Log Reference

FortiSandbox 5.0.0-5.0.4
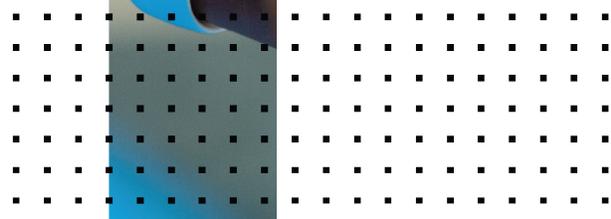
FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Introduction

This document provides information about all the log messages applicable to the FortiSandbox 5.0.0-5.0.4 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 5.0.0-5.0.4 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.

List of log types and subtypes

Type	Description	Subtype
event	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	• Unknown • Input Event • SNMP Event • HA Event • VM Event • Notification Event • Job Event • Threat Event • DB Event • System Event

Type	Description	Subtype
		• Report Event • Performance Event • Resource Event
malware	Records malware logs.	• Malware
netalert	Records netalert logs.	• Netattack • Netbotnet • Neturl

FortiSandbox priority levels

Level (0 is highest)	Name	Description
0	Emergency	The system is unusable or not responding.
1	Alert	Immediate action required. Used in security logs.
2	Critical	Functionality is affected.
3	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notice	Information about normal events.
6	Information	General information about system operations. Used in event logs to record configuration changes.
7	Debug	Extra information from system operations.

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 Information

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

FortiSandbox 5.0 Log Messages

The following tables list the FortiSandbox 5.0 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
scaned	Scan End Time	uint32	32
srcip	Source IP address	string	45
srcport	Source Port Number	int32	32

Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	string	45
dstport	Destination Port Number	int32	32
stype	Source Type	string	16
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

Log Field Name	Description	Data Type	Length
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

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
action	Action	string	64
admin	Admin User Name	string	128
blacklist	Blacklist Name	string	128
cip	Source IP	string	45
cloneidx	Virtual Machine Clone Index	uint32	32
cport	Source Port	string	8
date	Date If the log server type is Syslog or CEF, the date is in UTC format. If type is FortiAnalyzer or a local log, then it is the local date. In both cases, the tz and tzone fields indicate the timezone of FortiSandbox.	string	16
dbid	DB Identifier	uint32	32
device	FortiGate or other device name	string	16
email	Email	string	128
emailrcvr	Email Receiver	string	128
emailsndr	Email Sender	string	64
error	Error Message	string	128
etime	Finish Timestamp	uint32	32
fcuid	FortiClient UID	string	32
filepath	File Path	string	1024
from	Access From	string	32
ftype	File Type	string	64
harole	HA Cluster Role Name	string	16
hostname	Hostname	string	128
http_host	http hostname	string	256
index	Index	uint32	32

Log Field Name	Description	Data Type	Length
ip	IPv4 or IPv6 Address	string	45
jobcount	Job Count	uint32	32
jobtype	Job Type	string	64
letype	sub of subcategory	uint8	8
mcate	Malware category	string	256
md5	MD5 checksum	string	32
officekt	Office key type	string	32
os	OS Name	string	128
pid	Process ID	uint32	32
pidstatus	Process Status	uint32	32
port	Interface Port	string	8
quarantine	Network Share Quarantine	string	128
reason	Reason	string	128
retcode	Report return code	uint32	32
rptfmt	Report Format	string	16
rpttype	Report Type	string	8
rsrc	Submit Source	string	16
serial	Serial Number	string	16
service	Service	string	32
session_id	Email Session ID	string	64
sha1	SHA1 Checksum	string	41
sid	Job Submission ID	string	16
sip	Destination IP	string	45
sizebin	Size of Binary	uint32	32
sizeconf	Size of Configuration	uint32	32
snmpaction	SNMP Action	string	128
snmpoid	SNMP Object ID	string	128
sport	Destination Port	string	8
status	Status	string	16
stime	Start Timestamp	uint64	64

Log Field Name	Description	Data Type	Length	
subject	Email Subject	string	128	
susr	Source User Name	string	64	
time	Time If the log server type is Syslog or CEF, the time is in UTC format. If type is FortiAnalyzer or a local log, then it is the local time. In both cases, the tz and tzone fields indicate the timezone of FortiSandbox.	string	16	
trueclient	True Client IP	string	40	
tz	time zone abbreviation. e.g. PST, PDT	string	8	
ui	User Interface	string	128	
unauthuser	Unauthorized User	string	66	
unauthusersource	Unauthorized User Source	string	66	
urlcat	URL Category	string	64	
user	User Name	string	64	
version	Version	string	16	
vmkey	Virtual Machine Key	string	16	
vmname	Virtual Machine Name	string	64	
whitelist	Whitelist Name	string	128	
xforwarded	X-FORWARDED-FOR	string	128	
sha256	SHA256 checksum		string	64
url	URL		string	2048
fname	File Name		string	1024
office_version	Office version		string	32
clientvd	Client VDOM		string	64
share	Network Share		string	128
clientdev	Client Device		string	17
clientvd	Client VDOM		string	32
allowlist	Allowlist Names		string	128
blocklist	Blocklist Names		string	128
mname	Malware Name		string	256

Log Field Name	Description	Data Type	Length
proto	Protocol	string	16
stype	Source Type	string	16
vmos	Virtual Machine OS	string	128
fctuid	Forticlient ID	string	40

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
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

Log Field Name	Description	Data Type
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
pfavgvmscantm	VM Scan Time	uint32
Pfmedianvmscantm	Median VM Scan Time	uint32
pfmaxvmscantm	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
2024-11-29	Initial release.
2024-12-18	Updated Event on page 11.

FORTINET

www.fortinet.com