20
from	email from	string	128
hostname	host name of local machine	string	256
id	log id	int	20
ip	IP address	string	260
level	log level	enumeration string	20
locip	local ip	string	20
locport	local port	int	20
logver	log protocol version	int	20
msg	description of this log	string	512
os	operating system	string	96
path	path of process	string	260
payload_process	payload process	string	260
pcdomain	domain name of local machine	string	128
processname	process name	string	128
remip	remote ip	string	20
remotegw	remote gateway	string	256
remport	remote port	int	20
ruleuuid	uuid of violated rule	string	260
score	file score	int	20
service	network protocol	string	64

Log Field Name	Description	Data Type	Length
sigid	signature id	string	260
site	Multi-tenancy site	string	32
status	scan status	string	16
status	status	enumeration string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
time	time	string	260
to	email to	string	512
type	Traffic, Security Event or System Event	string	16
uid	FortiClient unique ID	string	32
user	current logged on user	string	256
username	username of process	string	260
usingpolicy	current policy name	string	64
vid	virus id	int	20
virus	virus name	string	512
viruscat	virus category	string	260
vpn	vpn tunnel name	string	32
vpnstate	tunnel status	enumeration string	64
vpntunnel	tunnel name	string	128
vpnuser	vpn tunnel user name	string	128
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnengine	engine version	string	64
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnproducts	name of the vulnerable product	string	2048
vulnref	reference of the vulnerability	string	256
vulnseverity	severity level	string	8
vulnsignature	signature version	string	260

systemevent

Log Field Name	Description	Data Type	Length
appengine	app DB engine	string	260
apppath	process name	string	128
appsig	app DB signature	string	11
avaleng	AV allowlist engine version	string	260
avalsig	AV allowlist signatures version	string	260
avengine	AV engine	string	11
avsig	AV signature	string	11
avsigetm	AV extreme signature	string	11
avsigext	AV extended signature	string	11
avsigheu	AV heuristic signature	string	11
avsiglastupdate	last update time	string	260
avsigpallas	AV pallas signature	string	260
date	date	string	260
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
devid	device ID	string	16
emshostname	EMS host name	string	64
emsip	EMS IP	string	20
emsserial	EMS serial number	string	16
epenfeatures	enabled features list	string	128
epfeatures	installed features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
epmgmtst	management status	enumeration string	64
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
epquarmsg	quarant message	string	260

Log Field Name	Description	Data Type	Length
eventtype	type of event	enumeration string	32
fctip	FCT IP	string	20
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
file	file or registry path	string	256
hostname	host name of local machine	string	256
id	log id	int	20
ipseng	firewall engine	string	11
ipssig	firewall signature	string	11
irdbsig	irdb signature	string	260
level	log level	enumeration string	20
logver	log protocol version	int	20
msg	description of this log	string	512
os	operating system	string	96
pcdomain	domain name of local machine	string	128
polycname	policy name	string	64
processname	blocked process	string	128
rootkitengine	anti-rootkit engine	string	11
rootkitsig	anti-rootkit signature	string	11
site	Multi-tenancy site	string	32
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
status	status description	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
time	time	string	260
type	Traffic, Security Event or System Event	string	16

Log Field Name	Description	Data Type	Length
uid	FortiClient unique ID	string	32
user	current logged on user	string	256
usingpolicy	current policy name	string	64
vulnengine	vulnerability engine	string	64
vulnsig	vulnerability signature	string	11

traffic

Log Field Name	Description	Data Type	Length
browsetime	user browsing time of web page(in seconds)	int	20
date	date	string	260
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
devid	device ID	string	16
direction	traffic direction	string	8
dstip	destination IP	string	20
dstport	destination port	int	20
emsserial	EMS serial number	string	16
eventtype	type of event	enumeration string	32
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
hostname	host name of local machine	string	256
id	log id	int	20
level	log level	enumeration string	20
logver	log protocol version	int	20
msg	description of this log	string	512
os	operating system	string	96
pcdomain	domain name of local machine	string	128
proto	network protocol	int	20
rcvdbyte	data received (in bytes)	int	20

Log Field Name	Description	Data Type	Length
regip	regip	string	64
remotename	remote name	string	256
sentbyte	data sent (in bytes)	int	20
service	network protocol	string	64
sessionid	network session	string	64
site	Multi-tenancy site	string	32
srcip	source IP	string	20
srcname	source name	string	256
srcport	source port	int	20
srcproduct	source product	string	256
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
threat	threat	string	128
time	time	string	260
type	Traffic, Security Event or System Event	string	16
uid	FortiClient unique ID	string	32
url	url	string	512
user	current logged on user	string	256
userinitiated	if user initiated url request	int	20
usingpolicy	current policy name	string	64
utmaction	utm action	string	32
utmevent	utm event	string	32

Log message by type

securityevent > antiexploit

Log ID	Level	Sub Type	Event Type	Message
96548	warning	antiexploit	action	AntiExpoit has detected violation

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				action	action taken for violation	enumeration string
				ae_api	API used of the violation	string
				ae_reason	reason of the violation	string
				app	application	string
				payload_process	payload process	string

securityevent > antiransomware

Log ID	Level	Sub Type	Event Type	Message															
98000	warning	antiransomware	status	AntiRansomware has found a suspicious process															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>action</td><td>file action (1 = kill 2 = resume)</td><td>enumeration string</td></tr><tr><td>default_used</td><td>if process is handled by default action</td><td>int</td></tr><tr><td>checksum</td><td>file SHA256 checksum</td><td>string</td></tr></table>	Field	Field Description	Field Type	file	file location	string	action	file action (1 = kill 2 = resume)	enumeration string	default_used	if process is handled by default action	int	checksum	file SHA256 checksum	string
Field	Field Description	Field Type																	
file	file location	string																	
action	file action (1 = kill 2 = resume)	enumeration string																	
default_used	if process is handled by default action	int																	
checksum	file SHA256 checksum	string																	
98001	warning	antiransomware	status	AntiRansomware has recovered a file															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>file</td><td>file location</td><td>string</td></tr></table>	Field	Field Description	Field Type	file	file location	string									
Field	Field Description	Field Type																	
file	file location	string																	
98002	warning	antiransomware	status	AntiRansomware has quarantined a file															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>checksum</td><td>file SHA256 checksum</td><td>string</td></tr></table>	Field	Field Description	Field Type	file	file location	string	checksum	file SHA256 checksum	string						
Field	Field Description	Field Type																	
file	file location	string																	
checksum	file SHA256 checksum	string																	
98003	info	antiransomware	status	AntiRansomware has completed the quarantine and restoration of relevant files															

securityevent > applicationcontrol

Log ID	Level	Sub Type	Event Type	Message		
96701	warning	applicationcontrol	error	Application Control found a rule violation		
				Field	Field Description	Field Type
				path	path of process	string
				username	username of process	string
				domain	domain of user	string
				ruleuuid	uuid of violated rule	string
				action	block or monitor	string

securityevent > av

Log ID	Level	Sub Type	Event Type	Message		
96530	warning	av	action	Found virus		
				Field	Field Description	Field Type
				action	action taken for the infected item	enumeration string
				file	file location	string
				virus	virus name	string
				viruscat	virus category	string
				sigid	signature id	string
				vid	virus id	int
				from	email from	string
				to	email to	string
				service	network protocol	string
				vpn	vpn tunnel name	string
				filesize	file size	int
				checksum	file crc32 checksum	int

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				detectedby	the security feature that detected virus	enumeration string
				detectedin	where the virus is detected	enumeration string
96531	warning	av	action	Found malware		
				Field	Field Description	Field Type
				action	action taken for the infected item	enumeration string
				file	file location	string
				virus	virus name	string
				sigid	signature id	string
				filesize	file size	int
				checksum	file crc32 checksum	int
				detectedby	the security feature that detected virus	enumeration string
				detectedin	where the virus is detected	enumeration string
96534	warning	av	status	User disabled Realtime AntiVirus protection		
96535	info	av	error	Communication error with other modules		
96536	warning	av	action	AntiVirus realtime protection killed malware process		
				Field	Field Description	Field Type
				processname	process name	string
				detectedby	the security feature that detected virus	enumeration string
96537	info	av	status	av_task scan thread is suspended		
96538	info	av	status	av_task scan thread is resumed		
96540	info	av	error	Cannot start scan task, license expired		
96541	info	av	status	av_task scan is started		
96542	info	av	status	av_task scan is stopped		

Log ID	Level	Sub Type	Event Type	Message		
96543	error	av	error	Scheduled scan failed: Path to file/folder no longer exists		
				Field	Field Description	Field Type
				file	file or directory does not exist	string
96550	error	av	error	Failed to restore quarantined file		
				Field	Field Description	Field Type
				action	action taken for the infected item	enumeration string
				file	file location	string
				virus	virus name	string
				sigid	signature id	string
				filesize	file size	int
				checksum	file crc32 checksum	int
				detectedby	the security feature that detected virus	enumeration string
96551	info	av	action	A quarantined file was restored		
				Field	Field Description	Field Type
				action	action taken for the infected item	enumeration string
				file	file location	string
				virus	virus name	string
				sigid	signature id	string
				filesize	file size	int
				checksum	file crc32 checksum	int
				detectedby	the security feature that detected virus	enumeration string

securityevent > cloudscan

Log ID	Level	Sub Type	Event Type	Message		
97100	debug	cloudscan	status	file score received		
				Field	Field Description	Field Type
				file	file location	string
				score	file score	int
				checksum	file SHA256 checksum	string

securityevent > firewall

Log ID	Level	Sub Type	Event Type	Message
96645	warning	firewall	error	The application firewall has been disabled because it's driver could not be loaded

securityevent > fsso

Log ID	Level	Sub Type	Event Type	Message		
96980	info	fsso	status	Single Sign-On event		
				Field	Field Description	Field Type
				action	action	enumeration string
				domain	domain name	string
				remotegw	remote gateway	string
96983	info	fsso	status	Single Sign-On Mobility Agent is starting		
96984	info	fsso	status	Single Sign-On Mobility Agent is stopping		

securityevent > ipsecvpn

Log ID	Level	Sub Type	Event Type	Message		
96560	info	ipsecvpn	status	VPN tunnel status		
				Field	Field Description	Field Type
				vpnstate	tunnel status	enumeration string
				vpntunnel	tunnel name	string
				vpnuser	vpn tunnel user name	string
				remotegw	remote gateway	string
				locip	local ip	string
				locport	local port	int
				remip	remote ip	string
				remport	remote port	int
96561	warning	ipsecvpn	error	No response from the peer, phase1 retransmit reaches maximum count		
				Field	Field Description	Field Type
				vpntunnel	tunnel name	string
				locip	local ip	string
				locport	local port	int
				remip	remote ip	string
				remport	remote port	int
96562	warning	ipsecvpn	error	No response from the peer, phase2 retransmit reaches maximum count		
				Field	Field Description	Field Type
				vpntunnel	tunnel name	string
				locip	local ip	string
				locport	local port	int
				remip	remote ip	string
				remport	remote port	int

Log ID	Level	Sub Type	Event Type	Message																		
96563	warning	ipsecvpn	status	Received delete payload from peer check xauth password																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
locip	local ip	string																				
locport	local port	int																				
remip	remote ip	string																				
remport	remote port	int																				
96564	error	ipsecvpn	error	Failed to acquire an IP address for the virtual adapter																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
locip	local ip	string																				
locport	local port	int																				
remip	remote ip	string																				
remport	remote port	int																				
96565	error	ipsecvpn	error	General error of IKE																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
locip	local ip	string																				
locport	local port	int																				
remip	remote ip	string																				
remport	remote port	int																				
96566	info	ipsecvpn	status	negotiation information																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
96567	error	ipsecvpn	error	negotiation error																		

Log ID	Level	Sub Type	Event Type	Message																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
				Field	Field Description	Field Type																
vpntunnel	tunnel name	string																				
96568	error	ipsecvpn	status	replayed packet detected (packet dropped)																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
				Field	Field Description	Field Type																
vpntunnel	tunnel name	string																				
96569	info	ipsecvpn	status	The VPN user accept the banner warning																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
				Field	Field Description	Field Type																
				vpntunnel	tunnel name	string																
				locip	local ip	string																
				locport	local port	int																
				remip	remote ip	string																
remport	remote port	int																				
96570	info	ipsecvpn	status	The VPN user reject the banner warning and disconnect the tunnel																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
				Field	Field Description	Field Type																
				vpntunnel	tunnel name	string																
				locip	local ip	string																
				locport	local port	int																
				remip	remote ip	string																
remport	remote port	int																				
96571	info	ipsecvpn	status	Send sa to the IPsec driver																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int						
				Field	Field Description	Field Type																
				vpntunnel	tunnel name	string																
				locip	local ip	string																
locport	local port	int																				

Log ID	Level	Sub Type	Event Type	Message																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	remip	remote ip	string	remport	remote port	int									
				Field	Field Description	Field Type																
				remip	remote ip	string																
remport	remote port	int																				
96574	error	ipsecvpn	error	Logged when a VPN authorization rule failed																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
				Field	Field Description	Field Type																
vpntunnel	tunnel name	string																				
96575	warning	ipsecvpn	error	VPN cannot connect because the specified application is not running																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>app</td><td>application</td><td>string</td></tr></table>	Field	Field Description	Field Type	app	application	string												
				Field	Field Description	Field Type																
app	application	string																				
96576	info	ipsecvpn	error	IKE phase1 authentication fail as peer's certificate is not verified																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
				Field	Field Description	Field Type																
				vpntunnel	tunnel name	string																
				locip	local ip	string																
				locport	local port	int																
				remip	remote ip	string																
remport	remote port	int																				
96577	info	ipsecvpn	error	IKE phase1 authentication fail as peer's certificate is not verified																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>locip</td><td>local ip</td><td>string</td></tr><tr><td>locport</td><td>local port</td><td>int</td></tr><tr><td>remip</td><td>remote ip</td><td>string</td></tr><tr><td>remport</td><td>remote port</td><td>int</td></tr></table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int
				Field	Field Description	Field Type																
				vpntunnel	tunnel name	string																
				locip	local ip	string																
				locport	local port	int																
				remip	remote ip	string																
remport	remote port	int																				

securityevent > removablemediaaccess

Log ID	Level	Sub Type	Event Type	Message		
96620	info	removablemediaaccess	status	usb storage activity		
				Field	Field Description	Field Type
				action	action	enumeration string
				activity	activity	enumeration string
				description	description	string

securityevent > sandboxing

Log ID	Level	Sub Type	Event Type	Message		
96545	debug	sandboxing	error	Failed to connect to FortiSandbox server		
				Field	Field Description	Field Type
				failed_reason	reason of the failure	string
96556	warning	sandboxing	error	Failed to submit file to FortiSandbox server		
				Field	Field Description	Field Type
				file	file location	string
				error_code	reason of the failure	int
96557	warning	sandboxing	error	Failed to query checksum to FortiSandbox server		
				Field	Field Description	Field Type
				file	file location	string
				error_code	reason of the failure	int

Log ID	Level	Sub Type	Event Type	Message																											
96546	warning	sandboxing	action	Found virus																											
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>action</td><td>action taken for the infected item</td><td>enumeration string</td></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>virus</td><td>virus name</td><td>string</td></tr><tr><td>sigid</td><td>signature id</td><td>string</td></tr><tr><td>filesize</td><td>file size</td><td>int</td></tr><tr><td>checksum</td><td>file crc32 checksum</td><td>int</td></tr><tr><td>detectedby</td><td>the security feature that detected virus</td><td>enumeration string</td></tr><tr><td>detectedin</td><td>where the virus is detected</td><td>enumeration string</td></tr></table>	Field	Field Description	Field Type	action	action taken for the infected item	enumeration string	file	file location	string	virus	virus name	string	sigid	signature id	string	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string
Field	Field Description	Field Type																													
action	action taken for the infected item	enumeration string																													
file	file location	string																													
virus	virus name	string																													
sigid	signature id	string																													
filesize	file size	int																													
checksum	file crc32 checksum	int																													
detectedby	the security feature that detected virus	enumeration string																													
detectedin	where the virus is detected	enumeration string																													
96547	info	sandboxing	error	Sandbox is not authorized																											
96554	info	sandboxing	status	file is submitted to Sandbox service																											
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>checksum</td><td>file SHA256 checksum</td><td>string</td></tr></table>	Field	Field Description	Field Type	file	file location	string	checksum	file SHA256 checksum	string																		
Field	Field Description	Field Type																													
file	file location	string																													
checksum	file SHA256 checksum	string																													
96555	debug	sandboxing	status	file score received																											
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>score</td><td>file score</td><td>int</td></tr><tr><td>checksum</td><td>file SHA256 checksum</td><td>string</td></tr></table>	Field	Field Description	Field Type	file	file location	string	score	file score	int	checksum	file SHA256 checksum	string															
Field	Field Description	Field Type																													
file	file location	string																													
score	file score	int																													
checksum	file SHA256 checksum	string																													

securityevent > sslvpn

Log ID	Level	Sub Type	Event Type	Message
96600	info	sslvpn	status	SSLVPN tunnel status

Log ID	Level	Sub Type	Event Type	Message															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpnstate</td><td>tunnel status</td><td>enumeration string</td></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string						
				Field	Field Description	Field Type													
				vpnstate	tunnel status	enumeration string													
				vpntunnel	tunnel name	string													
96601	error	sslvpn	error	Telephony service (TapiSrv) is not running															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpnstate</td><td>tunnel status</td><td>enumeration string</td></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>vpnuser</td><td>tunnel user name</td><td>string</td></tr><tr><td>remotegw</td><td>remote gateway</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string	vpnuser	tunnel user name	string	remotegw	remote gateway	string
				Field	Field Description	Field Type													
				vpnstate	tunnel status	enumeration string													
				vpntunnel	tunnel name	string													
				vpnuser	tunnel user name	string													
remotegw	remote gateway	string																	
96602	info	sslvpn	status	SSLVPN service started successfully															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpnstate</td><td>tunnel status</td><td>enumeration string</td></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>vpnuser</td><td>tunnel user name</td><td>string</td></tr><tr><td>remotegw</td><td>remote gateway</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string	vpnuser	tunnel user name	string	remotegw	remote gateway	string
				Field	Field Description	Field Type													
				vpnstate	tunnel status	enumeration string													
				vpntunnel	tunnel name	string													
				vpnuser	tunnel user name	string													
				remotegw	remote gateway	string													
96603	error	sslvpn	error	SSLVPN tunnel connection failed															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpnstate</td><td>tunnel status</td><td>enumeration string</td></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr><tr><td>vpnuser</td><td>tunnel user name</td><td>string</td></tr><tr><td>remotegw</td><td>remote gateway</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string	vpnuser	tunnel user name	string	remotegw	remote gateway	string
				Field	Field Description	Field Type													
				vpnstate	tunnel status	enumeration string													
				vpntunnel	tunnel name	string													
				vpnuser	tunnel user name	string													
remotegw	remote gateway	string																	
96605	warning	sslvpn	error	SSLVPN cannot connect because the specified application is not running															

Log ID	Level	Sub Type	Event Type	Message									
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>app</td><td>application</td><td>string</td></tr></table>	Field	Field Description	Field Type	app	application	string			
				Field	Field Description	Field Type							
app	application	string											
96610	info	sslvpn	status	SSLVPN(DTLS) tunnel status									
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>vpnstate</td><td>tunnel status</td><td>enumeration string</td></tr><tr><td>vpntunnel</td><td>tunnel name</td><td>string</td></tr></table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string
				Field	Field Description	Field Type							
				vpnstate	tunnel status	enumeration string							
vpntunnel	tunnel name	string											

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message		
96520	info	vulnerabilityscan	status	The vulnerability scan status has changed		
				Field	Field Description	Field Type
				status	scan status	string
96521	warning	vulnerabilityscan	status	A vulnerability scan result has been logged		
				Field	Field Description	Field Type
				vulnid	id of the vulnerability	int
				vulnname	name of the vulnerability	string
				vulnseverity	severity level	string
				vulncat	category	string
				vulncvss	cvss score	string
				vulnref	reference of the vulnerability	string
				vulnengine	engine version	string
				vulnsignature	signature version	string
				vulnproducts	name of the vulnerable product	string

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				detectedpath	detected path(s)	string
96522	info	vulnerabilityscan	action	Applying patch for vulnerability found		
				Field	Field Description	Field Type
				vulnid	id of the vulnerability	int
				vulnname	name of the vulnerability	string
				vulnseverity	severity level	string
				vulncat	category	string
				vulncvss	cvss score	string
				vulnref	reference of the vulnerability	string
				vulnengine	engine version	string
				vulnsignature	signature version	string
				vulnproducts	name of the vulnerable product	string
96523	info	vulnerabilityscan	action	Applying patch for Windows vulnerability		
				Field	Field Description	Field Type
				vulnid	id of the vulnerability	int
				vulnname	name of the vulnerability	string
				vulnseverity	severity level	string
				vulncat	category	string
				vulncvss	cvss score	string
				vulnref	reference of the vulnerability	string
				vulnengine	engine version	string
				vulnsignature	signature version	string
				vulnproducts	name of the vulnerable product	string

securityevent > webfilter

Log ID	Level	Sub Type	Event Type	Message		
96500	info	webfilter	status	User enabled Webfilter		
96501	warning	webfilter	status	User disabled Webfilter		
96502	warning	webfilter	action	user's access to the url is blocked		
				Field	Field Description	Field Type
				cat	category id	int
				category	category name	string
				service	network protocol	string
				ip	IP address	string
				status	status	enumeration string
96503	info	webfilter	action	user's access to the url is bypassed		
				Field	Field Description	Field Type
				cat	category id	int
				category	category name	string
				service	network protocol	string
				ip	IP address	string
				status	status	enumeration string

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message		
96953	info	endpoint	status	Endpoint Control Status Changed		
				Field	Field Description	Field Type
				eponlinest	online status	enumeration string
				epplace	EP place	enumeration string

Log ID	Level	Sub Type	Event Type	Message																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr><tr><td>status</td><td>status description</td><td>string</td></tr></table>	Field	Field Description	Field Type	emshostname	EMS host name	string	status	status description	string									
				Field	Field Description	Field Type																
				emshostname	EMS host name	string																
				status	status description	string																
96955	info	endpoint	status	Endpoint Control Registration Status Changed																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr><tr><td>status</td><td>status description</td><td>string</td></tr><tr><td>emsip</td><td>EMS IP</td><td>string</td></tr><tr><td>fctip</td><td>FCT IP</td><td>string</td></tr></table>	Field	Field Description	Field Type	emshostname	EMS host name	string	status	status description	string	emsip	EMS IP	string	fctip	FCT IP	string			
				Field	Field Description	Field Type																
				emshostname	EMS host name	string																
				status	status description	string																
				emsip	EMS IP	string																
				fctip	FCT IP	string																
96956	info	endpoint	status	Endpoint Quarantine Status Changed																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>epmgmtst</td><td>management status</td><td>enumeration string</td></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr><tr><td>epquarmsg</td><td>quarant message</td><td>string</td></tr></table>	Field	Field Description	Field Type	epmgmtst	management status	enumeration string	emshostname	EMS host name	string	epquarmsg	quarant message	string						
				Field	Field Description	Field Type																
				epmgmtst	management status	enumeration string																
				emshostname	EMS host name	string																
epquarmsg	quarant message	string																				
96957	info	endpoint	status	Endpoint Ext Log to FAZ																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>epfeatures</td><td>installed features list</td><td>string</td></tr><tr><td>epenfeatures</td><td>enabled features list</td><td>string</td></tr><tr><td>ephbemsduration</td><td>EMS heart beat duration</td><td>int</td></tr><tr><td>ephbemslast</td><td>EMS heart beat last time</td><td>string</td></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr></table>	Field	Field Description	Field Type	epfeatures	installed features list	string	epenfeatures	enabled features list	string	ephbemsduration	EMS heart beat duration	int	ephbemslast	EMS heart beat last time	string	emshostname	EMS host name	string
				Field	Field Description	Field Type																
				epfeatures	installed features list	string																
				epenfeatures	enabled features list	string																
				ephbemsduration	EMS heart beat duration	int																
				ephbemslast	EMS heart beat last time	string																
emshostname	EMS host name	string																				
96958	info	endpoint	status	User social media information																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>social_ srvc</td><td>social service</td><td>string</td></tr></table>	Field	Field Description	Field Type	social_ srvc	social service	string												
				Field	Field Description	Field Type																
social_ srvc	social service	string																				

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				social_user	social user name	string
				social_email	social email	string
				social_phone	social phone number	string
96959	info	endpoint	status	Current AV allowlist engine/signatures this endpoint is using		
				Field	Field Description	Field Type
				emshostname	EMS host name	string
				avaleng	AV allowlist engine version	string
				avalsig	AV allowlist signatures version	string

systemevent > system

Log ID	Level	Sub Type	Event Type	Message		
96800	info	system	error	Forcefully kill a child process after grace period expires		
				Field	Field Description	Field Type
				apppath	process name	string
96801	error	system	error	The scheduler cannot start the scheduled task because the task's license is expired		
96812	info	system	error	Update allowed only if you have a valid license		
96813	info	system	status	Software updates are disabled		
96814	info	system	status	Software updates from FortiGuard have been disabled because this client is managed		
96815	info	system	error	Software updates require administrative privileges		
96816	info	system	status	Software update successful		
96817	info	system	error	Software update failed		

Log ID	Level	Sub Type	Event Type	Message		
96818	info	system	error	Unable to perform software update. Registry does not contain image id to download		
96820	error	system	error	Failed to load the av engine		
96821	error	system	error	Error patching AV signatur		
96822	error	system	error	Unable to load FASLE engine		
96823	info	system	status	Checking for updates		
96824	info	system	status	Software update started		
96825	info	system	status	Update was successful, current engine/signature information recorded		
				Field	Field Description	Field Type
				avengine	AV engine	string
				avsig	AV signature	string
				avsigext	AV extended signature	string
				avsigetm	AV extreme signature	string
				avsigheu	AV heuristic signature	string
				rootkitengine	anti-rootkit engine	string
				rootkitsig	anti-rootkit signature	string
				appsig	app DB signature	string
				appengine	app DB engine	string
				vulnsig	vulnerability signature	string
				vulnengine	vulnerability engine	string
				ipseng	firewall engine	string
				ipssig	firewall signature	string
				irdbsig	irdb signature	string
96840	warning	system	status	Fortiproxy is disabled		
96841	info	system	status	Fortiproxy is enabled		
96851	info	system	status	FortiShield is enabled		
96850	warning	system	status	FortiShield is disabled		
96855	warning	system	action	FortiShield has prevented an application from modifying a file or registry setting protected by FortiClient		

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				processname	blocked process	string
				file	file or registry path	string
96873	info	system	status	FortiClient is shutting down		
96882	info	system	status	Logged when push configuration is received		
				Field	Field Description	Field Type
				polycname	policy name	string

systemevent > update

Log ID	Level	Sub Type	Event Type	Message		
96650	info	update	status	Update was successful		
				Field	Field Description	Field Type
				avengine	AV engine	string
				avsig	AV signature	string
				avsigext	AV extended signature	string
				avsigetm	AV extreme signature	string
				avsigheu	AV heuristic signature	string
				avsigpallas	AV pallas signature	string
				rootkitengine	anti-rootkit engine	string
				rootkitsig	anti-rootkit signature	string
				appsig	app DB signature	string
				appengine	app DB engine	string
				vulnsig	vulnerability signature	string
				vulnengine	vulnerability engine	string
				ipseng	firewall engine	string

Log ID	Level	Sub Type	Event Type	Message																																													
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>ipssig</td><td>firewall signature</td><td>string</td></tr><tr><td>irdbsig</td><td>irdb signature</td><td>string</td></tr><tr><td>avsiglastupdate</td><td>last update time</td><td>string</td></tr></table>	Field	Field Description	Field Type	ipssig	firewall signature	string	irdbsig	irdb signature	string	avsiglastupdate	last update time	string																																	
				Field	Field Description	Field Type																																											
				ipssig	firewall signature	string																																											
				irdbsig	irdb signature	string																																											
avsiglastupdate	last update time	string																																															
96819	info	update	status	Update was successful to the given version for the given module																																													
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>avengine</td><td>AV engine</td><td>string</td></tr><tr><td>avsig</td><td>AV signature</td><td>string</td></tr><tr><td>avsigext</td><td>AV extended signature</td><td>string</td></tr><tr><td>avsigetm</td><td>AV extreme signature</td><td>string</td></tr><tr><td>avsigheu</td><td>AV heuristic signature</td><td>string</td></tr><tr><td>rootkitengine</td><td>anti-rootkit engine</td><td>string</td></tr><tr><td>rootkitsig</td><td>anti-rootkit signature</td><td>string</td></tr><tr><td>appsig</td><td>app DB signature</td><td>string</td></tr><tr><td>appengine</td><td>app DB engine</td><td>string</td></tr><tr><td>vulnsig</td><td>vulnerability signature</td><td>string</td></tr><tr><td>vulnengine</td><td>vulnerability engine</td><td>string</td></tr><tr><td>ipseng</td><td>firewall engine</td><td>string</td></tr><tr><td>ipssig</td><td>firewall signature</td><td>string</td></tr><tr><td>irdbsig</td><td>irdb signature</td><td>string</td></tr></table>	Field	Field Description	Field Type	avengine	AV engine	string	avsig	AV signature	string	avsigext	AV extended signature	string	avsigetm	AV extreme signature	string	avsigheu	AV heuristic signature	string	rootkitengine	anti-rootkit engine	string	rootkitsig	anti-rootkit signature	string	appsig	app DB signature	string	appengine	app DB engine	string	vulnsig	vulnerability signature	string	vulnengine	vulnerability engine	string	ipseng	firewall engine	string	ipssig	firewall signature	string	irdbsig	irdb signature	string
				Field	Field Description	Field Type																																											
				avengine	AV engine	string																																											
				avsig	AV signature	string																																											
				avsigext	AV extended signature	string																																											
				avsigetm	AV extreme signature	string																																											
				avsigheu	AV heuristic signature	string																																											
				rootkitengine	anti-rootkit engine	string																																											
				rootkitsig	anti-rootkit signature	string																																											
				appsig	app DB signature	string																																											
				appengine	app DB engine	string																																											
				vulnsig	vulnerability signature	string																																											
				vulnengine	vulnerability engine	string																																											
				ipseng	firewall engine	string																																											
				ipssig	firewall signature	string																																											
irdbsig	irdb signature	string																																															

traffic > system

Log ID	Level	Sub Type	Event Type	Message
96900	info	system	traffic	Traffic log

Log ID	Level	Sub Type	Event Type	Message																																																															
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>sessionid</td><td>network session</td><td>string</td></tr><tr><td>regip</td><td>regip</td><td>string</td></tr><tr><td>srcname</td><td>source name</td><td>string</td></tr><tr><td>srcproduct</td><td>source product</td><td>string</td></tr><tr><td>srcip</td><td>source IP</td><td>string</td></tr><tr><td>srcport</td><td>source port</td><td>int</td></tr><tr><td>direction</td><td>traffic direction</td><td>string</td></tr><tr><td>dstip</td><td>destination IP</td><td>string</td></tr><tr><td>remotename</td><td>remote name</td><td>string</td></tr><tr><td>dstport</td><td>destination port</td><td>int</td></tr><tr><td>proto</td><td>network protocol</td><td>int</td></tr><tr><td>rcvdbyte</td><td>data received (in bytes)</td><td>int</td></tr><tr><td>sentbyte</td><td>data sent (in bytes)</td><td>int</td></tr><tr><td>utmaction</td><td>utm action</td><td>string</td></tr><tr><td>utmevent</td><td>utm event</td><td>string</td></tr><tr><td>threat</td><td>threat</td><td>string</td></tr><tr><td>service</td><td>network protocol</td><td>string</td></tr><tr><td>userinitiated</td><td>if user initiated url request</td><td>int</td></tr><tr><td>browsetime</td><td>user browsing time of web page(in seconds)</td><td>int</td></tr><tr><td>url</td><td>url</td><td>string</td></tr></table>	Field	Field Description	Field Type	sessionid	network session	string	regip	regip	string	srcname	source name	string	srcproduct	source product	string	srcip	source IP	string	srcport	source port	int	direction	traffic direction	string	dstip	destination IP	string	remotename	remote name	string	dstport	destination port	int	proto	network protocol	int	rcvdbyte	data received (in bytes)	int	sentbyte	data sent (in bytes)	int	utmaction	utm action	string	utmevent	utm event	string	threat	threat	string	service	network protocol	string	userinitiated	if user initiated url request	int	browsetime	user browsing time of web page(in seconds)	int	url	url	string
				Field	Field Description	Field Type																																																													
				sessionid	network session	string																																																													
				regip	regip	string																																																													
				srcname	source name	string																																																													
				srcproduct	source product	string																																																													
				srcip	source IP	string																																																													
				srcport	source port	int																																																													
				direction	traffic direction	string																																																													
				dstip	destination IP	string																																																													
				remotename	remote name	string																																																													
				dstport	destination port	int																																																													
				proto	network protocol	int																																																													
				rcvdbyte	data received (in bytes)	int																																																													
				sentbyte	data sent (in bytes)	int																																																													
				utmaction	utm action	string																																																													
				utmevent	utm event	string																																																													
				threat	threat	string																																																													
				service	network protocol	string																																																													
				userinitiated	if user initiated url request	int																																																													
				browsetime	user browsing time of web page(in seconds)	int																																																													
				url	url	string																																																													

Linux

This section contains the following information for FortiClient (Linux):

- [Mandatory fields on page 35](#): fields that are mandatory to all FortiClient (Linux) logs.
- [Log fields by type on page 36](#): fields that only apply to security event logs.
- [Log message by type on page 39](#): lists each possible log message, sorted by log type and subtype.

Mandatory fields

Log Field Name	Description	Data Type
date	date	string
time	time	string
logver	log protocol version	int
id	log id	int
type	Traffic, Security Event or System Event	string
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string
eventtype	type of event	enumeration string
level	log level	enumeration string
uid	FortiClient unique ID	string
devid	device ID	string
hostname	host name of local machine	string
pcdomain	domain name of local machine	string
deviceip	device IP address	string
devicemac	device MAC address	string
vd	vdom	string
fctver	FCT version	string
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string

Log Field Name	Description	Data Type
os	operating system	string
user	current logged on user	string
msg	description of this log	string

Log fields by type

securityevent

Log Field Name	Description	Data Type	Length
action	block or monitor	string	32
file	file location	string	256
virus	virus name	string	512
sigid	signature id	string	260
from	email from	string	128
to	email to	string	512
service	network protocol	string	64
vpn	vpn tunnel name	string	32
filesize	file size	int	20
checksum	file crc32 checksum	int	20
detectedby	the security feature that detected virus	enumeration string	64
detectedin	where the virus is detected	enumeration string	64
viruscat	virus category	string	260
vulnid	id of the vulnerability	int	20
vulnname	name of the vulnerability	string	128
vulnseverity	severity level	string	8
vulncat	category	string	32
vulncvss	cvss score	string	64
vulnref	reference of the vulnerability	string	256
vulnengine	engine version	string	64

Log Field Name	Description	Data Type	Length
vulnsignature	signature version	string	260
vulnproducts	name of the vulnerable product	string	2048
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

systemevent

Log Field Name	Description	Data Type	Length
eponlinest	online status	enumeration string	32
epplace	EP place	enumeration string	32
emshostname	EMS host name	string	64
status	status description	string	16
emsip	EMS IP	string	20
fctip	FCT IP	string	20
epmgmtst	management status	enumeration string	64
epquarmsg	quarant message	string	260
epfeatures	installed features list	string	128
epenfeatures	enabled features list	string	128
ephbemsduration	EMS heart beat duration	int	20
ephbemslast	EMS heart beat last time	string	64
social_email	social email	string	128
social_phone	social phone number	string	64
social_srvc	social service	string	64
social_user	social user name	string	256
date	date	string	260
time	time	string	260
logver	log protocol version	int	20
id	log id	int	20
type	Traffic, Security Event or System Event	string	16
subtype	AntiVirus, FireWall, WebFilter ...	enumeration string	32
eventtype	type of event	enumeration string	32
level	log level	enumeration string	20
uid	FortiClient unique ID	string	32

Log Field Name	Description	Data Type	Length
devid	device ID	string	16
hostname	host name of local machine	string	256
pcdomain	domain name of local machine	string	128
deviceip	device IP address	string	20
devicemac	device MAC address	string	17
vd	vdom	string	512
fctver	FCT version	string	16
fgtserial	FGT serial number	string	16
emsserial	EMS serial number	string	16
usingpolicy	current policy name	string	64
os	operating system	string	96
user	current logged on user	string	256
msg	description of this log	string	512

Log message by type

securityevent > av

Log ID	Level	Sub Type	Event Type	Message		
96530	warning	av	action	Found virus		
				Field	Field Description	Field Type
				action	block or monitor	string
				file	file location	string
				virus	virus name	string
				sigid	signature id	string
				from	email from	string
				to	email to	string
				service	network protocol	string
				vpn	vpn tunnel name	string

Log ID	Level	Sub Type	Event Type	Message																														
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>filesize</td><td>file size</td><td>int</td></tr><tr><td>checksum</td><td>file crc32 checksum</td><td>int</td></tr><tr><td>detectedby</td><td>the security feature that detected virus</td><td>enumeration string</td></tr><tr><td>detectedin</td><td>where the virus is detected</td><td>enumeration string</td></tr></table>	Field	Field Description	Field Type	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string															
				Field	Field Description	Field Type																												
				filesize	file size	int																												
				checksum	file crc32 checksum	int																												
				detectedby	the security feature that detected virus	enumeration string																												
detectedin	where the virus is detected	enumeration string																																
96531	warning	av	warning	Found malware																														
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>action</td><td>block or monitor</td><td>string</td></tr><tr><td>file</td><td>file location</td><td>string</td></tr><tr><td>virus</td><td>virus name</td><td>string</td></tr><tr><td>viruscat</td><td>virus category</td><td>string</td></tr><tr><td>sigid</td><td>signature id</td><td>string</td></tr><tr><td>filesize</td><td>file size</td><td>int</td></tr><tr><td>checksum</td><td>file crc32 checksum</td><td>int</td></tr><tr><td>detectedby</td><td>the security feature that detected virus</td><td>enumeration string</td></tr><tr><td>detectedin</td><td>where the virus is detected</td><td>enumeration string</td></tr></table>	Field	Field Description	Field Type	action	block or monitor	string	file	file location	string	virus	virus name	string	viruscat	virus category	string	sigid	signature id	string	filesize	file size	int	checksum	file crc32 checksum	int	detectedby	the security feature that detected virus	enumeration string	detectedin	where the virus is detected	enumeration string
				Field	Field Description	Field Type																												
				action	block or monitor	string																												
				file	file location	string																												
				virus	virus name	string																												
				viruscat	virus category	string																												
				sigid	signature id	string																												
				filesize	file size	int																												
				checksum	file crc32 checksum	int																												
				detectedby	the security feature that detected virus	enumeration string																												
detectedin	where the virus is detected	enumeration string																																

securityevent > vulnerabilityscan

Log ID	Level	Sub Type	Event Type	Message		
96521	info	vulnerabilityscan	status	A vulnerability scan result has been logged		
				Field	Field Description	Field Type
				vulnid	id of the vulnerability	int
				vulnname	name of the vulnerability	string
				vulnseverity	severity level	string

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				vulncat	category	string
				vulncvss	cvss score	string
				vulnref	reference of the vulnerability	string
				vulnengine	engine version	string
				vulnsignature	signature version	string
				vulnproducts	name of the vulnerable product	string
96522	info	vulnerabilityscan	status	Applying patch for vulnerability found		
				Field	Field Description	Field Type
				vulnid	id of the vulnerability	int
				vulnname	name of the vulnerability	string
				vulnseverity	severity level	string
				vulncat	category	string
				vulncvss	cvss score	string
				vulnref	reference of the vulnerability	string
				vulnengine	engine version	string
				vulnsignature	signature version	string
				vulnproducts	name of the vulnerable product	string

systemevent > endpoint

Log ID	Level	Sub Type	Event Type	Message
96953	info	endpoint	status	Endpoint Control Status Changed

Log ID	Level	Sub Type	Event Type	Message																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>eponlinest</td><td>online status</td><td>enumeration string</td></tr><tr><td>epplace</td><td>EP place</td><td>enumeration string</td></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr><tr><td>status</td><td>status description</td><td>string</td></tr></table>	Field	Field Description	Field Type	eponlinest	online status	enumeration string	epplace	EP place	enumeration string	emshostname	EMS host name	string	status	status description	string			
				Field	Field Description	Field Type																
				eponlinest	online status	enumeration string																
				epplace	EP place	enumeration string																
				emshostname	EMS host name	string																
status	status description	string																				
96955	info	endpoint	status	Endpoint Control Registration Status Changed																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr><tr><td>status</td><td>status description</td><td>string</td></tr><tr><td>emsip</td><td>EMS IP</td><td>string</td></tr><tr><td>fctip</td><td>FCT IP</td><td>string</td></tr></table>	Field	Field Description	Field Type	emshostname	EMS host name	string	status	status description	string	emsip	EMS IP	string	fctip	FCT IP	string			
				Field	Field Description	Field Type																
				emshostname	EMS host name	string																
				status	status description	string																
				emsip	EMS IP	string																
fctip	FCT IP	string																				
96956	info	endpoint	status	Endpoint Quarantine Status Changed																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>epmgmtst</td><td>management status</td><td>enumeration string</td></tr><tr><td>epquarmsg</td><td>quarant message</td><td>string</td></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr></table>	Field	Field Description	Field Type	epmgmtst	management status	enumeration string	epquarmsg	quarant message	string	emshostname	EMS host name	string						
				Field	Field Description	Field Type																
				epmgmtst	management status	enumeration string																
				epquarmsg	quarant message	string																
emshostname	EMS host name	string																				
96957	info	endpoint	status	Endpoint Ext Log to FAZ																		
				<table><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr><tr><td>epfeatures</td><td>installed features list</td><td>string</td></tr><tr><td>epenfeatures</td><td>enabled features list</td><td>string</td></tr><tr><td>ephbemsduration</td><td>EMS heart beat duration</td><td>int</td></tr><tr><td>ephbemslast</td><td>EMS heart beat last time</td><td>string</td></tr><tr><td>emshostname</td><td>EMS host name</td><td>string</td></tr></table>	Field	Field Description	Field Type	epfeatures	installed features list	string	epenfeatures	enabled features list	string	ephbemsduration	EMS heart beat duration	int	ephbemslast	EMS heart beat last time	string	emshostname	EMS host name	string
				Field	Field Description	Field Type																
				epfeatures	installed features list	string																
				epenfeatures	enabled features list	string																
				ephbemsduration	EMS heart beat duration	int																
				ephbemslast	EMS heart beat last time	string																
emshostname	EMS host name	string																				
96958	info	endpoint	status	User social media information																		

Log ID	Level	Sub Type	Event Type	Message		
				Field	Field Description	Field Type
				social_email	social email	string
				social_phone	social phone number	string
				social_srvc	social service	string
				social_user	social user name	string



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. 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.