

Log Reference

FortiClient 6.4.7



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



November 25, 2021

FortiClient 6.4.7 Log Reference

04-647-757206-20211125

TABLE OF CONTENTS

Change Log	4
Introduction	5
Mandatory fields	5
Log fields by type	6
securityevent	6
systemevent	9
traffic	11
Log message by type	13
>	13

Change Log

Date	Change Description
2021-11-25	Initial release.

Introduction

This document provides information about all the log messages applicable to FortiClient 6.4.7. 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:

- [Mandatory fields on page 5](#): fields that are mandatory to all FortiClient logs.
- [Log fields by type on page 6](#): 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

Log Field Name	Description	Data Type
fgtserial	FGT serial number	string
emsserial	EMS serial number	string
usingpolicy	current policy name	string
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
deviceip	device IP address	string	20

Log Field Name	Description	Data Type	Length
devicemac	device MAC address	string	17
devid	device ID	string	16
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
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

Log Field Name	Description	Data Type	Length
service	network protocol	string	64
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
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
policyname	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

>

Log ID	Level	Sub Type	Event Type	Message																		
96500	info			User enabled Webfilter																		
96501	warning			User disabled Webfilter																		
96502	warning			user's access to the url is blocked																		
				<table><thead><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr></thead><tbody><tr><td>cat</td><td>category id</td><td>int</td></tr><tr><td>category</td><td>category name</td><td>string</td></tr><tr><td>service</td><td>network protocol</td><td>string</td></tr><tr><td>ip</td><td>IP address</td><td>string</td></tr><tr><td>status</td><td>status</td><td>enumeration string</td></tr></tbody></table>	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
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			user's access to the url is bypassed																		
				<table><thead><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr></thead><tbody><tr><td>cat</td><td>category id</td><td>int</td></tr><tr><td>category</td><td>category name</td><td>string</td></tr><tr><td>service</td><td>network protocol</td><td>string</td></tr><tr><td>ip</td><td>IP address</td><td>string</td></tr><tr><td>status</td><td>status</td><td>enumeration string</td></tr></tbody></table>	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
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																				
96520	info			The vulnerability scan status has changed																		
				<table><thead><tr><th>Field</th><th>Field Description</th><th>Field Type</th></tr></thead><tbody><tr><td>status</td><td>scan status</td><td>string</td></tr></tbody></table>	Field	Field Description	Field Type	status	scan status	string												
Field	Field Description	Field Type																				
status	scan status	string																				
96521	info			A vulnerability scan result has been logged																		

Log message by type

Log ID	Level	Sub Type	Event Type	Message																														
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vulnid</td><td>id of the vulnerability</td><td>int</td></tr> <tr> <td>vulnname</td><td>name of the vulnerability</td><td>string</td></tr> <tr> <td>vulnseverity</td><td>severity level</td><td>string</td></tr> <tr> <td>vulncat</td><td>category</td><td>string</td></tr> <tr> <td>vulncvss</td><td>cvss score</td><td>string</td></tr> <tr> <td>vulnref</td><td>reference of the vulnerability</td><td>string</td></tr> <tr> <td>vulnengine</td><td>engine version</td><td>string</td></tr> <tr> <td>vulnsignature</td><td>signature version</td><td>string</td></tr> <tr> <td>vulnproducts</td><td>name of the vulnerable product</td><td>string</td></tr> </tbody> </table>	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
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																																
96522	info			Applying patch for vulnerability found																														
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vulnid</td><td>id of the vulnerability</td><td>int</td></tr> <tr> <td>vulnname</td><td>name of the vulnerability</td><td>string</td></tr> <tr> <td>vulnseverity</td><td>severity level</td><td>string</td></tr> <tr> <td>vulncat</td><td>category</td><td>string</td></tr> <tr> <td>vulncvss</td><td>cvss score</td><td>string</td></tr> <tr> <td>vulnref</td><td>reference of the vulnerability</td><td>string</td></tr> <tr> <td>vulnengine</td><td>engine version</td><td>string</td></tr> <tr> <td>vulnsignature</td><td>signature version</td><td>string</td></tr> <tr> <td>vulnproducts</td><td>name of the vulnerable product</td><td>string</td></tr> </tbody> </table>	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
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			Applying patch for Windows vulnerability																														
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vulnid</td><td>id of the vulnerability</td><td>int</td></tr> <tr> <td>vulnname</td><td>name of the vulnerability</td><td>string</td></tr> <tr> <td>vulnseverity</td><td>severity level</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vulnid	id of the vulnerability	int	vulnname	name of the vulnerability	string	vulnseverity	severity level	string																		
Field	Field Description	Field Type																																
vulnid	id of the vulnerability	int																																
vulnname	name of the vulnerability	string																																
vulnseverity	severity level	string																																

Log message by type

Log ID	Level	Sub Type	Event Type	Message																																										
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vulncat</td><td>category</td><td>string</td></tr> <tr> <td>vulncvss</td><td>cvss score</td><td>string</td></tr> <tr> <td>vulnref</td><td>reference of the vulnerability</td><td>string</td></tr> <tr> <td>vulnengine</td><td>engine version</td><td>string</td></tr> <tr> <td>vulnsignature</td><td>signature version</td><td>string</td></tr> <tr> <td>vulnproducts</td><td>name of the vulnerable product</td><td>string</td></tr> </tbody> </table>	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																					
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																																												
96530	warning			Found virus																																										
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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>vid</td><td>virus id</td><td>int</td></tr> <tr> <td>from</td><td>email from</td><td>string</td></tr> <tr> <td>to</td><td>email to</td><td>string</td></tr> <tr> <td>service</td><td>network protocol</td><td>string</td></tr> <tr> <td>vpn</td><td>vpn tunnel name</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> </tbody> </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	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	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																																												
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																																												
detectedby	the security feature that detected virus	enumeration string																																												
detectedin	where the virus is detected	enumeration string																																												
96531	warning			Found malware																																										
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>action</td><td>action taken for the infected item</td><td>enumeration string</td></tr> </tbody> </table>	Field	Field Description	Field Type	action	action taken for the infected item	enumeration string																																				
Field	Field Description	Field Type																																												
action	action taken for the infected item	enumeration string																																												

Log message by type

Log ID	Level	Sub Type	Event Type	Message																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	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																										
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			User disabled Realtime AntiVirus protection																								
96535	info			Communication error with other modules																								
96536	warning			AntiVirus realtime protection killed malware process																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>processname</td><td>process name</td><td>string</td></tr> <tr> <td>detectedby</td><td>the security feature that detected virus</td><td>enumeration string</td></tr> </tbody> </table>	Field	Field Description	Field Type	processname	process name	string	detectedby	the security feature that detected virus	enumeration string															
Field	Field Description	Field Type																										
processname	process name	string																										
detectedby	the security feature that detected virus	enumeration string																										
96537	info			av_task scan thread is suspended																								
96538	info			av_task scan thread is resumed																								
96540	info			Cannot start scan task, license expired																								
96541	info			av_task scan is started																								
96542	info			av_task scan is stopped																								
96543	error			Scheduled scan failed: Path to file/folder no longer exists																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>file</td><td>file or directory does not exist</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	file	file or directory does not exist	string																		
Field	Field Description	Field Type																										
file	file or directory does not exist	string																										
96550	error			Failed to restore quarantined file																								

Log message by type

Log ID	Level	Sub Type	Event Type	Message																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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
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			A quarantined file was restored																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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
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																										
96548	warning			AntiExploit has detected violation																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>action</td><td>action taken for violation</td><td>enumeration string</td></tr> <tr> <td>ae_api</td><td>API used of the violation</td><td>string</td></tr> <tr> <td>ae_reason</td><td>reason of the violation</td><td>string</td></tr> <tr> <td>app</td><td>application</td><td>string</td></tr> </tbody> </table>	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									
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																										
96545	debug			Failed to connect to FortiSandbox server																								

Log message by type

Log ID	Level	Sub Type	Event Type	Message																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> </table>	Field	Field Description	Field Type																					
Field	Field Description	Field Type																										
				<table border="1"> <tbody> <tr> <td>failed_reason</td><td>reason of the failure</td><td>string</td></tr> </tbody> </table>	failed_reason	reason of the failure	string																					
failed_reason	reason of the failure	string																										
96556	warning			Failed to submit file to FortiSandbox server																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> </table>	Field	Field Description	Field Type																					
Field	Field Description	Field Type																										
				<table border="1"> <tbody> <tr> <td>file</td><td>file location</td><td>string</td></tr> <tr> <td>error_code</td><td>reason of the failure</td><td>int</td></tr> </tbody> </table>	file	file location	string	error_code	reason of the failure	int																		
file	file location	string																										
error_code	reason of the failure	int																										
96557	warning			Failed to query checksum to FortiSandbox server																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> </table>	Field	Field Description	Field Type																					
Field	Field Description	Field Type																										
				<table border="1"> <tbody> <tr> <td>file</td><td>file location</td><td>string</td></tr> <tr> <td>error_code</td><td>reason of the failure</td><td>int</td></tr> </tbody> </table>	file	file location	string	error_code	reason of the failure	int																		
file	file location	string																										
error_code	reason of the failure	int																										
96546	warning			Found virus																								
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> </table>	Field	Field Description	Field Type																					
Field	Field Description	Field Type																										
				<table border="1"> <tbody> <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> </tbody> </table>	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
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			Sandbox is not authorized																								
96554	info			file is submitted to Sandbox service																								

Log message by type

Log ID	Level	Sub Type	Event Type	Message															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			file score received															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																	
97100	debug			file score received															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																	
98000	warning			AntiRansomware has found suspicious process															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			
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																	
96560	info			VPN tunnel status															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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>vpn tunnel user name</td><td>string</td></tr> <tr> <td>remotecgw</td><td>remote gateway</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpnstate	tunnel status	enumeration string	vpntunnel	tunnel name	string	vpnuser	vpn tunnel user name	string	remotecgw	remote gateway	string
Field	Field Description	Field Type																	
vpnstate	tunnel status	enumeration string																	
vpntunnel	tunnel name	string																	
vpnuser	vpn tunnel user name	string																	
remotecgw	remote gateway	string																	

Log message by type

Log ID	Level	Sub Type	Event Type	Message																				
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	locip	local ip	string	locport	local port	int	remip	remote ip	string	remport	remote port	int					
Field	Field Description	Field Type																						
locip	local ip	string																						
locport	local port	int																						
remip	remote ip	string																						
remport	remote port	int																						
96561	warning			No response from the peer, phase1 retransmit reaches maximum count																				
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																						
96562	warning			No response from the peer, phase2 retransmit reaches maximum count																				
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																						
96563	warning			Received delete payload from peer check xauth password																				
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 message by type

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>remip</td><td>remote ip</td><td>string</td></tr> <tr> <td>rempor</td><td>remote port</td><td>int</td></tr> </tbody> </table>	Field	Field Description	Field Type	remip	remote ip	string	rempor	remote port	int									
Field	Field Description	Field Type																				
remip	remote ip	string																				
rempor	remote port	int																				
96564	error			Failed to acquire an IP address for the virtual adapter																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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>rempor</td><td>remote port</td><td>int</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	rempor	remote port	int
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
locip	local ip	string																				
locport	local port	int																				
remip	remote ip	string																				
rempor	remote port	int																				
96565	error			General error of IKE																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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>rempor</td><td>remote port</td><td>int</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string	locip	local ip	string	locport	local port	int	remip	remote ip	string	rempor	remote port	int
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
locip	local ip	string																				
locport	local port	int																				
remip	remote ip	string																				
rempor	remote port	int																				
96566	info			negotiation information																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vpntunnel</td><td>tunnel name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
96567	error			negotiation error																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vpntunnel</td><td>tunnel name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
96568	error			replayed packet detected (packet dropped)																		

Log message by type

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vpntunnel</td><td>tunnel name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
96569	info			The VPN user accept the banner warning																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			The VPN user reject the banner warning and disconnect the tunnel																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			Send sa to the IPsec driver																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																				
96574	error			Logged when a VPN authorization rule failed																		

Log message by type

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>vpntunnel</td><td>tunnel name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vpntunnel	tunnel name	string												
Field	Field Description	Field Type																				
vpntunnel	tunnel name	string																				
96575	warning			VPN cannot connect because the specified application is not running																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>app</td><td>application</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	app	application	string												
Field	Field Description	Field Type																				
app	application	string																				
96576	info			IKE phase1 authentication fail as peer's certificate is not verified																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			IKE phase1 authentication fail as peer's certificate is not verified																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																				
96600	info			SSLVPN tunnel status																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			Telephony service (TapiSrv) is not running																		

Log message by type

Log ID	Level	Sub Type	Event Type	Message															
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 service started successfully																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 tunnel connection failed																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 cannot connect because the specified application is not running																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>app</td><td>application</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	app	application	string									
Field	Field Description	Field Type																	
app	application	string																	
96610	info	SSLVPN(DTLS) tunnel status																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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																	

Log message by type

Log ID	Level	Sub Type	Event Type	Message																																	
96620	info			usb storage activity																																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>action</td><td>action</td><td>enumeration string</td></tr> <tr> <td>activity</td><td>activity</td><td>enumeration string</td></tr> <tr> <td>description</td><td>description</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	action	action	enumeration string	activity	activity	enumeration string	description	description	string																					
Field	Field Description	Field Type																																			
action	action	enumeration string																																			
activity	activity	enumeration string																																			
description	description	string																																			
96645	warning			The application firewall has been disabled because it's driver could not be loaded																																	
96701	warning			Application Control found a rule violation																																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>path</td><td>path of process</td><td>string</td></tr> <tr> <td>username</td><td>username of process</td><td>string</td></tr> <tr> <td>domain</td><td>domain of user</td><td>string</td></tr> <tr> <td>ruleuuid</td><td>uuid of violated rule</td><td>string</td></tr> <tr> <td>action</td><td>block or monitor</td><td>string</td></tr> </tbody> </table>	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															
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																																			
96650	info			Update was successful																																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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>avsigpallas</td><td>AV pallas 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> </tbody> </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	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
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																																			

Log message by type

Log ID	Level	Sub Type	Event Type	Message																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> <tr> <td>avsiglastupdate</td><td>last update time</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	vulnsig	vulnerability signature	string	vulnengine	vulnerability engine	string	ipseng	firewall engine	string	ipssig	firewall signature	string	irdbsig	irdb signature	string	avsiglastupdate	last update time	string
Field	Field Description	Field Type																							
vulnsig	vulnerability signature	string																							
vulnengine	vulnerability engine	string																							
ipseng	firewall engine	string																							
ipssig	firewall signature	string																							
irdbsig	irdb signature	string																							
avsiglastupdate	last update time	string																							
96800	info			Forcefully kill a child process after grace period expires																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>apppath</td><td>process name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	apppath	process name	string															
Field	Field Description	Field Type																							
apppath	process name	string																							
96801	error			The scheduler cannot start the scheduled task because the task's license is expired																					
96812	info			Update allowed only if you have a valid license																					
96813	info			Software updates are disabled																					
96814	info			Software updates from FortiGuard have been disabled because this client is managed																					
96815	info			Software updates require administrative privileges																					
96816	info			Software update successful																					
96817	info			Software update failed																					
96818	info			Unable to perform software update. Registry does not contain image id to download																					
96819	info			Update was successful to the given version for the given module																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	avengine	AV engine	string	avsig	AV signature	string	avsigext	AV extended signature	string	avsigetm	AV extreme 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																							

Log message by type

Log ID	Level	Sub Type	Event Type	Message																																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	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																																			
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																																			
96820	error			Failed to load the av engine																																	
96821	error			Error patching AV signatur																																	
96822	error			Unable to load FASLE engine																																	
96823	info			Checking for updates																																	
96824	info			Software update started																																	
96825	info			Update was successful, current engine/signature information recorded																																	
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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						
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																																			

Log message by type

Log ID	Level	Sub Type	Event Type	Message																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	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																							
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			Fortiproxy is disabled																					
96841	info			Fortiproxy is enabled																					
96851	info			FortiShield is enabled																					
96850	warning			FortiShield is disabled																					
96855	warning			FortiShield has prevented an application from modifying a file or registry setting protected by FortiClient																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>processname</td><td>blocked process</td><td>string</td></tr> <tr> <td>file</td><td>file or registry path</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	processname	blocked process	string	file	file or registry path	string												
Field	Field Description	Field Type																							
processname	blocked process	string																							
file	file or registry path	string																							
96873	info			FortiClient is shutting down																					
96882	info			Logged when push configuration is received																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>policyname</td><td>policy name</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	policyname	policy name	string															
Field	Field Description	Field Type																							
policyname	policy name	string																							
96900	info			Traffic log																					
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	sessionid	network session	string	regip	regip	string	srcname	source name	string									
Field	Field Description	Field Type																							
sessionid	network session	string																							
regip	regip	string																							
srcname	source name	string																							

Log message by type

Log ID	Level	Sub Type	Event Type	Message																																																						
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </table>	Field	Field Description	Field Type	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																																																								
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																																																								
96953	info			Endpoint Control Status Changed																																																						
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 Control Registration Status Changed																																																						

Log message by type

Log ID	Level	Sub Type	Event Type	Message																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 Quarantine Status Changed																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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 Ext Log to FAZ																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <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> </tbody> </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			User social media information																		
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>social_srvc</td><td>social service</td><td>string</td></tr> <tr> <td>social_user</td><td>social user name</td><td>string</td></tr> <tr> <td>social_email</td><td>social email</td><td>string</td></tr> <tr> <td>social_phone</td><td>social phone number</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	social_srvc	social service	string	social_user	social user name	string	social_email	social email	string	social_phone	social phone number	string			
Field	Field Description	Field Type																				
social_srvc	social service	string																				
social_user	social user name	string																				
social_email	social email	string																				
social_phone	social phone number	string																				

Log message by type

Log ID	Level	Sub Type	Event Type	Message												
96959	info			Current AV allowlist engine/signatures this endpoint is using												
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>emshostname</td><td>EMS host name</td><td>string</td></tr> <tr> <td>avaleng</td><td>AV allowlist engine version</td><td>string</td></tr> <tr> <td>avalsig</td><td>AV allowlist signatures version</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	emshostname	EMS host name	string	avaleng	AV allowlist engine version	string	avalsig	AV allowlist signatures version	string
Field	Field Description	Field Type														
emshostname	EMS host name	string														
avaleng	AV allowlist engine version	string														
avalsig	AV allowlist signatures version	string														
96980	info			Single Sign-On event												
				<table border="1"> <thead> <tr> <th>Field</th><th>Field Description</th><th>Field Type</th></tr> </thead> <tbody> <tr> <td>action</td><td>action</td><td>enumeration string</td></tr> <tr> <td>domain</td><td>domain name</td><td>string</td></tr> <tr> <td>remotegw</td><td>remote gateway</td><td>string</td></tr> </tbody> </table>	Field	Field Description	Field Type	action	action	enumeration string	domain	domain name	string	remotegw	remote gateway	string
Field	Field Description	Field Type														
action	action	enumeration string														
domain	domain name	string														
remotegw	remote gateway	string														
96983	info			Single Sign-On Mobility Agent is starting												
96984	info			Single Sign-On Mobility Agent is stopping												



www.fortinet.com

Copyright© 2021 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.