TREND MICRO™

7.1

TREND MICRO™ Deep Discovery™ Analyzer

Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks

Endpoint Security

Network Security

Protected Cloud

Document Part No.: APEM79311_210806

Release Date: September 2021

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:

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

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Analyzer collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 4: Syslog Content Mapping - TMEF

Index

Preface

Preface

Learn more about the following topics:

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: https://success.trendmicro.com

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

https://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

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

Trend Micro customers include 9 of the top 10 Fortune® Global 500 companies across automotive, banking, healthcare, telecommunications, and petroleum industries.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. https://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

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 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 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
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

CEF Key	Description	Value
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	
cs4Label	Submitter	submitter
cs5	Submitter host name	Example: shost1
cs5Label	Submitter host name	submitterName
cs6	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cs6Label	sha256	

CEF Key	Description	Value
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
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

CEF Key	Description	Value
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 cs6Label=sha256
cs6=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538A
```

```
ABF651FD0F deviceDirection=1 requestClientApplication=sogo
u_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
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

CEF Key	Description	Value
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 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

CEF Key	Description	Value
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3: Informational
act	The action in the event	Add
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
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

CEF Key	Description	Value
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 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

CEF Key	Description	Value
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
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
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"

CEF Key	Description	Value
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]/
```

CEF ICAP Pre-scan Detection Logs

TABLE 2-8. CEF ICAP Pre-scan Detection 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: 7.1.0.1088
Header (eventid)	Signature ID	200129
Header (eventName)	Event name	ICAP_PRESCAN_EVENT
Header (severity)	Risk level	8
rt	Log generation time	Example: May 31 2021 15:56:04 GMT +08:00
dvcmac	Appliance MAC address	Example: 00:0C:29:56:B3:57
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
src	Source IPv4 address	Example: 10.1.144.199
dst	Destination IPv4 address	Example: 10.1.144.198
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
cn1Label	Sample type	sampleType

CEF Key	Description	Value
cn1	Sample type	• 0: File sample • 1: URL sample
request	URL	Example: http://example.com:80/
cs1Label	Malware name	malName
cs1	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	submitterName	
cs2	ICAP client	Example: 10.205.190.3
cs3Label	icapMode	
cs3	ICAP mode	Example: • REQMOD: ICAP Request modification method • RESPMOD: ICAP Response modification method
cs4Label	sourceUser	
cs4	X-Authenticated-User ICAP header sent by the ICAP client	Example: test.com
cs5Label	identifiedBy	

CEF Key	Description	Value
cs5	The name of the detection module that processed the object	Example: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)
cs6Label	sha256	
cs6	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:31:35 GMT+00:00 d
vc=10.2.3.100 dvchost=DDAN dvcmac=00:50:56:98:33:69 device
ExternalId=627EE441-DD62-4483-B9E4-60B3C8A92529 src=10.2.1
1.122 cn1Label=sampleType cn1=1 fileHash=317D137FE590EE561
648ECA137CB2B6898526115 request=http://wrs21.test.com:80/
cs1Label=malName cs1=TSPY_KEYLOG.GC cs2Label=submitterName
 cs2=10.2.1.6 cs3Label=icapMode cs3=REQMOD cs4Label=source
User cs5Label=identifiedBy cs5=Web Reputation Services cs6
Label=sha256 cs6=F5C748A953D23B8CE4F5C792FDC1E7987471DD48F
E24ABA07C3CFD10B4AEF72F
```

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:31:31 GMT+00:00 d
vc=10.2.1.52 dvchost=DDAN dvcmac=00:50:56:98:33:69 deviceE
xternalId=627EE441-DD62-4483-B9E4-60B3C8A92529 dst=10.2.1.
122 src=10.2.1.123 cn1Label=sampleType cn1=0 fname=3-layer
.zip fileType=ZIP archive fileHash=D7273555CB0AC08303415CB
EB3F3D72DD0893BC4 request=http://test.com/3-layer.zip cs1L
abel=malName cs1=Eicar_test_file,TROJ_OLEXP.TPD cs2Label=s
ubmitterName cs2=10.2.1.6 cs3Label=icapMode cs3=RESPMODE c
s4Label=sourceUser cs5Label=identifiedBy cs5=Advanced Thre
at Scan Engine cs6Label=sha256 cs6=08F18BC62297A67DD91E192
A27C1EEDE3C1BBEE19A90FC0B1FADD07CE93B9823
```

Chapter 3

Syslog Content Mapping - LEEF

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

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: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
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: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

LEEF Key	Description	Value
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 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
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pcapReady	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
pComp	Detection engine / component	Sandbox

LEEF Key	Description	Value
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 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

LEEF Key	Description	Value
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
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

LEEF Key	Description	Value
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>
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
sha256	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

LEEF Key	Description	Value
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	
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>sha256=275A021BBFB64
89E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F<009>ur
l=http://stat.moji.com/aMoUp<009>app=HTTP<009>appGroup=HTT
P<009>submitter=Deep Discovery Inspector<009>submitterName
=TEST-DDI<009>deviceDirection=1<009>requestClientApplicati
on=Apache-HttpClient/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
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

LEEF Key	Description	Value
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 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

LEEF Key	Description	Value
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	Add
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
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

LEEF KEY	DESCRIPTION	VALUE
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

LEEF Key	Description	Value
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
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
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

LEEF Key	Description	Value
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]/
```

LEEF ICAP Pre-scan Detection Logs

TABLE 3-8. LEEF ICAP Pre-scan Detection Logs

CEF 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: 7.1.0.1088
Header (eventName)	Event name	ICAP_PRESCAN_EVENT
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
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: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
sha256	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
sampleType	Sample type	• 0: File sample • 1: URL sample

CEF Key	Description	Value
url	URL	Example: http://1.2.3.4/query?term=value
src	Source IPv4 address	Example: 10.1.144.199
dst	Destination IPv4 address	Example: 10.1.144.198
sourceUser	X-Authenticated-User ICAP header sent by the ICAP client	Example: test
sev	Risk level	8: High
malName	Malware name	Example: HEUR_NAMETRICK.A
icapMode	ICAP mode	Example: • REQMOD: ICAP Request modification method • RESPMOD: ICAP Response modification method
identifiedBy	The name of the detection module that processed the object	Example: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|7.1.0.1009|IC
AP_PRESCAN_EVENT|devTime=May 31 2021 15:56:04 GMT+08:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=8<009>dvc=1
0.204.191.223<009>dvchost=DDAN<009>deviceMacAddress=00:50:
56:98:39:75<009>deviceGUID=22DB5662-BDEC-4071-9D82-E5008EF
8B328<009>dst=10.204.190.8<009>src=10.204.190.7<009>sample
Type=1<009>fileHash=317D137FE590EE561648ECA137CB2B68985261
15<009>url=http://test.com:80/<009>malName=VAN_WEB_THREAT.
UMXX<009>submitterName=10.204.190.6<009>icapMode=RESPMODE<
009>sourceUser=auth_test2<009>identifiedBy=Web Reputation
Services<009>sha256=F5C748A953D23B8CE4F5C792FDC1E7987471DD
48FE24ABA07C3CFD10B4AEF72F
```

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|7.1.0.1009|IC
AP_PRESCAN_EVENT|devTime=Jun 02 2021 13:26:17 GMT+08:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=8<009>dvc=1
0.204.191.223<009>dvchost=DDAN<009>deviceMacAddress=00:50:
56:98:39:75<009>deviceGUID=22DB5662-BDEC-4071-9D82-E5008EF
8B328<009>dst=10.204.191.122<009>src=10.204.190.6<009>samp
leType=0<009>fname=\\x332d6c617965722e7a6970<009>fileType=
ZIP archive<009>fileHash=D7273555CB0AC08303415CBEB3F3D72DD
0893BC4<009>malName=TROJ_OLEXP.TPD,Eicar_test_file<009>sub
mitterName=10.204.190.6<009>icapMode=RESPMODE<009> sourceU
ser=auth_test<009>identifiedBy=Advanced Threat Scan Engine
<009>sha256=08F18BC62297A67DD91E192A27C1EEDE3C1BBEE19A90FC
0B1FADD07CE93B9823
```

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

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: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
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
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:

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
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

TMEF Key	Description	Value
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
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:

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

TMEF Key	Description	Value
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
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	
cs2Label	Submitter	submitter

TMEF Key	Description	Value
cs3	Submitter host name	Example: shost1
cs3Label	Submitter host name	submitterName
cs6	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cs6Label	SHA256	
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

TMEF Key	Description	Value
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
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 cs6Label=sha256 cs6=275A021BBFB
6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F devi
ceDirection=1 requestClient Application=sogou_ime/8.0.0.78
07
```

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

TMEF 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: 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:

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

TMEF Key	Description	Value
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
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
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

TMEF Key	Description	Value
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:

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

TMEF Key	Description	Value
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
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
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)

TMEF Key	Description	Value
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]/
```

TMEF ICAP Pre-scan Detection Logs

Table 4-8. TMEF ICAP Pre-scan Detection Logs

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro

TMEF Key	Description	Value
Header (pname)	Appliance product	Deep Discovery Analyzer
Header (pver)	Appliance version	Example: 7.1.0.1088
Header (eventName)	Event name	ICAP_PRESCAN_EVENT
Header (severity)	Risk level	8
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
rt	Log generation time	Example: May 31 2021 15:56:04 GMT +08:00
dvcmac	Appliance MAC address	Example: 00:0C:29:56:B3:57
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
sha256	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F
cn1Label	Sample type	sampleType
cn1	Sample type	• 0: File sample • 1: URL sample
request	URL	Example: http://example.com:80/
malName	Malware name	Example: HEUR_NAMETRICK.A

TMEF Key	Description	Value
src	Source IPv4 address	Example: 10.1.144.199
dst	Destination IPv4 address	Example: 10.1.144.198
cs1Label	submitterName	malName
cs1	ICAP client	Example: 10.205.190.3
cs2Label	icapMode	
cs2	ICAP mode	
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
cs2Label	submitterName	Example: • REQMOD: ICAP Request modification method • RESPMOD: ICAP Response modification method
cs3Label	sourceUser	

TMEF Key	Description	Value
cs3	X-Authenticated-User ICAP header sent by the ICAP client	Example: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)
cs4Label	identifiedBy	
cs4	The name of the detection module that processed the object	Example: • Web Reputation Services • Advanced Threat Scan Engine • Virtual Analyzer • Suspicious Object • User-defined Suspicious Object • YARA Rule (+ Yara_file_name) • Predictive Machine Learning Engine • ICAP: Password-protected file (bypass scanning) • ICAP: Password-protected file (non-malicious, unextracted)

TMEF Key	Description	Value
cs5Label	sha256	
cs5	SHA256	Example: 275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:36:08 GMT+00:00 d
vc=10.204.191.52 dvchost=DDAN deviceMacAddress=00:50:56:98
:33:69 deviceGUID=627EE441-DD62-4483-B9E4-60B3C8A92529 src
=10.2.11.122 cn1Label=sampleType cn1=1 fileHash=317D137FE5
90EE561648ECA137CB2B6898526115 request=http://wrs21.test.c
om:80/ malName=TSPY_KEYLOG.GC cs1Label=submitterName cs1=1
0.204.190.6 cs2Label=icapMode cs2=REQMOD cs3Label=sourceUs
er cs4Label=identifiedBy cs4=Web Reputation Services cs5La
bel=sha256 cs5=F5C748A953D23B8CE4F5C792FDC1E7987471DD48FE2
4ABA07C3CFD10B4AEF72F
```

```
CEF:0|Trend Micro|Deep Discovery Analyzer|7.1.0.1088|20012
9|ICAP_PRESCAN_EVENT|8|rt=Aug 01 2021 02:36:11 GMT+00:00 d
vc=10.204.191.52 dvchost=DDAN deviceMacAddress=00:50:56:98
:33:69 deviceGUID=627EE441-DD62-4483-B9E4-60B3C8A92529 dst
=10.2.1.123 src=10.2.1.122 cn1Label=sampleType cn1=0 fname
=3-layer.zip fileType=ZIP archive fileHash=D7273555CB0AC08
303415CBEB3F3D72DD0893BC4 request=http://test.com/3-layer.
zip malName=Eicar_test_file,TROJ_OLEXP.TPD cs1Label=submit
terName cs1=10.204.190.6 cs2Label=icapMode cs2=RESPMODE cs
3Label=sourceUser cs4Label=identifiedBy cs4=Advanced Threa
t Scan Engine cs5Label=sha256 cs5=08F18BC62297A67DD91E192A
27C1EEDE3C1BBEE19A90FC0B1FADD07CE93B9823
```

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: APEM79311/210806