FortiSandbox - Log Reference

Version 2.5.1

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

January 17, 2017
FortiSandbox 2.5.1 Log Reference
34-251-414841-20180117

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-01-17	Initial release.

Introduction

This document provides information about all the log messages applicable to the FortiSandbox 2.5.1 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 2.5.1 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 2.5 Log Messages

The following tables list the FortiSandbox 2.5 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
dstip	Destination IP Address	string	45

Log Field Name	Description	Data Type	Length
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

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

Log Field Name	Description	Data Type	Length
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
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
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

Log Field Name	Description	Data Type	Length
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

Log Field Name	Description	Data Type	Length
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

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

Index

Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.