FORTINET
High Performance Network Security

FortiSandbox - Log Reference

VERSION 2.4.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

June 22, 2017

FortiSandbox 2.4.1 Log Reference

34-240-414841-20170622

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-06-22	Updated for 2.4.1 release.

Introduction

This document provides information about all the log messages applicable to the FortiSandbox 2.4.1 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, please see the *FortiSandbox 2.4.1 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 2.4 Log Messages

The following tables list the FortiSandbox 2.4 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
scaned	Scan End Time	uint32	32

Log Field Name	Description	Data Type	Length
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
suser	Source User Name	string	64
url	URL	string	2048
vd	VDOM	string	32
vmos	Virtual Machine OS	string	64

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

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

Log Field Name	Description	Data Type	Length
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

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

Log Field Name	Description	Data Type	Length
botnetname	Botnet Name	string	128
vd	VDOM	string	32

Event

SYSTEM

Log Field Name	Description	Data Type	Length
date	Date	string	16
time	Time	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

Log Field Name	Description	Data Type	Length
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
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	32
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

Log Field Name	Description	Data Type	Length
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
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

FORTINET®

High Performance Network Security