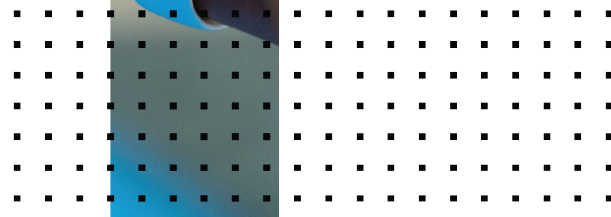
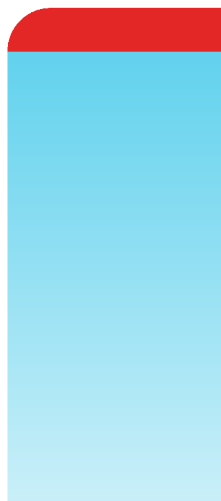


Log Reference

FortiSandbox 4.4.0



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>

FORTINET TRAINING 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



July 11, 2023

FortiSandbox 4.4.0 Log Reference

34-440-922625-20230711

TABLE OF CONTENTS

Introduction	4
Log Information	5
Log Types	5
Type	5
Subtype	5
Log Field	5
FortiSandbox 4.4 Log Messages	6
Alert	6
MALWARE	6
NETATTACK	7
NETBOTNET	7
NETURL	8
Event	8
SYSTEM	8
PERFORMANCE	11
RESOURCE	13
REPORT	13
Change Log	14

Introduction

This document provides information about all the log messages applicable to the FortiSandbox 4.4.0 and higher. The logs are intended for administrators to be used as reference for more information about a specific log entry and message that is generated.

For more information on logs, see the [FortiSandbox 4.4.0 Administration Guide](#).

Log Information

Log Types

Type	Description	Subtype
Alert	Records virus attack and intrusion attempts.	Malware Netattack Netbotnet Neturl
Event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	System

Type

Each log message contains a Type (type) field that indicates its category, and in which log file it is stored.

Subtype

Each log message contains a Sub Type (subtype) field that further subdivides its category based on the feature associated with the cause of the log message.

Log Field

The following table describes the standard format in which each log type is described in this document. For documentation purposes, all log types and sub types follow this generic table format to present the log entry information.

Log Field	Log Field Description	Data Type	Length
devid	Device ID for FortiSandbox in FortiAnalyzer	string	16

FortiSandbox 4.4 Log Messages

The following tables list the FortiSandbox 4.4 log messages.

Alert

MALWARE

Log Field Name	Description	Data Type	Length
devid	Device ID for FortiSandbox in FortiAnalyzer	string	16
logid	Log ID	string	8
type	Log Type	string	16
subtype	Log Subtype	string	32
level	Log Level	string	16
tzone	time offset in seconds to UTC	int32	32
clientdev	Client Device	string	64
clientvd	Client VDOM	string	64
fname	File Name	string	1024
jobid	Job process ID	string	16
md5	MD5 checksum	string	32
mname	Malware Name	string	256
proto	Protocol	string	16
risk	Risk name	string	16
sha256	SHA256 checksum	string	64
scanstart	Scan Start Time	uint32	32
scanned	Scan End Time	uint32	32
srcip	Source IP address	string	45
srcport	Source Port Number	int32	32
dstip	Destination IP Address	string	45
dstport	Destination Port Number	int32	32
stype	Source Type	string	16

Log Field Name	Description	Data Type	Length
suser	Source User Name	string	64
url	URL	string	2048
vd	VDOM	string	32
vmos	Virtual Machine OS	string	128
jstatus	Job Status	string	16
malwarecategory	Malware category	string	256

NETATTACK

Log Field Name	Description	Data Type	Length
virusid	Virus ID	int32	32
attackid	Attack ID	int32	32
srcipport	source ip and port	string	48
dstipport	destination ip and port	string	48
host	Host name	string	256
attackname	Attack Name	string	128
botnetname	Botnet Name	string	128
jstatus	Job Status	string	16

NETBOTNET

Log Field Name	Description	Data Type	Length
devid	Device ID for FortiSandbox in FortiAnalyzer	string	16
logid	Log ID	string	8
type	Log Type	string	16
subtype	Log Subtype	string	32
level	Log Level	string	16
virusid	Virus ID	int32	32
attackid	Attack ID	int32	32
srcipport	source ip and port	string	48
dstipport	destination ip and port	string	48

Log Field Name	Description	Data Type	Length
host	Host name	string	256
attackname	Attack Name	string	128
botnetname	Botnet Name	string	128
vd	VDOM	string	32
jstatus	Job Status	string	16

NETURL

Log Field Name	Description	Data Type	Length
devid	Device ID for FortiSandbox in FortiAnalyzer	string	16
logid	Log ID	string	8
type	Log Type	string	16
subtype	Log Subtype	string	32
level	Log Level	string	16
virusid	Virus ID	int32	32
attackid	Attack ID	int32	32
srcipport	source ip and port	string	48
dstipport	destination ip and port	string	48
host	Host name	string	256
attackname	Attack Name	string	128
botnetname	Botnet Name	string	128
vd	VDOM	string	32
jstatus	Job Status	string	16

Event

SYSTEM

Log Field Name	Description	Data Type	Length
date	Date If the log server <code>type</code> is <code>Syslog</code> or <code>CEF</code> , the date is in UTC format.	string	16

Log Field Name	Description	Data Type	Length
	<p>If <code>type</code> is <code>FortiAnalyzer</code> or a local log, then it is the local date.</p> <p>In both cases, the <code>tz</code> and <code>tzzone</code> fields indicate the timezone of FortiSandbox.</p>		
time	<p>Time</p> <p>If the log server <code>type</code> is <code>Syslog</code> or <code>CEF</code>, the time is in UTC format.</p> <p>If <code>type</code> is <code>FortiAnalyzer</code> or a local log, then it is the local time.</p> <p>In both cases, the <code>tz</code> and <code>tzzone</code> fields indicate the timezone of FortiSandbox.</p>	string	16
tz	time zone abbreviation. e.g. PST, PDT	string	8
user	User Name	string	64
ui	User Interface	string	128
action	Action	string	64
status	Status	string	16
error	Error Message	string	128
reason	Reason	string	128
letype	sub of subcategory	uint8	8
admin	Admin User Name	string	128
blacklist	Blacklist Name	string	128
emailsndr	Email Sender	string	64
emailrcvr	Email Receiver	string	128
cloneidx	Virtual Machine Clone Index	uint32	32
jobcount	Job Count	uint32	32
device	FortiGate or other device name	string	16
dbid	DB Identifier	uint32	32
email	Email	string	128
etime	Finish Timestamp	uint32	32
rptfmt	Report Format	string	16
harole	HA Cluster Role Name	string	16
hostname	Hostname	string	128
index	Index	uint32	32

Log Field Name	Description	Data Type	Length
ip	IPv4 or IPv6 Address	string	45
jobtype	Job Type	string	64
snmpoid	SNMP Object ID	string	128
officekt	Office key type	string	32
os	OS Name	string	128
filepath	File Path	string	1024
pid	Process ID	uint32	32
pidstatus	Process Status	uint32	32
port	Interface Port	string	8
quarantine	Network Share Quarantine	string	128
rpttype	Report Type	string	8
retcode	Report return code	uint32	32
serial	Serial Number	string	16
from	Access From	string	32
sha1	SHA1 Checksum	string	41
subject	Email Subject	string	128
sharename	Network Share Name	string	256
sid	Job Submission ID	string	16
sizebin	Size of Binary	uint32	32
sizeconf	Size of Configuration	uint32	32
snmpaction	SNMP Action	string	128
stime	Start Timestamp	uint64	64
susr	Source User Name	string	64
urlcat	URL Category	string	64
version	Version	string	16
vmname	Virtual Machine Name	string	64
vmkey	Virtual Machine Key	string	16
whitelist	Whitelist Name	string	128
cip	Source IP	string	45
cport	Source Port	string	8

Log Field Name	Description	Data Type	Length
sip	Destination IP	string	45
sport	Destination Port	string	8
service	Service	string	32
ftype	File Type	string	64
rsrc	Submit Source	string	16
fcuid	FortiClient UID	string	32
unauthuser	Unauthorized User	string	66
unauthusersource	Unauthorized User Source	string	66
xforwarded	X-FORWARDED-FOR	string	128
trueclient	True Client IP	string	40
session_id	Email Session ID	string	64
mcate	Malware category	string	256
http_host	http hostname	string	256

PERFORMANCE

Log Field Name	Description	Data Type
pfdur	Performance Data Collecting Duration	
pfendtm	Performance Data Collecting End Time	
pftjob	Total Scanned Jobs	uint32
pftexe	Total EXE Jobs	uint32
pftpdf	Total PDF Jobs	uint32
pftoffice	Total Office Jobs	uint32
pftflash	Total Flash Jobs	
pftweb	Total Web Jobs	uint32
pftarch	Total Compressed Jobs	uint32
pftandroid	Total Android Jobs	uint32
pftmac	Total Mac Jobs	uint32
pftlinux	Total Linux Jobs	uint32
pfturl	Total URL Jobs	uint32
pftuser	Total User defined Jobs	uint32

Log Field Name	Description	Data Type
pfvjob	Total VM Scanned Jobs	uint32
pfvexe	VM EXE Jobs	uint32
pfvpdf	VM PDF Jobs	uint32
pfvoffice	VM Office Jobs	uint32
pfvflash	VM Flash Jobs	uint32
pfvweb	VM Web Jobs	uint32
pfvarch	VM Compressed Jobs	uint32
pfvandroid	VM Android Jobs	uint32
pfvmac	VM Mac Jobs	uint32
pfvlinux	VM Linux Jobs	uint32
pfvurl	VM URL Jobs	uint32
pfvuser	VM User defined Jobs	uint32
pfavgscantm	Average Scan Time	uint32
pfmedianscantm	Median Scan Time	uint32
pfmaxscantm	Max Scan Time	uint32
pfavgvmcantm	VM Scan Time	uint32
Pfmedianvmcantm	Median VM Scan Time	uint32
pfmaxvmcantm	Max VM Scan Time	uint32
pfavgwait	Average Wait Time	uint32
pfmedianwait	Median Wait Time	uint32
pfmaxwait	Max Wait Time	uint32
pfavgvmwait	Average VM Wait Time	uint32
pfmedianvmwait	Median VM Wait Time	uint32
pfmaxvmwait	Max VM Wait Time	uint32
pf0dayfile	0Day File	uint32
pf0dayurl	0Day URL File	uint32
pfmalfile	Malicious File	uint32
pfmalurl	Malicious URL File	uint32
pfai	AI Detected File	uint32
pfurl	Suspicious URL	uint32

RESOURCE

Field Name	Description	Data Type
cpu	CPU Usage	uint8
mem	Memory Usage	uint8
disk	HDD Disk Usage	uint8
ramdisk	Ram Disk Usage	uint8
vmdisk	VM Disk Usage	uint8
snifferbw	Sniffer Port Speed	uint64
pending	Pending Jobs	uint32

REPORT

Log Field Name	Description	Data Type	Length
rpttype	report type	enum	16
rptfmt	report format	enum	16
etime	finish timestamp	uint32	
stime	start timestamp	uint32	
fname	file name	string	1024
retcode	report return code	int32	

Change Log

Date	Change Description
2023-07-11	Initial release.



www.fortinet.com

Copyright© 2023 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.