

FortiSandbox - Log Reference

Version 3.1.0

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



June 18, 2019

FortiSandbox 3.1.0 Log Reference

34-310-548349-20190618

TABLE OF CONTENTS

| | |
|--|-----------|
| Introduction | 4 |
| Log Information | 5 |
| Log Types | 5 |
| Type | 5 |
| Subtype | 5 |
| Log Field | 5 |
| FortiSandbox 3.1 Log Messages | 6 |
| Alert | 6 |
| MALWARE | 6 |
| NETATTACK | 7 |
| NETBOTNET | 7 |
| NETURL | 8 |
| Event | 8 |
| SYSTEM | 8 |
| Change Log | 12 |

Introduction

This document provides information about all the log messages applicable to the FortiSandbox 3.1.0 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, please see the [FortiSandbox 3.1.0 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 3.1 Log Messages

The following tables list the FortiSandbox 3.1 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 |

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 |
| host | Host name | string | 256 |

| Log Field Name | Description | Data Type | Length |
|----------------|-------------|-----------|--------|
| 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 |

| Log Field Name | Description | Data Type | Length |
|----------------|--------------------------------|-----------|--------|
| 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 |
| 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 |

| Log Field Name | Description | Data Type | Length |
|------------------|--------------------------|-----------|--------|
| 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 |
| urcat | 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 |

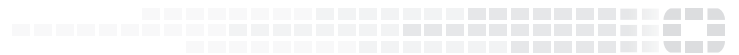
| Log Field Name | Description | Data Type | Length |
|----------------|------------------|-----------|--------|
| trueclient | True Client IP | string | 40 |
| session_id | Email Session ID | string | 64 |

Change Log

| Date | Change Description |
|------------|--------------------|
| 2019-06-18 | Initial release. |
| | |
| | |
| | |



FORTINET[®]



Copyright© 2019 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.