TREND MICRO

6.1 Deep Discovery™ Analyzer

Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

Document Part No.: APEM68236/180418

Release Date: July 2018

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Preface

Preface iii

Documentation iv

Audience v

Document Conventions v

About Trend Micro vi

Chapter 1: Introduction

Terminology 1-2

Events 1-2

Version History 1-3

Chapter 2: Syslog Content Mapping - CEF

CEF Virtual Analyzer Analysis Logs: File Analysis Events 2-2

CEF Virtual Analyzer Analysis Logs: URL Analysis Events 2-4

CEF Integrated Product Detection Logs: Detection Results Events 2-6

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events 2-10

CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events .. 2-12

CEF System Event Logs 2-14

CEF Alert Event Logs 2-15

Chapter 3: Syslog Content Mapping - LEEF

LEEF Virtual Analyzer Analysis Logs: File Analysis Events 3-2

LEEF Virtual Analyzer Analysis Logs: URL Analysis Events 3-4

LEEF Integrated Product Detection Logs: Detection Results Events .. 3-6

LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events 3-9

LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events 3-11

LEEF System Events Logs 3-13

LEEF Alert Event Logs 3-14

Chapter 4: Syslog Content Mapping - TMEF

TMEF Virtual Analyzer Analysis Logs: File Analysis Events 4-2

TMEF Virtual Analyzer Analysis Logs: URL Analysis Events 4-4

TMEF Integrated Product Detection Logs: Detection Results Events 4-6

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events 4-10

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events 4-12

TMEF System Event Logs 4-14

TMEF Alert Event Logs 4-15

Index

Index IN-1

Preface

Preface

Learn more about the following topics:

- *Documentation on page iv*
- *Audience on page v*
- *Document Conventions on page v*
- *About Trend Micro on page vi*

Documentation

The documentation set for Deep Discovery Analyzer includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Analyzer, and explanations on Deep Discovery Analyzer concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Analyzer.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Analyzer to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.

Document	Description
Online Help	Web-based documentation that is accessible from the Deep Discovery Analyzer management console. The Online Help contains explanations of Deep Discovery Analyzer components and features, as well as procedures needed to configure Deep Discovery Analyzer.
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: http://esupport.trendmicro.com

View and download product documentation from the Trend Micro Online Help Center:

http://docs.trendmicro.com/en-us/home.aspx

Audience

The Deep Discovery Analyzer documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
 **Note**	Configuration notes
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Chapter 1

Introduction

The Deep Discovery Analyzer Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Trend Micro Deep Discovery Analyzer.

To enable flexible integration with third-party log management systems, Deep Discovery Analyzer supports the following syslog formats:

Log Management System	Description
Common Event Format (CEF) For details, see *Syslog Content Mapping - CEF on page 2-1*	CEF is an open log management standard created by HP ArcSight. Deep Discovery Analyzer uses a subset of the CEF dictionary.
Log Event Extended Format (LEEF) For details, see *Syslog Content Mapping - LEEF on page 3-1*	LEEF is an event format developed for IBM Security QRadar. Deep Discovery Analyzer uses a subset of the LEEF dictionary.
Trend Micro Event Format (TMEF) For details, see *Syslog Content Mapping - TMEF on page 4-1*	TMEF is a superset of log fields that allow a third-party syslog collector to better control and mitigate detection events provided by Deep Discovery Analyzer.

Terminology

TERM	DESCRIPTION
CEF	Common Event Format
LEEF	Log Event Extended Format
TMEF	Trend Micro Event Format

Events

Trend Micro Deep Discovery Analyzer supports the following events:

TABLE 1-1. Supported Events

EVENT NAME	EVENT DESCRIPTION
Virtual Analyzer Analysis Logs: File Analysis Events	File analysis events from Virtual Analyzer.
Virtual Analyzer Analysis Logs: URL Analysis Events	URL analysis events from Virtual Analyzer.
Integrated Product Detection Logs: Detection Results Events	Detections from integrated products, like Deep Discovery Inspector or IWSVA.
Virtual Analyzer Analysis Logs: Notable Characteristics Events	Notable characteristics from Virtual Analyzer results.
Virtual Analyzer Analysis Logs: Deny List Transaction Events	Suspicious objects from Virtual Analyzer results.
System Event Logs	Event logs generated by the system.
Alert Event Logs	Event logs generated by alerts.

Version History

TABLE 1-2. Deep Discovery Analyzer Version History

VERSION	REVISIONS
5.5	Initial version
5.5 SP1	Added **Integrated Product Detection Logs: Detection Results Events**
6.0	• Added **System Event Logs** • Added **Alert Event Logs** • Updated value of `deviceDirection` for **ICAP protocol** for **Integrated Product Detection Logs: Detection Results Events**

Chapter 2

Syslog Content Mapping - CEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and CEF syslog types:

- *CEF Virtual Analyzer Analysis Logs: File Analysis Events on page 2-2*
- *CEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 2-4*
- *CEF Integrated Product Detection Logs: Detection Results Events on page 2-6*
- *CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 2-10*
- *CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 2-12*
- *CEF System Event Logs on page 2-14*
- *CEF Alert Event Logs on page 2-15*

CEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 2-1. CEF Virtual Analyzer Analysis Logs: File Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200119
Header (eventName)	Description	Sample file sandbox analysis is finished
Header (severity)	Severity	3: Informational
cn1	Result of GRID/CSSS	• -1: GRID is unknown • 0: GRID is not known good • 1: GRID is known good
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.

CEF Key	Description	Value
cn2Label	ROZ rating (Virtual Analyzer internal code for analysis results)	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
cs2	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	Malware name	MalwareName
cs3	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
cs3Label	Parent SHA1	ParentFileSHA1
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

CEF KEY	DESCRIPTION	VALUE
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
19|Sample file sandbox analysis is finished|3|rt=Feb 27 20
15 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=DDAN dvcm
ac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B
527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe fileHash=C
F1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN32 EXE
 fsize=117248 cs1Label=SandboxImageType cs1=win8 cs3Label=
ParentFileSHA1 cs3=FF47AEE003778AA51E0326F53EF235C96D71D7C
A cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3
 cs2Label=MalwareName cs2=TSPY_FAREIT.WT cn3Label=PcapRead
y cn3=1
```

CEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 2-2. CEF Virtual Analyzer Analysis Logs: URL Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL sandbox analysis is finished
Header (severity)	Severity	3: Informational

CEF Key	Description	Value
cn2	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.
cn2Label	ROZ rating (Virtual Analyzer internal code for analysis results)	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

CEF KEY	DESCRIPTION	VALUE
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
26|URL sandbox analysis is finished|3|rt=Feb 27 2015 09:3
6:26 GMT+00:00 dvc=10.204.191.249 dvchost=DDAN dvcmac=EC:
F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B527-A
BCB84FDAC83 request=http://www.baidu.com:80/ fileHash=ACB
5175554463DD2ADBDFF78AD82C7D6BB8C8B6B cs1Label=SandboxIma
geType cs1=win8 cn2Label=ROZRating cn2=0 cn3Label=PcapRea
dy cn3=1
```

CEF Integrated Product Detection Logs: Detection Results Events

TABLE 2-3. CEF Integrated Product Detection Logs: Detection Results Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200128
Header (eventName)	Description	SUBMISSION_ANALYZED

CEF Key	Description	Value
Header (severity)	Deep Discovery Analyzer risk level mapping:	• 1: Unrated • 2: No risk • 4: Low • 6: Medium • 8: High
app	Application protocol	Example: FTP/HTTPS/MSN/...
c6a2	Source IPv6 address	Example: 2001:db8::1
c6a2Label	Source IPv6 address	srcIPv6
c6a3	Destination IPv6 address	Example: 2001:db8:a0b:12f0::1
c6a3Label	Destination IPv6 address	dstIPv6
cn1	Sample type	• 0: File sample • 1: URL sample
cn1Label	Sample type	sampleType
cs1	Malware name	Example: HEUR_NAMETRICK.A
cs1Label	Malware name	malName
cs2	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	Email ID	messageId
cs3	Application protocol group	Example: SMTP/HTTP/…
cs3Label	Application protocol group	appGroup
cs4	Submitter	Example: Deep Discovery Inspector
cs4Label	Submitter	submitter

CEF Key	Description	Value
cs5	Submitter host name	Example: shost1
cs5Label	Submitter host name	submitterName
deviceDirection	Associated direction	For ICAP protocol: • 0: ICAP REQMOD • 1: ICAP RESPMOD For other protocols: • 0: inbound • 1: outbound • 2: unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceProcessName	Appliance process name	Example: explorer.exe
dhost	Destination host name	Example: dhost1
dmac	Destination MAC address	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 0 and 65535
dst	Destination IPv4 address	Example: 10.1.144.199
duser	Email recipients	Example: user1@domain2.com;test@163.com
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

CEF Key	Description	Value
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Email subject	Example: hello
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
requestClientApplication	User agent	Example: IE
rt	Event generation time at submitter	Example: Mar 09 2015 17:05:21 GMT+08:00
shost	Source host name	Example: shost1
smac	Source MAC address	Example: 00:0C:29:6E:CB:F9
spt	Source port	Value between 0 and 65535
src	Source IPv4 address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.1.1034|20012
8|SUBMISSION_ANALYZED|1|rt=May 06 2016 14:34:29 GMT+08:00
dvc=192.168.1.1 dvchost=DDAN-Active dvcmac=B8:CA:3A:68:2F:
CC deviceExternalId=F8E649AA-AF79-4545-9B5A-580BA993D5E3 s
rc=192.168.14.59 spt=20819 smac=98:90:96:CA:78:1F shost=nj
-host1 dst=106.120.188.47 dpt=80 dmac=00:00:0C:9F:F0:0E dh
ost=106.120.188.47 cn1Label=sampleType cn1=0 fname=sgim_us
rzoneext.zip fsize=692 fileType=PKZIP fileHash=9D49696A96D
B224F7E884146D801DD8C828D17BF request=http://pc.profile.pi
nyin.sogou.com/upload.php?hid\\\=sgpy-windows-generic-devi
ce-id&v\\\=7.9.0.7504&brand\\\=1&platform\\\=1&ifbak\\\=1&
ifmobile\\\=0&ifauto\\\=0&filename\\\=sgim_usrzoneext.zip&
```

```
m\\\=ACB0BDECEF76784CD482133A068241B7 app=HTTP cs3Label=ap
pGroup cs3=HTTP cs4Label=submitter cs4=Deep Discovery Insp
ector cs5Label=submitterName cs5=TEST-DDI deviceDirection=
1 requestClientApplication=sogou_ime/7.9.0.7504
```

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 2-4. CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200127
Header (eventName)	Description	Notable Characteristics of the analyzed sample
Header (severity)	Severity	6: Warning
cs1	Violated policy name	Example: Internet Explorer Setting Modification
cs1Label	Violated policy name	PolicyCategory
cs2	Violated event analysis	Example: Modified important registry items
cs2Label	Violated event analysis	PolicyName
cs3	Sandbox image type	Example: win7
cs3Label	Sandbox image type	SandboxImageType

CEF Key	Description	Value
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: Source: ATSE \nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.1246\nMalware Pattern Version: 11.501.90
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
27|Notable Characteristics of the analyzed sample|6|rt=Feb
 27 2015 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=DDA
N dvcmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-
4B8A-B527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe file
Hash=CF1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN
32 EXE fsize=117248 cs1Label=PolicyCategory cs1=Malformed,
 defective, or with known malware traits msg=Source: ATSE\
nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.124
6\nMalware Pattern Version: 11.501.90 cs2Label=PolicyName
cs2=Detected as known malware
```

CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 2-5. CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3: Informational
act	The action in the event	• Add • Remove
cs1	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Deny List type	type
cs2	Risk level	• Low • Medium • High • Confirmed Malware
cs2Label	Risk level	RiskLevel

CEF Key	Description	Value
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IPv4 address	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
end	Deny List expired time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
20|Deny List updated|3|rt=Feb 27 2015 09:49:41 GMT+00:00 d
vc=10.204.191.249 dvchost=DDAN dvcmac=EC:F4:BB:C6:F1:D0 de
viceExternalId=758B04C9-F577-4B8A-B527-ABCB84FDAC83  cs1La
bel=type cs1=Deny List File SHA1 end=Mar 29 2015 09:49:06
GMT+00:00 act=Add fileHash=CF1A6CF231BDA185DEBF70B85623017
98F286FAD cs2Label=RiskLevel cs2=High
```

CEF System Event Logs

TABLE 2-6. CEF System Event Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001
Header (eventid)	Event ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	Description	Example:Updates: Component update settings modified by 'admin' from 192.168.10.2.
Header (severity)	Severity	3: Informational
dvc	Appliance IP address	Example: IPV4: 192.168.10.1
devmac	Appliance Mac address	Example: 00:0D:60:AF:1B:61
dvchost	Appliance host name	Example: DDAN
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time	Example: Mar 03 2016 16:28:20 GMT+08:00
cs1Label	Event type label	eventType
cs1	Event type	Example: Account Logon/Logoff
duser	User name	Example: admin
src	Source IPv4 address	Example: IPV4:192.168.10.1

CEF KEY	DESCRIPTION	VALUE
c6a2Label	Source IPv6 address label	srcIPv6
c6a2	Source IPv6 address	Example: 2620:0101:4002:0401::131
shost	Source host name	Example: shost1
outcome	Result status	• Success • Failure

Log sample:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|3009
99|Log Settings: Settings modified by 'admin' from 10.204.
1.2|3|rt=Nov 07 2017 10:05:58 GMT+00:00 dvc=10.204.1.1 dvc
host=DDAN dvcmac=00:0C:29:2F:3B:6B deviceExternalId=423E63A
A-D466-406E-A15F-6AC6F3CEE50A cs1Label=eventType cs1=System
Setting duser=admin src=10.204.1.2 outcome=Success
```

CEF Alert Event Logs

TABLE 2-7. CEF Alert Event Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001
Header (eventid)	Event ID	300105
Header (eventName)	Description	ALERT_EVENT

CEF KEY	DESCRIPTION	VALUE
Header (severity)	Severity	• 2: Informational • 6: Important • 8: Critical
dvc	Appliance IP address	Example: • IPV4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
devmac	Appliance MAC address	Example:00:0D:60:AF:1B:61
dvchost	Appliance host name	Example: DDAN
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Event logged	Example: Mar 03 2016 16:28:20 GMT+08:00
cs1Label	Rule name label	"ruleName"
cs1	Rule name	Example: High Memory Usage
cs2Label	Affected Appliance label	"affectedAppliance"
cs2	Affected Appliance	Example: DDAN.com (10.204.1.2 | FE80:: 29FF:29FF: 29FF: 29FF)
cs3Label	Subject label	"subject"
cs3	Subject	Example: DDAN Important Alert - High Memory Usage
cs4Label	Message label	"ruleContent"
cs4	Message	Message content

Log sample:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300105
|ALERT_EVENT|6|rt=Nov 07 2017 08:39:54 GMT+00:00 dvc=10.204.
1.1 dvchost=DDAN dvcmac=00:0C:29:2F:3B:6B deviceExternalId=4
23E63AA-D466-406E-A15F-6AC6F3CEE50A cs1Label=ruleName cs1=Hi
gh CPU Usage cs2Label=affectedAppliance cs2=DDAN ( 10.204.19
1.1 | FE80::20C:29FF:FE2F:3011 ) cs3Label=subject cs3=DDAN I
mportant Alert - High CPU Usage cs4Label=ruleContent cs4=The
 average CPU usage in the last 5 minutes exceeded the thresh
old of 90%.\n\nAverage CPU usage: 96%\nAffected appliance: D
DAN (10.204.191.1 | FE80::20C:29FF:FE2F:3011)\n\nReduce the 
number of Virtual Analyzer instances, or add a secondary app
liance to improve performance.\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=
\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\nAlert time: 20
17-11-07 08:39:54\nManagement console: https://10.204.191.1/
 | https://[FE80::20C:29FF:FE2F:3011]/
```

Chapter 3

Syslog Content Mapping - LEEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and LEEF syslog types:

- *LEEF Virtual Analyzer Analysis Logs: File Analysis Events on page 3-2*
- *LEEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 3-4*
- *LEEF Integrated Product Detection Logs: Detection Results Events on page 3-6*
- *LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 3-9*
- *LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 3-11*
- *LEEF System Events Logs on page 3-13*
- *LEEF Alert Event Logs on page 3-14*

Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

LEEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 3-1. LEEF Virtual Analyzer Analysis Logs: File Analysis Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventName)	Event Name	FILE_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar

LEEF Key	Description	Value
fsize	File size	Example: 131372
gridIsKnownGood	Result of GRID/CSSS	• -1: GRID is unknown • 0: GRID is not known good • 1: GRID is known good
malName	Malware name	Example: HEUR_NAMETRICK.A
pcapReady	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.
sev	Severity	3: Informational

Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|FILE
_ANALYZED|devTime=Feb 28 2015 02:45:48 GMT+00:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009>
```

```
dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC:F
4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABCB84FD
AC83<009>fname=Invoice_06202013_QBK.exe<009>fileHash=CF1A6CF2
31BDA185DEBF70B8562301798F286FAD<009>deviceProcessHash=FF47AE
E003778AA51E0326F53EF235C96D71D7CA<009>malName=TSPY_FAREIT.WT
<009>fileType=WIN32 EXE<009>fsize=117248<009>deviceOSName=win
8<009>gridIsKnownGood=-1<009>rozRating=3<009>pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 3-2. LEEF Virtual Analyzer Analysis Logs: URL Analysis Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventName)	Event Name	URL_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

LEEF KEY	DESCRIPTION	VALUE
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pcapReady	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.
sev	Severity	3: Informational
url	URL	Example: http://1.2.3.4/query?term=value

Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|URL_
ANALYZED|devTime=Feb 27 2015 09:36:26 GMT+00:00<009>devTimeFo
rmat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009>d
vc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC:F4
:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABCB84FDA
```

```
C83<009>fileHash=ACB5175554463DD2ADBDFF78AD82C7D6BB8C8B6B<009
>deviceOSName=win8<009>url=http://www.baidu.com:80/<009>rozRa
ting=0<009>pcapReady=1
```

LEEF Integrated Product Detection Logs: Detection Results Events

TABLE 3-3. LEEF Integrated Product Detection Logs: Detection Results Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventName)	Description	SUBMISSION_ANALYZED
app	Application protocol	Example: FTP/HTTPS/MSN/...
appGroup	Application protocol group	Example: SMTP/HTTP/…
deviceDirection	Associated direction	For ICAP protocol: • 0: ICAP REQMOD • 1: ICAP RESPMOD For other protocols: • 0: inbound • 1: outbound • 2: unknown
deviceProcessName	Appliance process name	Example: explorer.exe
devTime	Event generation time at submitter	Example: Jan 28 2015 02:00:36 GMT+08:00

LEEF Key	Description	Value
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dhost	Destination host name	Example: dhost1
dst	Destination IPv4 address Destination IPv6 address	Example: 10.1.144.199 Example: 2001:db8:a0b:12f0::1
dstMAC	Destination MAC address	Example: 00:0C:29:6E:CB:F9
dstPort	Destination port	Value between 0 and 65535
duser	Email recipients	Example: user1@domain2.com;test@163.com
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
mailMsgSubject	Email subject	Example: hello
malName	Malware name	Example: HEUR_NAMETRICK.A
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>

LEEF KEY	DESCRIPTION	VALUE
requestClientApplication	User agent	Example: IE
sampleType	Sample type	• 0: File sample • 1: URL sample
sev	Deep Discovery Analyzer risk level mapping:	• 1: Unrated • 2: No risk • 4: Low • 6: Medium • 8: High
shost	Source host name	Example: shost1
src	Source IPv4 address Source IPv6 address	Example: 10.1.144.199 Example: 2001:db8::1
srcMAC	Source MAC address	Example: 00:0D:60:AF:1B:61
srcPort	Source port	Value between 0 and 65535
submitter	Submitter	Example: Deep Discovery Inspector
submitterName	Submitter host name	Example: shost1
suser	Email sender	Example: user2@domain.com
url	URL	Example: http://1.2.3.4/query?term=value

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.1.1034|SU
BMISSION_ANALYZED|devTime=May 06 2016 14:33:52 GMT+08:00<0
09>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=1<009>dvc=
192.168.1.1<009>dvchost=DDAN-Active<009>deviceMacAddress=B
8:CA:3A:68:2F:C0<009>deviceGUID=F8E649AA-AF79-4545-9B5A-58
0BA993D5E3<009>src=192.168.88.108<009>srcPort=40167<009>sr
```

```
cMAC=9C:99:A0:4B:7B:76<009>shost=android-e1b7f2d1e98eb838<
009>dst=42.62.93.35<009>dstPort=80<009>dstMAC=3C:61:04:96:
97:00<009>dhost=42.62.93.35<009>sampleType=0<009>fname=lla
.zip<009>fsize=423<009>fileType=PKZIP<009>fileHash=4511117
B782C243E01E830ED63BCBAB6B9BD111E<009>url=http://stat.moji
.com/aMoUp<009>app=HTTP<009>appGroup=HTTP<009>submitter=De
ep Discovery Inspector<009>submitterName=TEST-DDI<009>devi
ceDirection=1<009>requestClientApplication=Apache-HttpClie
nt/UNAVAILABLE (java 1.4)
```

LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 3-4. LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventName)	Event Name	NOTABLE_CHARACTERISTICS
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199

LEEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: Process ID: 884 \nFile: %TEMP%\~DF7A0C28F4D7D9E792.TMP \nType: VSDT_ERROR
pComp	Detection engine / component	Sandbox
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items
sev	Severity	6: Warning

Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|NOTA
BLE_CHARACTERISTICS|devTime=Feb 28 2015 02:46:33 GMT+00:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>pComp=Sa
ndbox<009>dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAd
dress=EC:F4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B52
7-ABCB84FDAC83<009>fname=a254i.doc<009>fileHash=7A75D6934C5CD
AAF6CA13F8FA4CA03E46DAA7623<009>fileType=Microsoft RTF<009>fs
ize=86016<009>ruleCategory=File drop, download, sharing, or r
```

```
eplication<009>ruleName=Deletes file to compromise the system
 or to remove traces of the infection<009>msg=Process ID: 884
\nFile: %TEMP%\~DF7A0C28F4D7D9E792.TMP\nType: VSDT_ERROR
```

LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 3-5. LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	• Add • Remove
deviceExternalRiskType	Risk level	• Low • Medium • High • Confirmed Malware
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z

LEEF KEY	DESCRIPTION	VALUE
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IPv4 address	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
sev	Severity	3: Informational
type	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
url	URL	Example: http://1.2.3.4/query?term=value

Note

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|DENY
LIST_CHANGE|devTime=Feb 28 2015 02:50:03 GMT+00:00<009>devTim
eFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<00
```

```
9>dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC
:F4:BB:C6:F1:D0<009> deviceGUID=758B04C9-F577-4B8A-B527-ABCB8
4FDAC83<009>end=Mar 30 2015 02:45:48 GMT+00:00<009>act=Add<00
9>fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD<009>devic
eExternalRiskType=High<009>type=Deny List File SHA1
```

LEEF System Events Logs

TABLE 3-6. LEEF System Events Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001
Header (eventName)	Event name	• PRODUCT_UPDATE • SYSTEM_EVENT
sev	Severity	3: Informational
dvc	Appliance IP address	Example: 192.168.10.1
deviceMacAddress	Appliance MAC address	Example:00:0D:60:AF:1B:61
dvchost	Appliance host name	Examples: DDAN
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Event logged	Example: Mar 03 2016 16:28:20 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z

LEEF KEY	DESCRIPTION	VALUE
eventType	Event type	• System Setting • Account Logon/Logoff • System Update
duser	User Name	Example: admin
msg	Details	Example:Updates: Component update settings modified by 'admin' from 10.64.54.159.
src	IPV4 /IPv6 source address	Example: 192.168.100.100
shost	Source hostname	Example: shost1
outcome	Result status	• Success • Failure

Log sample:

```
LEEF: 1.0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|SYS
TEM_EVENT|devTime=Nov 07 2017 10:08:30 GMT+00:00<009>devTime
Format=MMM dd yyyy HH:mm:ss z<009>sev=3<009>dvc=10.204.1.1<0
09>dvchost=DDAN<009>deviceMacAddress=00:0C:29:2F:3B:6B<009>d
eviceGUID=423E63AA-D466-406E-A15F-6AC6F3CEE50A<009>eventType
=System Setting<009>duser=admin<009>src=10.204.1.2<009>msg=L
og Settings: Settings modified by 'admin' from 10.204.1.2<00
9>outcome=Success
```

LEEF Alert Event Logs

TABLE 3-7. LEEF Alert Event Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	1.0

LEEF Key	Description	Value
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001
Header (eventName)	Event Name	ALERT_EVENT
sev	Severity	• 2: Informational • 6: Important • 8: Critical
dvc	Appliance IP address	Example: • IPV4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
deviceMacAddress	Appliance MAC address	Example: 00:0D:60:AF:1B:61
dvchost	Appliance host name	Example: DDAN
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Event logged	Example: Mar 03 2016 16:28:20 GMT+08:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
ruleName	Rule name	Example: High Memory Usage
affectedAppliance	Affected Appliance	Example: DDAN.com (10.204.1.1 | FE80:: 29FF:29FF: 29FF: 29FF)
subject	Subject	Example: DDAN Important Alert - High Memory Usage
ruleContent	Message	Message content

Log sample:

```
LEEF: 1.0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|ALE
RT_EVENT|devTime=Nov 07 2017 08:39:54 GMT+00:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>dvc=10.204.1.1<00
9>dvchost=DDAN<009>deviceMacAddress=00:0C:29:2F:3B:6B<009>de
viceGUID=423E63AA-D466-406E-A15F-6AC6F3CEE50A<009>ruleName=H
igh CPU Usage<009>affectedAppliance=DDAN ( 10.204.1.1 | FE80
::20C:29FF:FE2F:1B6B )<009>subject=DDAN Important Alert - Hi
gh CPU Usage<009>ruleContent=The average CPU usage in the la
st 5 minutes exceeded the threshold of 90%.\n\nAverage CPU u
sage: 96%\nAffected appliance: DDAN (10.204.1.1 | FE80::20C:
29FF:FE2F:1B6B)\n\nReduce the number of Virtual Analyzer ins
tances, or add a secondary appliance to improve performance.
\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=
\=\=\=\=\=\=\=\nAlert time: 2017-11-07 08:39:54\nManagement
console: https://10.204.1.1/ | https://[FE80::20C:29FF:FE2F:
1B6B]/
```

Chapter 4

Syslog Content Mapping - TMEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and TMEF syslog types:

- *TMEF Virtual Analyzer Analysis Logs: File Analysis Events on page 4-2*
- *TMEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 4-4*
- *TMEF Integrated Product Detection Logs: Detection Results Events on page 4-6*
- *TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 4-10*
- *TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 4-12*
- *TMEF System Event Logs on page 4-14*
- *TMEF Alert Event Logs on page 4-15*

TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 4-1. TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200119
Header (eventName)	Description	FILE_ANALYZED
Header (severity)	Severity	3: Informational
cn1	Result of GRID/CSSS	• -1: GRID is unknown • 0: GRID is not known good • 1: GRID is known good
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.

TMEF KEY	DESCRIPTION	VALUE
cn2Label	ROZ rating (Virtual Analyzer internal code for analysis results)	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
malName	Malware name	Example: HEUR_NAMETRICK.A
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
19|FILE_ANALYZED|3|rt=Jun 26 2015 05:29:57 GMT+00:00 pComp=
Sandbox dvc=10.204.70.173 dvchost=DDAN deviceMacAddress=00:
0C:29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19F
EF4 fname=Establishes_uncommon_connection fileHash=0C450F48
E48CEF0B161C254C9E57816CD20FA918 deviceProcessHash=A754E779
292F392AE7692D0D2A55D2ECB71B5332 malName=BKDR_NORAWEC.SMG f
ileType=UPX EXE fsize=149504 deviceOSName=fsdf cn1Label=GRI
DIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapR
eady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 4-2. TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL_ANALYZED
Header (severity)	Severity	3: Informational

TMEF KEY	DESCRIPTION	VALUE
cn2	ROZ rating (Virtual Analyzer internal code for analysis results)	• -1: Unsupported file type in ROZ • 0: No risk found • 1: Low risk • 2: Medium risk • 3: High risk **Note** Negative values always indicate errors.
cn2Label	ROZ rating (Virtual Analyzer internal code for analysis results)	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox

TMEF KEY	DESCRIPTION	VALUE
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
26|URL_ANALYZED|3|rt=Jun 26 2015 05:24:26 GMT+00:00 pComp=San
dbox dvc=10.104.70.173 dvchost=DDAN deviceMacAddress=00:0C:29
:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 req
uest=https://wx.qq.com:443/ fileHash=BA4AA53108D98F5195D1F490
D05716F0B6D7B7EA deviceOSName=fsdf cn2Label=ROZRating cn2=-14
 cn3Label=PcapReady cn3=0
```

TMEF Integrated Product Detection Logs: Detection Results Events

TABLE 4-3. TMEF Integrated Product Detection Logs: Detection Results Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200128
Header (eventName)	Description	SUBMISSION_ANALYZED

TMEF KEY	DESCRIPTION	VALUE
Header (severity)	Deep Discovery Analyzer risk level mapping:	• 1: Unrated • 2: No risk • 4: Low • 6: Medium • 8: High
app	Application protocol	Example: FTP/HTTPS/MSN/...
appGroup	Application protocol group	Example: SMTP/HTTP/…
c6a2	Source IPv6 address	Example: 2001:db8::1
c6a2Label	Source IPv6 address	srcIPv6
c6a3	Destination IPv6 address	Example: 2001:db8:a0b:12f0::1
c6a3Label	Destination IPv6 address	dstIPv6
cn1	Sample type	• 0: File sample • 1: URL sample
cn1Label	Sample type	sampleType
cs1	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs1Label	Email ID	messageId
cs2	Submitter	Example: Deep Discovery Inspector
cs2Label	Submitter	submitter
cs3	Submitter host name	Example: shost1
cs3Label	Submitter host name	submitterName

TMEF KEY	DESCRIPTION	VALUE
deviceDirection	Associated direction	For ICAP protocol: • 0: ICAP REQMOD • 1: ICAP RESPMOD For other protocols: • 0: inbound • 1: outbound • 2: unknown
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceProcessName	Appliance process name	Example: explorer.exe
dhost	Destination host name	Example: dhost1
dmac	Destination MAC address	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 0 and 65535
dst	Destination IPv4 address	Example: 10.1.144.199
duser	Email recipients	Example: user1@domain2.com;test@163.com
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar

TMEF Key	Description	Value
fsize	File size	Example: 131372
mailMsgSubject	Email subject	Example: hello
malName	Malware name	Example: HEUR_NAMETRICK.A
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
requestClientApplication	User agent	Example: IE
rt	Event generation time at submitter	Example: Mar 09 2015 17:05:21 GMT+08:00
shost	Source host name	Example: shost1
smac	Source MAC address	Example: 00:0C:29:6E:CB:F9
spt	Source port	Value between 0 and 65535
src	Source IPv4 address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.1.1034|20012
8|SUBMISSION_ANALYZED|1|rt=May 06 2016 09:03:17 GMT+08:00
dvc=192.168.1.1 dvchost=DDAN-Active deviceMacAddress=B8:CA
:3A:68:2F:CC deviceGUID=F8E649AA-AF79-4545-9B5A-580BA993D5
E3 src=192.168.50.93 spt=57775 smac=F4:8E:38:94:D1:71 shos
t=nj-host1 dst=106.120.188.46 dpt=80 dmac=00:00:0C:9F:F0:3
2 dhost=106.120.188.46 cn1Label=sampleType cn1=0 fname=sgi
m_phrases.zip fsize=935 fileType=PKZIP fileHash=022D399592
43995944F024C3E079CAD8EFF06468 request=http://pc.profile.p
inyin.sogou.com/upload.php?hid\\\=sgpy-windows-generic-dev
ice-id&v\\\=8.0.0.7807&brand\\\=1&platform\\\=6&ifbak\\\=1
&ifmobile\\\=0&ifauto\\\=1&filename\\\=sgim_phrases.zip&m\
\\=6A844AC16D9A0CBB99D333F9EDDA4DD5 app=HTTP appGroup=HTTP
```

```
 cs2Label=submitter cs2=Deep Discovery Inspector cs3Label=
submitterName cs3=TEST-DDI deviceDirection=1 requestClient
Application=sogou_ime/8.0.0.7807
```

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 4-4. TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200127
Header (eventName)	Description	NOTABLE_CHARACTERISTICS
Header (severity)	Severity	6: Warning
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceOSName	Sandbox image type	Example: win7
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file

TMEF KEY	DESCRIPTION	VALUE
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: ATSE\nDetection Name: TROJ_FAM_00004f2.TOMA \nEngine Version: 9.826.1078\nMalware Pattern Version: 11.749.92
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+08:00
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
27|NOTABLE_CHARACTERISTICS|6|rt=Jun 26 2015 05:24:01 GMT+00:0
0 pComp=Sandbox dvc=10.204.70.173 dvchost=DDAN deviceMacAddre
ss=00:0C:29:69:19:13 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789
F19FEF4 fname=Sends_email fileHash=1A37D76D3669FC0BF0CBAABB3C
149BAC43491663 fileType=WIN32 EXE fsize=92160 ruleCategory=Ma
lformed, defective, or with known malware traits ruleName=Det
ected as probable malware msg=Source: ATSE\nDetection Name: T
ROJ_FAM_00004f2.TOMA\nEngine Version: 9.826.1078\nMalware Pat
tern Version: 11.749.92 deviceOSName=fsdf
```

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 4-5. TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 5.5.0.1191
Header (eventid)	Signature ID	200120
Header (eventName)	Description	DENYLIST_CHANGE
Header (severity)	Severity	3: Informational
act	The action in the event	• Add • Remove
cs1	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Deny List type	type
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9

TMEF KEY	DESCRIPTION	VALUE
deviceExternalRiskType	Risk level	• Low • Medium • High • Confirmed Malware
dhost	Destination host name	Example: dhost1
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+08:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+08:00

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
20|DENYLIST_CHANGE|3|rt=Jun 26 2015 05:55:02 GMT+00:00 pComp=
Sandbox dvc=10.204.70.17 dvchost=DDAN deviceMacAddress=01:0C:
29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 c
s1Label=type cs1=Deny List Domain end=Jul 26 2015 05:47:16 GM
T+00:00 act=Add dhost=ns1.player1352.com deviceExternalRiskTy
pe=High
```

TMEF System Event Logs

TABLE 4-6. TMEF System Event Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001
Header (eventid)	Event ID	• 300102 • 300999
Header (eventName)	Description	• PRODUCT_UPDATE • SYSTEM_EVENT
Header (severity)	Severity	3: Informational
dvc	Appliance IP address	Example: 192.168.10.1
deviceMacAddress	Appliance MAC address	Example: 00:0D:60:AF:1B:61
dvchost	Appliance host name	Example: DDAN
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Event logged	Example: Mar 03 2016 16:28:20 GMT+08:00
cs1Label	Event type label	"eventType"
cs1	Event type	• System Setting • Account Logon/Logoff • Logoff System Update
duser	User Name	Example: admin

TMEF KEY	DESCRIPTION	VALUE
msg	Details	Example:Updates: Component update settings modified by 'admin' from 192.168.10.2.
src	IPV4 source address	Example: 192.168.100.100
c6a2Label	IPV6 address label	"srcIPv6"
c6a2	IPV6 address	Example: 2001:db8::1
shost	Source hostname	Example: shost1
outcome	Result status	• Success • Failure

Log sample:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300999
|SYSTEM_EVENT|3|rt=Nov 07 2017 10:05:58 GMT+00:00 dvc=10.204
.1.1 dvchost=DDAN deviceMacAddress=00:0C:29:2F:3B:6B deviceG
UID=423E63AA-D466-406E-A15F-6AC6F3CEE50A cs1Label=eventType
cs1=System Setting duser=admin src=10.204.1.2 msg=Log Settin
gs: Settings modified by 'admin' from 10.204.1.2 outcome=Suc
cess
```

TMEF Alert Event Logs

TABLE 4-7. TMEF Alert Event Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 6.0.0.1001

TMEF KEY	DESCRIPTION	VALUE
Header (eventid)	Event ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Severity	• 2: Informational • 6: Important • 8: Critical
dvc	Appliance IP address	Example: • IPV4: 192.168.10.1 • IPv6: 2620:0101:4009:0401::1
deviceMacAddress	Appliance MAC address	Example:00:0D:60:AF:1B:61
dvchost	Appliance host name	Example: DDAN
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Event logged	Example: Mar 03 2016 16:28:20 GMT+08:00
ruleName	Rule name	Example: High Memory Usage
cs1Label	Affected Appliance label	"affectedAppliance"
cs1	Affected Appliance	Example: DDAN.com (10.204.1.2 | FE80:: 29FF:29FF: 29FF: 29FF)
cs2Label	Subject label	"subject"
cs2	Subject	Example: DDAN Important Alert - High Memory Usage
cs3Label	Message label	"ruleContent"
cs3	Message	Message content

Log sample:

```
CEF: 0|Trend Micro|Deep Discovery Analyzer|6.0.0.1119|300105
|ALERT_EVENT|6|rt=Nov 07 2017 08:39:54 GMT+00:00 dvc=10.204.
1.1 dvchost=DDAN deviceMacAddress=00:0C:29:2F:3B:6B deviceGU
ID=423E63AA-D466-406E-A15F-6AC6F3CEE50A ruleName=High CPU Us
age cs1Label=affectedAppliance cs1=DDAN ( 10.204.1.1 | FE80:
:20C:29FF:FE2F:1B6B ) cs2Label=subject cs2=DDAN Important Al
ert - High CPU Usage cs3Label=ruleContent cs3=The average CP
U usage in the last 5 minutes exceeded the threshold of 90%.
\n\nAverage CPU usage: 96%\nAffected appliance: DDAN (10.204
.1.1 | FE80::20C:29FF:FE2F:1B6B)\n\nReduce the number of Vir
tual Analyzer instances, or add a secondary appliance to imp
rove performance.\n\n\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\
=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\=\nAlert time: 2017-11-07 08:3
9:54\nManagement console: https://10.204.1.1/ | https://[FE8
0::20C:29FF:FE2F:1B6B]/
```

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM68236/180418