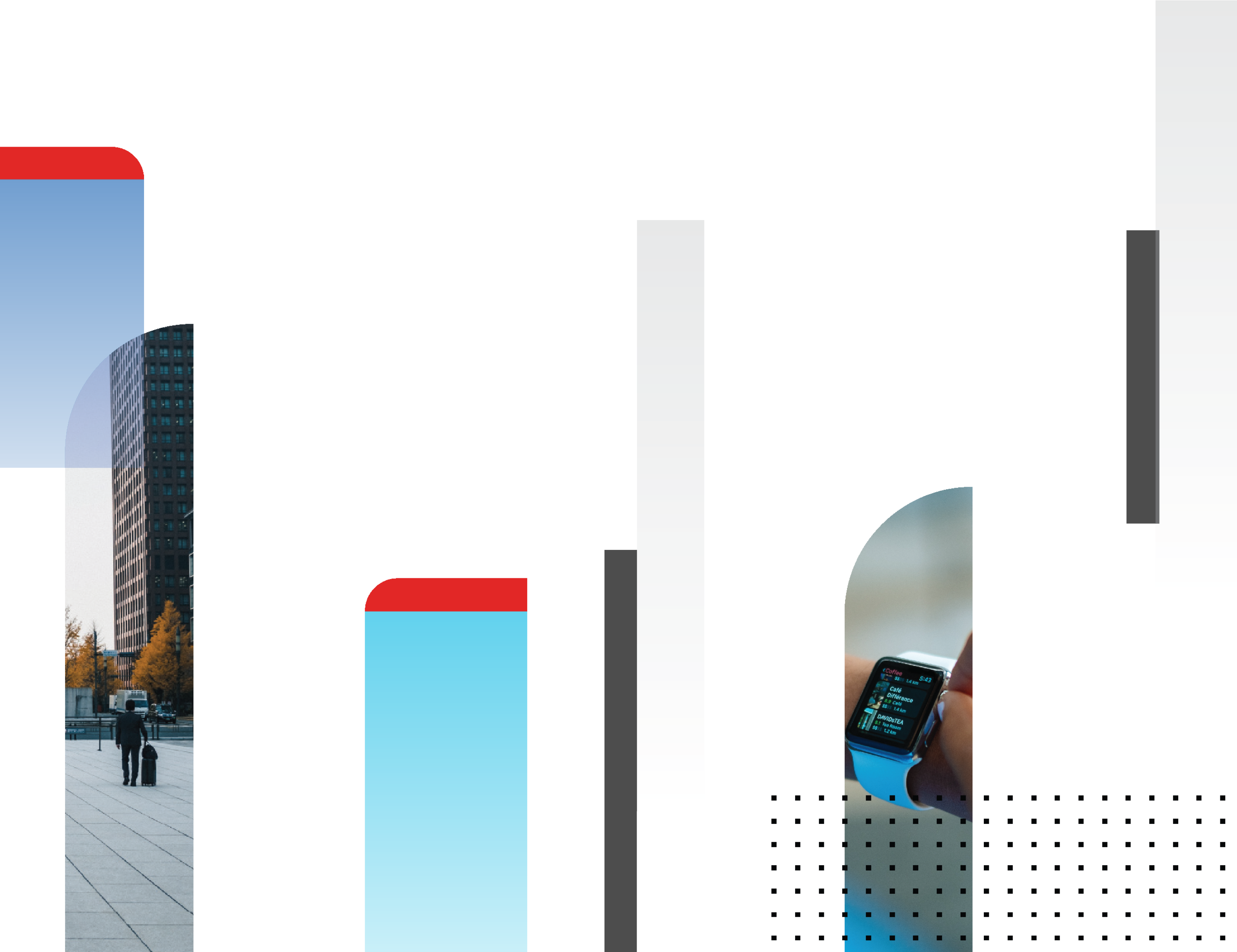
Log Message Reference

FortiDeceptor 5.0.0



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

NSE 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

March 1, 2023
FortiDeceptor 5.0.0 Log Message Reference
55-500-877430-20230301

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-01	Initial release.

Introduction

This reference provides detailed information about FortiDeceptor log messages. Log messages provide an audit log of actions made by users of FortiDeceptor units. The information in this document is useful for system administrators when recording, monitoring, and tracing the operation of FortiDeceptor units.

Regular event

```
EventID=2999850772968973605 IncidentID=2999783180299782560
     Tagkey=10.11.4.24:27149:10.11.4.21:445:2999677334472857190-066b950c-9c93-11ed-ba4f-
     52d7cbdbef3e DecoyGroup=IT_Decoy DecoyType=Windows11 AttackerIP=10.11.4.24
     AttackerPort=27149 VictimIP=10.11.4.21 VictimPort=445 Operation=Logoff_via_net_share
     Service=SMB Username=NA Password=NA Description="User karl SMB Logoff"
```

Log Field Name	Description	Data Type
AttackerIP	Event source ip	string
AttackerPort	Event source port	int
DecoyGroup	Decoy group name	string
DecoyType	Decoy OS type	string
Description	Extra information for event, for example, ssh command, file changes, etc	string
EventID	Event id	int
IncidentID	Incident id	int
Operation	Event operation	string
Password	Password used to attack the decoy	string
Service	Event service, for example, samba, ssh	string
Tagkey	Key used to group events into incident	string
Username	The username used to attack decoy	string
VictimIP	Event destination ip	string
VictimPort	Event destination port	int

IPS web filtering event

```
EventID=3001014396436619828 IncidentID=3001014743178499216
     Tagkey=10.11.4.27:62677:172.16.69.18:80:3000982640374151870-f4841228-9d39-11ed-bce7-
     523d411b9405 DecoyGroup=IT_Decoy DecoyType=Windows10 AttackerIP=10.11.4.27
     AttackerPort=62677 VictimIP=172.16.69.18 VictimPort=80 Operation=FortiGuard_Web_
     Filtering Host=172.16.69.18 URL=/sample/eicar.tgz
     Description="172.16.69.18/sample/eicar.tgz" Category=Unknown
```

Log Field Name	Description	Data Type
AttackerIP	Event source ip	string
AttackerPort	Event source port	int
Category	Category name	string
DecoyGroup	Decoy group name	string
DecoyType	Decoy OS type	string
Description	Extra information about the event. For example, ssh command, file changes, etc.	string
EventID	Event id	int
Host	Host IP	string
IncidentID	Incident id	int
Operation	Event operation	string
Tagkey	Key used to group events into incident	string
URL	The URL used to log in to the decoy and browse the endpoint.	string
VictimIP	Event destination ip	string
VictimPort	Event destination port	int

ips attack event

```
EventID=3011256137575066658 IncidentID=3011256354125025046
     Tagkey=10.11.4.26:50226:10.11.4.27:25:3000982640374151870-66b6bb70-a213-11ed-af92-
     52201c5a5c62 DecoyGroup=IT_Decoy DecoyType=Windows10 AttackerIP=10.11.4.26
     AttackerPort=50226 VictimIP=10.11.4.27 VictimPort=25 Operation=SMTP_Disconnect
     Service=SMTP Username=NA Password=NA Description="disconnect"
EventID=3011251782973974539 IncidentID=3011251971142112465
     Tagkey=10.11.4.26:38658:10.11.4.27:3389:3000982640374151870-cedbe696-a212-11ed-a422-
     52201c5a5c62 DecoyGroup=IT_Decoy DecoyType=Windows10 AttackerIP=10.11.4.26
     AttackerPort=38658 VictimIP=10.11.4.27 VictimPort=3389 Operation=IPS_attack
     Attack=tools: Nmap.Script.Scanner (#1 in pkt 5754) Description="tools:
     Nmap.Script.Scanner (#1 in pkt 5754)"
```

Log Field Name	Description	Data Type
Attack	Attack name This field may not appear in every log.	string
AttackerIP	Event source ip	string
AttackerPort	Event source port	int
DecoyGroup	Decoy group name	string
DecoyType	Decoy OS type	string
Description	Extra detail	string
eventID	Event id	int
incidentID	Incident id	int
Operation	Event operation	string
Password	Password used to attack the decoy This field may not appear in every log.	string
Service	Event service, for example, samba, ssh This field may not appear in every log.	string
Tagkey	Key used to group events into incident	string
Username	The username used to attack decoy This field may not appear in every log.	string
VictimIP	Event destination ip	string
VictimPort	Event destination port	int

nmap attack event

Example of scan of all ports with nmap, and TCP:

```
EventID=3011388922094660568 IncidentID=3011389064053784202
     Tagkey=10.11.4.26:39512:10.11.4.27:11110:3000982640374151870-15ec7092-a2b8-11ed-b46b-
     52201c5a5c62 DecoyGroup=IT_Decoy DecoyType=Windows10 AttackerIP=10.11.4.26
     AttackerPort=39512 VictimIP=10.11.4.27 VictimPort=11110 Operation=Disconnect_TCP_
     connection Service=TCPListener Username=NA Password=NA Description="Disconnection"
```

Example of port scanning:

```
Operation=Port_Scan AttackerIP=10.12.4.1 VictimIP=10.12.4.21 Description="Port.Scanning"
```

Log Field Name	Description	Data Type
Operation	Operation name	string
AttackerIP	Attacker ip address	string
VictimIP	Victim ip address	string
Description	Attack detail	string

Raw Elog Format

```
Sample {"logid": 3003761664159323711, "msg": "{\"protocol\": 10, \"dport\": 22, \"unique_
id\": \"9dad1304-9e6a-11ed-9c13-5253c2c5478a\", \"service\": 100, \"logtype\": 1, \"service_
name\": \"SSH\", \"optype\": 103, \"trapid\": 3003737929141591102, \"dip\": \"10.95.6.10\",
\"compromised\": true, \"timestamp\": 1212, \"sip\": \"10.95.6.11\", \"version\": 1,
\"instance_id\": \"3003737905335958931\", \"gateway\": \"10.95.6.1\", \"direction\": 0,
\"sport\": 48070, \"tagkey\": \"10.95.6.11-48070\",  \"netmask\": \"255.255.255.0\"}",
"trapid": "3003737929141591102", "sn": "FDC-VM0000069086", "caddr": "10.254.254.10"}
```

```
{"sn":"FDC-VMTM21000123", "logid":2981810861599983867, "caddr":null,
"trapid":2948983245847949350, "instance_id":2948983232583473085, "msg":"
{\"sip\":\"10.10.1.117\", \"sport\":null, \"dip\":\"255.255.255.255\", \"dport\":null,
\"optype\":20401, \"log_type\":0, \"timestamp\":1673564235, \"protocol\":239,
\"vifname\":\"bp2\", \"vlanid\":0, \"service\":2600,\"service_name\":\"ARP\", \"sn\":\"FDC-
VMTM21000123\", \"trapid\":2948983245847949350, \"instance_id\":2948983232583473085,
\"desc\":\"The MAC address for 10.10.1.117 flipflopped: 52:4A:DF:AC:C1:DE and
52:0E:D2:51:15:99\"}"}
```

Log Field Name	Description	Data Type
Logid	Log ID	int
msg	event detail	map
trapid	Trap ID	int/string
sn	Fortideceptor Serial Number	string
caddr	callback server ip address	string

Message content table

Msg field name	Description	Data type
protocol	Event protocol	int
dport	Destination port	int
unique_id	Unique id	string
service	raw coding, will be translated to services you see on GUI	int
logtype	Log type number	int
service_name	Name of service	string
optype	Event action type	int
log_type	Type of log	int
trapid	Decoy id	int
dip	Destination IP	string

Msg field name	Description	Data type
compromised	Has decoy been attacked	bool
timestamp	Time stamp	int
sip	Source IP	int
version	Log format version	int
instance_id	Vm instance id	string/int
gateway	Gateway ip	stirng
direction	traffic inbound or outbound	int
sport	Source port	int
tagkey	Key for event grouping	string
unique_id	Key for event grouping/addition to tagkey	string
netmask	netmask	string
desc	Event detail, will show on gui	string

Login/ Logout GUI

```
Administrator {username} logged into website successfully from {ip} by username and
     password.
Administrator {username} logged out website successfully from {ip}
Session timeout, administrator admin logged out from {ip}.
```

Example:

```
Administrator admin logged into website successfully from 172.16.197.157 by username and
     password.
Administrator admin logged out website successfully from 172.19.161.86
Session timeout, administrator admin logged out from 172.16.198.217.
```

Login/ Logout CLI

```
Administrator {username} logged into CLI successfully from {method} ({ip}).
Administrator {username} logged out CLI successfully from {method} ({ip}).
```

Example:

```
Administrator admin logged into CLI successfully from ssh(172.16.198.69).
Administrator admin logged out CLI successfully from telnet(127.0.0.1).
```

Deploy Decoy

```
Successfully operated on the following decoy(s): {decoy name}
Decoy {decoy name} was successfully deployed.
Generate lures successfully for services {service names}
Save the config for lure generator successfully.
```

Examples:

```
Successfully operated on the following decoy(s): test7
Decoy test7 was successfully deployed.
Generate lures successfully for services rdp, smb, smtp, ftp_v3 of OS win7x64v1.
Save the config for lure generator successfully.
```

Edit Dashboard

```
{Widget name} was created/deleted with id {id number} in dashboard.
Widget {widget name} was updated with {id number}.
Dashboard layout successfully reset.
```

Examples:

```
Incidents & Events Distribution was created with id 9 in dashboard.
Incidents & Events Count was deleted with id 7 in dashboard.
Widget Top 10 Attackers by Events was updated with id 10.
Dashboard layout successfully reset.
```

Mail

Mail server set

```
Mail Server config successfully saved.
Mail Server config has been successfully reset
Examples:
Mail Server config successfully saved.
Mail Server config has been successfully reset.
```

Send test email

```
Test email was sent out. Please check your mail box.
Failed to send out test email: Failed to send email, error=[error number] Connection
     refused.
```

Example:

```
Test email was sent out. Please check your mail box.
Failed to send out test email: Failed to send email, error=[Errno 111] Connection refused.
```

Add or update email alert rule

This log format shows the rule name and when the rule has been saved, updated or deleted.

```
{rule name} mail alert rule has been saved.
{rule name} mail alert rule has been updated.
{rule name} ip mail alert rule has been deleted
```

Examples:

```
newnewnew mail alert rule has been saved.
content mail alert rule has been updated.
content mail alert rule has been deleted.
```

Reminder email

The log shows:

1. When an incident occurs and which rule it matches.
   `Incident {incident ID} match with the rule [u'rule name1', u'rule name2', u'rule name3']`
2. The rule that triggered the email and the email address it was sent to.
   `Sent email to [u'{receiver email address}'], triggerred by {email alter rule name}`

Examples:

```
Incident 3012970260036983659 match with the rule [u'newtest', u'newnew', u'newnewnew']
Sent email to [u'receiver1@fdc.net'], triggerred by http
```

Network config

```
The deployment network for PORT {portID} {VLAN Number} was created with address {IP address}
     successfully.
```

Examples:

```
The deployment network for PORT port2 VLAN 0 was created with address 10.10.4.191/24
     successfully.
```

Image Upload

```
Image file {file name} was uploaded successfully.
Debug image {file name} was uploaded successfully.
Firmware was successfully upgraded. System will reboot in a few seconds.
```

Examples:

```
Image file FDC_VM-v500-build0107-FORTINET.deb was uploaded successfully.
Debug image FDC_VM-v500-build0104-FORTINET-dbgcore.dbg was uploaded successfully
Firmware was successfully upgraded. System will reboot in a few seconds.
```

Fabric

```
Fabric configuration {name} was successfully created.
Fabric configuration was successfully deleted.
Fabric configuration was successfully .
```

Examples:

```
Fabric configuration fgtblocker1 was successfully created.
Fabric configuration was successfully deleted.
Fabric configuration was successfully .
```

Install or Customize OS

```
Successfully initialize VM, name: {name}
VM package {package name} was successfully installed
```

Examples:

```
Successfully initialize VM, name: cus_test
VM package outbreakv1 was successfully installed
```

Token

```
Package was generated successfully for token campaign: {name}
The Token Campaign for Name {name} was created by admin successfully.
The Token Deployment Status was retrieved successfully.
The token package for campaign Name {name} was retrieved successfully.
```

Example:

```
Package was generated successfully for token campaign: moxaoffline
The Token Campaign for Name moxaoffline was created by admin successfully.
The Token Deployment Status was retrieved successfully. =
The token package for campaign Name moxaoffline was retrieved successfully.
```

Operations

```
Table View Settings were updated successfully.
```

```
DNS configuration was successfully updated
Routing configuration was deleted
```

```
Disclaimer message was updated successfully.
```

```
Remote log server was successfully added
Remote log server information was successfully updated
```

```
Package was generated successfully for token campaign: {name}
The Token Campaign for Name {name} was created by admin successfully.
The Token Deployment Status was retrieved successfully.
The token package for campaign Name {name} was retrieved successfully.
```

www.fortinet.com