TREND MICRO

5.0 TREND MICRO™ Deep Discovery™ Email Inspector

Syslog Content Mapping Guide

Advanced Protection Against Targeted Email Threats

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

Document Part No.: APEM58978/200508

Release Date: July 2020

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

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 Email Inspector 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 - LEEF

Chapter 5: Syslog Content Mapping - TMEF

Index

Preface

Preface

Learn more about the following topics:

Documentation

The documentation set for Deep Discovery Email Inspector includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Email Inspector, and explanations on Deep Discovery Email Inspector concepts and features.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Email Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Email Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Email Inspector 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.
Online Help	Web-based documentation that is accessible from the Deep Discovery Email Inspector management console. The Online Help contains explanations of Deep Discovery Email Inspector components and features, as well as procedures needed to configure Deep Discovery Email Inspector.

Document	Description
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://success.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 Email Inspector 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
- Email routing
- SMTP

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

CONVENTION	DESCRIPTION
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. http://www.trendmicro.com

Chapter 1

Introduction

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

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

Log Management System	Description
Common Event Format (CEF) For details, see *Syslog Content Mapping - CEF on page 3-1*	CEF is an open log management standard created by HP ArcSight. Deep Discovery Email Inspector uses a subset of the CEF dictionary.
Log Event Extended Format (LEEF) For details, see *Syslog Content Mapping - LEEF on page 4-1*	LEEF is an event format developed for IBM Security QRadar. Deep Discovery Email Inspector uses a subset of the LEEF dictionary.
Trend Micro Event Format (TMEF) For details, see *Syslog Content Mapping - TMEF on page 5-1*	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 Email Inspector.

Syslog Events

Deep Discovery Email Inspector supports the following events.

TABLE 1-1. Syslog events

EVENT	DESCRIPTION
Detection Logs: Email Detection Logs	Email detection logs from Deep Discovery Email Inspector. These logs contain information related to the detected email messages (such as sender, recipients, subject, and message ID).
Detection Logs: Attachment Detection Logs	Attachment detection logs from Deep Discovery Email Inspector. These logs contain information related to the detected attachments (such as file name, file size, and file type).
Detection Logs: URL Detection Logs	URL detection logs from Deep Discovery Email Inspector. These logs contain the URLs detected and potential threats.
Alert Logs	Alert logs from Deep Discovery Email Inspector. These logs contain information related to the alerts (such as alert name and alert notification content).
Virtual Analyzer Analysis Logs: File Analysis Events	File analysis events from Virtual Analyzer. These logs contain information related to the analyzed files (such as file name, file size, and file type).
Virtual Analyzer Analysis Logs: URL Analysis Events	URL analysis events from Virtual Analyzer. These logs contain the URLs analyzed and potential threats.
Virtual Analyzer Analysis Logs: Notable Characteristics Events	Notable characteristics events from Virtual Analyzer. These logs contain information about notable characteristics events that are triggered by the analyzed samples.
Virtual Analyzer Analysis Logs: Deny List Transaction Events	Deny list transaction events from Virtual Analyzer. These logs contain actions performed on specific deny lists and information about the deny list objects (such as SHA1 or URL).

Event	Description
Message Tracking Logs	These logs indicate if email messages are received or sent from Deep Discovery Email Inspector and include evidence of email message investigation.
Sender Filtering/ Authentication Logs	These logs include sender authentication results and actions performed.
System Logs	These are audit logs or update logs from Deep Discovery Email Inspector.
MTA Logs	These logs contain information on Postfix connections and SMTP activities on Deep Discovery Email Inspector. Raw MTA logs are sent directly to syslog servers.

Terminology

Term	Description
CEF	Common Event Format
LEEF	Log Event Extended Format
TMEF	Trend Micro Event Format

Chapter 2

Revision History

The following table provides the revision history for this document.

VERSION	DESCRIPTION

3.1	• Added Unsuccessful DKIM Signing system alert
	• Added new logs for the following events:
	  • Message tracing
	  • Sender filtering/authentication
	  • MTA

VERSION	DESCRIPTION

3.0	• Added the following for email detection logs:
	  • `Unavailable` severity type
	  • `deleted`, `delivered directly`, and `cleaned up` action types
	  • `Spam/Graymail`, `Phishing`, and `Content violation` threat types
	• Added `Unavailable` severity type for attachment detection logs
	• Added new system alerts:
	  • Account Locked
	  • Low Free Spam Quarantine Disk Space
	  • Long Message Deferred Queue
	• Renamed the following system alerts:
	  • "Quarantined Messages" to "Quarantined Messages with Detected Threats"
	  • "Detection Surge" to "Threat Detection Surge"
	  • "Low Free Quarantine Disk Space" to "Low Free Threat Quarantine Disk Space"

2.6	Added High Memory Usage system alert log

2.5 SP1	• Removed Signature ID (`eventid`) for the following LEEF logs:
	  • Email detection logs
	  • Attachment detection logs
	  • URL detection logs
	  • Alert logs
	• Added Quarantined Messages security alert log

2.5	First release

Chapter 3

Syslog Content Mapping - CEF

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

CEF Detection Logs: Email Detection Logs

TABLE 3-1. CEF Detection Logs: Email 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 Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted

CEF KEY	DESCRIPTION	VALUE
cn1	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
cn1Label	Threat type	threatType
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	Email ID	messageId
cs4	Sender email address	Example: user1@domain.com
cs4Label	Label for sender email address	senderMail

CEF KEY	DESCRIPTION	VALUE
cs5	Recipient email address	Example: user2@domain.com
cs5Label	Label for recipient email address	rcptMail
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
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
msg	Email subject	Example: hello
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|100130|EMAIL_DETECTION|6|rt=Mar
23 2015 11:53:17 GMT+00:00 src=150.70.186.134 cs3Label=mess
ageId cs3=<20150323115314.BCA2C9168EA@internalbeta.bcc.ddei
> deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 act
=passed dvchost=internalbeta.bcc.ddei dvc=10.64.1.131 duser
=user1@domain1.com;user2@domain1.com;user3@domain1.com msg=
Virus_Report-20150323_02:00 cn2Label=msgSize cn2=83878 cn1L
abel=threatType cn1=3 suser=user@domain2.com dvcmac=C4:34:6
B:B8:09:BC cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB
5EC111FE7 cs1Label=threats cs1=PUA_Test_File|TROJ_GEN.R04AC
0PAH15|PAK_Generic.005|ADW_DOWNLOADER.WRS|LOW-REPUTATION-UR
L_BLOCKED-LIST.SCORE.WRS|LOW-REPUTATION-URL_BLOCKED-LIST.SC
```

```
ORE.WRS|TROJ_GEN.R02SC0OLH14|TROJ_GENERIC.WRS|TROJ_DOWNLOAD
ER.WRS
```

CEF Detection Logs: Attachment Detection Logs

TABLE 3-2. CEF Detection Logs: Attachment 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 Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
cs1	Threat name	Example:VAN_BOT.UMXX
cs1Label	Threat name	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
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
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|100131|ATTACHMENT_DETECTION|6|rt
=Mar 23 2015 14:04:46 GMT+00:00 fileHash=E49395FEACC12A5613
E7BA6C69AC5E42EDFDA42D fsize=17681 fileType=MIME Base64 dvc
host=internalbeta.bcc.ddei dvc=10.64.1.131 deviceExternalId
=c425624a-e9db-4f3f-8088-2726f15e6587 cs2Label=msgUuid cs2=
E89A23BE-11F5-2505-BCEE-21027D078154 fname=3C761B45-626D-4E
75-B4782FD0E5E8369C.eml dvcmac=C4:34:6B:B8:09:BC cs1Label=t
hreats cs1=TROJ_UP.258A1A7D
```

CEF Detection Logs: URL Detection Logs

TABLE 3-3. CEF Detection Logs: URL Detection Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0

CEF Key	Description	Value
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	Email severity	• 4: Low • 6: Medium • 8: High
cat	Category	Example: 90:02
cs1	Threat name	Example: LOW-REPUTATION-URL_MALWARE.WRS
cs1Label	Threat name	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
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
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+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1139|100132|URL_DETECTION|6|rt=Mar 2
3 2015 11:57:46 GMT+00:00 cs2Label=msgUuid cs2=73A9FA6A-11F
3-4F05-BCEE-6BB5EC111FE7 dvcmac=C4:34:6B:B8:09:BC dvchost=i
nternalbeta.bcc.ddei request=http://www.alltobid.com/guopai
/upload/dan201401.zip dvc=10.64.1.131 deviceExternalId=c425
624a-e9db-4f3f-8088-2726f15e6587
```

CEF Alert Logs

TABLE 3-4. CEF Alert Logs

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	• 2: Informational • 6: Important • 8: Critical
cs1	Alert name	Example: Security: Suspicious Messages Identified

CEF KEY	DESCRIPTION	VALUE
cs1Label	Alert name	ruleName
cs2	Description	Example: 1 or more messages detected with threats
cs2Label	Description	ruleCriteria
cs3	Triggered value	Example: 35
cs3Label	Triggered value	eventTriggeredValue

cs4	Notification content	Example:
		`The following email messages contain threats:`
		
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <20150619032243.5923E650365@localhost.ddei-164>`
		`Recipients: fake@test.com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263`
		`Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		
		`Alert time: 2015-05-25 11:11:27 +0800`
		
		Note
		The maximum length is 1023 characters.

cs4Label	Notification content	ruleContent

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
externalId	The logid in the alert database	Example: 1648
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1009|300105|ALERT_EVENT|6|rt=Jun 16 2
015 09:26:25 GMT+00:00 cs1Label=ruleName cs1=Security: Thre
at Messages cnt=1 cs2Label=ruleCriteria cs2=At least 1 thre
at message detected externalId=1299 cs3Label=ruleContent cs
3=The%20following%20email%20messages%20contain%20threats%3A
%0A%0A%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3
D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%
3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D
%3D%3D%3D%0ARisk%3A%20Medium%20%28Malware%29%0AAction%3A%20
%20Quarantined%0AMessage%20ID%3A%20%3C20150616092610.B56A66
503C6%40localhost.ddei-164%3E%0ARecipients%3A%20fake%40test
.com%3Btest%40test.com%0ASender%3A%20test%40fake.test%0ASub
ject%3A%20temail%20-%20Copyaaa... dvcmac=00:50:56:01:2C:BC
dvchost=localhost.ddei-164 deviceExternalId=361a091c-addd-
40cf-98e7-710e43500a66 dvc=10.204.253.164
```

CEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 3-5. CEF Virtual Analyzer Analysis Logs: File Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200119
Header (eventName)	Description	Sample file sandbox analysis is finished
Header (severity)	Severity	3: Informational
cn1	Result of GRID/CSSS	• 0: GRID is not known good • 1: GRID is known good
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7

CEF Key	Description	Value
cs1Label	Sandbox image type	SandboxImageType
cs2	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	Malware name	MalwareName
cs3	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
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: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200119|Sample file sandbox analy
sis is finished|3|rt=Mar 23 2015 14:48:24 GMT+00:00 dvc=10.
64.1.131 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6B:B8:0
9:BC deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587
fname=Wonga Express Loan Promtion 3.5% Offer.doc fileHash=A
```

```
46E1F56969DECC5FEAF120A2279946A2F42D619 fileType=MS Office
fsize=53760 cs1Label=SandboxImageType cs1=win81en cn1Label=
GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=1 cs2Label=Ma
lwareName cs2=VAN_MALWARE.UMXX cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 3-6. CEF Virtual Analyzer Analysis Logs: URL Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL sandbox analysis is finished
Header (severity)	Severity	3
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7

CEF KEY	DESCRIPTION	VALUE
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
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+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200126|URL sandbox analysis is
finished|3|rt=Mar 23 2015 16:32:15 GMT+00:00 dvc=10.64.1.1
31 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC
deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 requ
est=http://paypal-world.ga/home/? fileHash=5EA358C987D1FDE
34957B9A36AF38321C5F37D8B cs1Label=SandboxImageType cs1=wi
n81en cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 3-7. CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200127
Header (eventName)	Description	Notable Characteristics of the analyzed sample
Header (severity)	Severity	6
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
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199

CEF KEY	DESCRIPTION	VALUE
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: Process ID: 3020\n Image Path: %ProgramFiles%\ \Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 /prefetch:2
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200127|Notable Characteristics o
f the analyzed sample|6|rt=Mar 23 2015 10:44:28 GMT+00:00 d
vc=10.64.1.131 dvchost=internalbeta.bcc.ddei dvcmac=C4:34:6
B:B8:09:BC deviceExternalId=c425624a-e9db-4f3f-8088-2726f15
e6587 fname=http://bsjv.tk/bbb/bbb/bbb fileHash=2D302EEEF70
3CBB8713B806B3C5B4B3A2A28E92A fileType=URL fsize=0 cs1Label
=PolicyCategory cs1=Process, service, or memory object chan
ge msg=Process ID: 3020\nImage Path: %ProgramFiles%\\Intern
et Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 /prefet
ch:2 cs2Label=PolicyName cs2=Creates process
```

CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 3-8. CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3
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

CEF KEY	DESCRIPTION	VALUE
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 IP 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	Report end time	Example: Mar 09 2015 17:05:21 GMT+00:00
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+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|200120|Deny List updated|3|rt=Ma
```

```
r 24 2015 10:10:20 GMT+00:00 dvc=10.64.1.131 dvchost=intern
albeta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c
425624a-e9db-4f3f-8088-2726f15e6587 cs1Label=type cs1=Deny
List File SHA1 end=Apr 19 2015 16:03:13 GMT+00:00 act=Add
fileHash=41D188169D9B986818A437DD80814FA84B0522FB cs2Label=
RiskLevel cs2=High
```

CEF Message Tracking Logs

TABLE 3-9. CEF Message Tracking Logs

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100136
Header (eventName)	Description	MESSAGE_TRACKING
Header (severity)	Email severity	• 2: Unavailable • 2: Unrated • 2: Normal • 4: Low • 6: Medium • 8: High
dvc	Appliance IP address	Example: 10.1.144.199

CEF KEY	DESCRIPTION	VALUE
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
cs1Label	Label for Email ID	messageId
cs1	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	Label for internal email ID	msgUuid
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
msg	Email subject	Example: hello
reason	Reason for block action	Example: Timeout period expired
cs3Label	Latest status	latestStatus
cs3	Details	• Quarantined • Delivered • Delivery unsuccessful • Processing completed • Deleted

CEF Key	Description	Value
src	Source IP address	Example: 10.1.144.199
cs4Label	Label for sender email address	senderMail
cs4	Sender email address	Example: user1@domain.com
cs5Label	Label for recipient email address	rcptMail
cs5	Recipient email address	Example: user2@domain.com
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
cs6Label	Label for process history	procHistory
cs6	Process history	Example: Action taken by the device. The format: "timestamp1 act1,timestamp2 act2,…, timestampn actn"

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1106|100136|MESSAGE_TRACKING|2|rt=A
pr 27 2018 02:55:53 GMT+00:00 cs3Label=latestStatus cs3=De
livery unsuccessful dvchost=localhost.localdomain deviceEx
ternalId=9ceb7be2-3ec5-4b80-8697-6b4913eb044b dvc=10.204.6
3.177 duser=test@test.com dvcmac=00:50:56:A7:5F:AD reason=
host 10.204.253.179[10.204.253.179] said: 552 test@test.co
m mailbox full (in reply to end of DATA command) cs1Label=
messageId cs1=20180427025553.4D771D6135F@localhost.localdo
main cs4Label=senderMail cs4=marks@relay.ddei.comsuser=fak
e@test.testmsg=plain_text_upper_case.HTML/HTM cs2Label=msg
Uuid cs2=EB715918-6ACB-A405-BF46-56F53CE3FD86 cs6Label=pro
cHistory cs6=Apr 27 2018 02:55:53 GMT+00:00 Received,Apr 2
7 2018 02:55:53 GMT+00:00 Sent for analysis,Apr 27 2018 02
:56:48 GMT+00:00 Action set to 'pass',Apr 27 2018 02:56:48
 GMT+00:00 Delivery unsuccessful,Reason:host 10.204.253.17
```

```
9[10.204.253.179] said: 552 test@test.com mailbox full (in
 reply to end of DATA command)
```

CEF Sender Filtering/Authentication Logs

TABLE 3-10. CEF Sender Filtering/Authentication Logs

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100137
Header (eventName)	Description	SENDER_FILTERING
Header (severity)	Email severity	2
dvc	Appliance IP address	Example: 10.1.144.199
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)

CEF KEY	DESCRIPTION	VALUE
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
cn1Label	Label for event type	eventType
cn1	Event type	• 1: Email reputation • 2: DHA protection • 3: Bounce attack protection • 4: SMTP traffic throttling (IP address) • 5: SMTP traffic throttling (email address) • 6: SPF • 7: DKIM • 8: DMARC
act	The action in the event	• 2: Block temporarily • 3: Block permanently
cn2Label	Label for sender authentication result	rfcResult

CEF KEY	DESCRIPTION	VALUE
cn2	Sender authentication result	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	Reason for block action	Example: No DNS txt record

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1133|100137|SENDER_FILTERING|2|rt=A
pr 27 2018 01:59:38 GMT+00:00 cn1Label=eventType cn1=7 cn2
Label=rfcResult cn2=5 dvchost=localhost.localdomain device
TranslatedAddress=10.206.155.122 deviceExternalId=15129231
-f1dc-4941-8014-1a1b9fbc9253 dvc=10.206.155.128 act=2 duse
r=user1@domain1.com;user2@domain1.com;user223@domain1.com;
user4@domain1.com reason=102 suser=user1@domain2.com dvcma
c=00:0C:29:8D:2E:74
```

CEF System Logs

TABLE 3-11. CEF System Logs

CEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	CEF: 0

CEF KEY	DESCRIPTION	VALUE
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	Description	• PRODUCT_UPDATE (300102) • SYSTEM_EVENT (300999)
Header (severity)	Severity	3
cn1	Event ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
cn1Label	Event ID	operationId
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
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1139|300999|SYSTEM_EVENT|3|rt=Mar 24
2015 08:43:35 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC cn3Label=
operationId cn3=30000 msg=Account 'admin' logged on from 1
0.64.50.147 deviceExternalId=c425624a-e9db-4f3f-8088-2726f
15e6587 dvchost=internalbeta.bcc.ddei dvc=10.64.1.131
```

MTA Logs

There is no syslog content mapping information for MTA logs. Deep Discovery Email Inspector sends raw MTA logs directly to syslog servers.

Log sample:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```

Chapter 4

Syslog Content Mapping - LEEF

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

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

LEEF Detection Logs: Email Detection Logs

TABLE 4-1. LEEF Detection Logs: Email Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	EMAIL_DETECTION
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z

LEEF KEY	DESCRIPTION	VALUE
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
mailMsgSubject	Email subject	Example: hello
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
rcptMail	Recipient email address	Example: user2@domain.com
senderMail	Sender email address	Example: user1@domain.com
sev	Severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

LEEF KEY	DESCRIPTION	VALUE
threatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|EMAIL_DETECTION|=8\0x09threatType=
4\0x09deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e0x09mess
ageId=<20150413072949.E8C0D1E9A363@internalbeta.bcc.ddei>\0x0
9msgUuid=6C4A91D7-1396-1405-94C5-D955018F938E\0x09mailMsgSubj
ect=Orcamento Total - 5636005\0x09src=69.162.64.30\0x09msgSiz
e=397113\0x09dvchost=internalbeta.bcc.ddei\0x09dvc=10.64.1.13
1\0x09act=passed\0x09duser=user1@domain1.com\0x09devTime=Apr
13 2015 07:29:50 GMT+00:00\0x09suser=www-data@contato30.danet
mail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09devTimeFormat=MMM d
d yyyy HH:mm:ss z\0x09threatName=VAN_BACKDOOR.UMXX
```

LEEF Detection Logs: Attachment Detection Logs

TABLE 4-2. LEEF Detection Logs: Attachment Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	ATTACHMENT_DETECTION
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00

LEEF Key	Description	Value
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
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
emailSeverity	Email severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file

LEEF KEY	DESCRIPTION	VALUE
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
mailMsgSubject	Email subject	Example: hello
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	Severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|ATTACHMENT_DETECTION|sev=8\0x09msgU
uid=6C4A91D7-1396-1405-94C5-D955018F938E\0x09fileHash=2EF0B334
EFDE7F1BA16011158E25555C2B9D7BC5\0x09emailSeverity=8\0x09suser
=www-data@contato30.danetmail.net\0x09dvchost=internalbeta.bcc
.ddei\0x09emailThreatType=4\0x09duser=spam@support.trendmicro.
```

```
com\0x09messageId=<20150413072949.E8C0D1E9A363@internalbeta.bc
c.ddei>\0x09src=69.162.64.30\0x09deviceGUID=034eb532-9318-40d9
-b27b-d9feba7c269e\0x09mailMsgSubject=Orcamento Total - 563600
5\0x09msgSize=397113\0x09fileType=Directory\0x09dvc=10.64.1.13
1\0x09devTime=Apr 13 2015 15:45:58 GMT+00:00\0x09fname=Orcamen
to%20Total.zip\0x09act=passed\0x09dvcmac=C4:34:6B:B8:09:BC\0x0
9devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09threatName=VAN_BACKD
OOR.UMXX\0x09emailThreats=VAN_BACKDOOR.UMXX
```

LEEF Detection Logs: URL Detection Logs

TABLE 4-3. LEEF Detection Logs: URL Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	URL_DETECTION

LEEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
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

LEEF Key	Description	Value
eventTriggeredValue	Triggered value	Example: 35
emailSeverity	Email severity	• 4: Low • 6: Medium • 8: High
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
mailMsgSubject	Email subject	Example: hello
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	Severity	• 4: Low • 6: Medium • 8: High

LEEF KEY	DESCRIPTION	VALUE
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX| FRAUD_PHISHING.WRS
url	URL	Example: http://1.2.3.4/query?term=value
urlCat	Category	Example: 90:02

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|URL_DETECTION|sev=4\0x09deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e\0x09msgUuid=6C4A91D7-13
96-1405-94C5-D955018F938E\0x09mailMsgSubject=Orcamento Total
-5636005\0x09src=69.162.64.30\0x09emailSeverity=8\0x09msgSize
=397113\0x09dvchost=internalbeta.bcc.ddei0x09dvc=10.64.1.131\
0x09emailThreatType=4\0x09duser=user1@domain1.com\0x09url=htt
p://200.98.168.34/testam1/t3zs3.html\0x09act=passed\0x09devTi
me=Apr 13 2015 15:45:58 GMT+00:00\0x09suser=www-data@contato3
0.danetmail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09devTimeForma
t=MMM dd yyyy HH:mm:ss z\0x09messageId=<20150413072949.E8C0D1
E9A363@internalbeta.bcc.ddei>\0x09emailThreats=VAN_BACKDOOR.U
MXX
```

LEEF Alert Logs

TABLE 4-4. LEEF Alert Logs

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	ALERT_EVENT
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
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
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
eventTriggeredValue	Triggered value	Example: 35
externalId	The logid in the alert database	Example: 1648

LEEF KEY	DESCRIPTION	VALUE

ruleContent	Notification content	Example:
		`The following email messages contain threats:`
		
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <201506190 32243.5923E650365@loca lhost.ddei-164>`
		`Recipients: fake@test. com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_5 07ECC33FA60979F6B97D84 DA47972096185C263`
		`Attachment: 4_file_507 ECC33FA60979F6B97D84DA 47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		
		`Alert time: 2015-05-25 11:11:27 +0800`
		`Generated by: localhost. localdomain (192.168.1. 100)`
		`Management console: https://192.168.1.100/ loginPage.ddei`
		
		Note
		The maximum length is 20000 characters.

ruleCriteria	Description	Example: 1 or more messages detected with threats

LEEF KEY	DESCRIPTION	VALUE
ruleEventType	Alert type	• 0: System event • 1: Security event and the event severity is "High", "Medium", or "Low" • 2: Security event and the even severity is "High", or "Medium" • 3: Security event and the event severity is "High"
ruleId	Alert ID	Value between 1 and 15
ruleName	Alert name	Example: Security: Suspicious Messages Identified
sev	Severity	• 2: Informational • 6: Important • 8: Critical

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1009|ALERT_EVENT|sev=2\0x09cnt=8\0x09rul
eEventType=0\0x09ruleId=10\0x09ruleCriteria=At least 1 message
s processed\0x09dvchost=localhost.ddei-164\0x09dvc=10.204.253.
164\0x09deviceGUID=361a091c-addd-40cf-98e7-710e43500a66\0x09ex
ternalId=1684\0x09devTime=Jun 19 2015 03:18:48 GMT+00:00\0x09r
uleName=System: Processing Surge\0x09dvcmac=00:50:56:01:2C:BC\
0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09ruleContent=The%2
0number%20of%20processed%20messages%20reached%20the%20specifie
d%20threshold%20%281%29.%0A%0AMessages%20processed%3A%208%0ACh
ecking%20interval%3A%200%20minutes%0A%0AAlert%20time%3A%202015
-06-19%2003%3A18%3A48%20%2B0000%0AGenerated%20by%3A%20localhos
```

```
t.ddei-164%20%2810.204.253.164%29%0AManagement%20console%3A%20
https%3A//10.204.253.164/loginPage.ddei
```

LEEF Virtual Analyzer Analysis Logs: File Analysis

TABLE 4-5. LEEF Virtual Analyzer Analysis Logs: File Analysis

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
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
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z

LEEF Key	Description	Value
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
gridIsKnownGood	Result of GRID/CSSS	• 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	Example: 3: High risk
sev	Severity	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|FILE_ANALYZED|devTime=Apr 13 2015
07:45:54 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x
09sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=inte
rnalbeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09d
eviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fname=Or\x8
```

```
7amento Total.cpl\0x09fileHash=2EF0B334EFDE7F1BA16011158E25555
C2B9D7BC5\0x09deviceProcessHash=61DD815ABF2D1FFC58F261392DAFF4
F11B59D79C\0x09malName=VAN_BACKDOOR.UMXX\0x09fileType=Win32 DL
L\0x09fsize=482816\0x09deviceOSName=win81en\0x09gridIsKnownGoo
d=-1\0x09rozRating=3\0x09pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: URL Analysis

TABLE 4-6. LEEF Virtual Analyzer Analysis Logs: URL Analysis

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	URL_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceOSName	Sandbox image type	Example: win7
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D

LEEF Key	Description	Value
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
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
rozRating	ROZ rating	Example: 3: High risk
sev	Severity	3
url	URL	Example: http://1.2.3.4/query?term=value

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|2.5.1.1161|URL_ANALYZED|devTime=Apr 13 2015 07
:34:41 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09
sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=intern
albeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09dev
iceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fileHash=BF68
52C834224BD2C26AC4BE20E7E08930B39FEF\0x09deviceOSName=win7sp1e
```

```
n\0x09url=http://climtorg.ru/bitrix/admin/1up\0x09rozRating=3\
0x09pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 4-7. LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	NOTABLE_CHARACTERISITICS
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+00:00
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
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: msg=Dropping Process ID: 2984\n File: %USERPROFILE%\AppData\Local\MICROSOFT\INTERNET EXPLORER\Recovery\High\LAST ACTIVE\{D78424A0 E1AA-11E4-B7C5-7CC9C8DA4AD 2}.DAT \nType: VSDT_WINWORD\
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	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|NOTABLE_CHARACTERISTICS|devTime=Ap
r 13 2015 07:01:13 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:
mm:ss z\0x09sev=6\0x09pComp=Sandbox\0x09dvc=10.64.1.132\0x09dv
chost=internalbeta.tapping.ddei\0x09deviceMacAddress=B0:83:FE:
DD:21:98\0x09deviceGUID=e57f0651-b197-42d4-a643-271c1277b5ff\0
```

```
x09fname=http://yt1nutj.wvp78.com/\0x09fileHash=8213271FD287C3
F27D6975FE0545AB77DC8EBF73\0x09fileType=URL\0x09fsize=0\0x09ru
leCategory=File drop, download, sharing, or replication\0x09ru
leName=Drops file that can be used to infect systems\0x09msg=D
ropping Process ID: 2984\nFile: %USERPROFILE%\AppData\Local\MI
CROSOFT\INTERNET EXPLORER\Recovery\High\LAST ACTIVE\{D78424A0-
E1AA-11E4-B7C5-7CC9C8DA4AD2}.DAT\nType: VSDT_WINWORD\0x09devic
eOSName=win7sp1en
```

LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 4-8. LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	• Add • Remove
deviceExternalRiskType	Risk level	• Low • Medium • High • Confirmed Malware

LEEF KEY	DESCRIPTION	VALUE
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+00:00
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 IP 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+00:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
sev	Severity	3
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 \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost  LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|DENYLIST_CHANGE|devTime=Apr 13 201
5 07:47:01 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\
0x09sev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=in
ternalbeta.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x0
9deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09end=May 1
3 2015 07:44:37 GMT+00:00\0x09act=Add\0x09dst=200.98.168.34\0x
09dpt=80\0x09deviceExternalRiskType=Medium\0x09type=Deny List
IP/Port
```

LEEF Message Tracking Logs

TABLE 4-9. LEEF Message Tracking Logs

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	MESSAGE_TRACKING

LEEF KEY	DESCRIPTION	VALUE
sev	Email severity	• 2: Unavailable • 2: Unrated • 2: Normal • 4: Low • 6: Medium • 8: High
dvc	Appliance IP address	Examples: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
mailMsgSubject	Email subject	Example: hello

LEEF KEY	DESCRIPTION	VALUE
reason	Reason for block action	Example: Timeout period expired
latestStatus	Latest status	• Quarantined • Delivered • Delivery unsuccessful • Processing completed • Deleted
src	Source IP address	Example: 10.1.144.199
senderMail	Sender email address	Example: user1@domain.com
rcptMail	Recipient email address	Example: user2@domain.com
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
procHistory	Process history	Example: Action taken by the device. The format: "timestamp1 act1,timestamp2 act2,…, timestampn actn"

Log sample:

```
May 15 16:00:4 7 internalbeta LEEF:1.0|Trend Micro|Deep Di
scovery Email Inspector|3.1.0.1154|MESSAGE_TRACKING|sev=2<
009>latestStatus=Processing completed<009>procHistory=May
15 2018 08:00:33 GMT+00:00 Received,May 15 2018 08:00:33 G
MT+00:00 Action set to 'pass',May 15 2018 08:00:33 GMT+00:
00 Processing completed<009>msgUuid=46252714-6C39-FF05-98F
4-5C63BCB20569<009>mailMsgSubject=Time is running out: New
 data privacy permissions<009>src=104.130.122.63<009>sende
rMail=sap@mailsap.com<009>suser=bounce+814a73.7ecda73-jeff
_lovelace=trendmicro.com@mailsap.com<009>dvchost=internalb
eta.bcc.ddei<009>dvc=10.64.1.131<009>duser=jeff_lovelace@t
rendmicro.com<009>deviceGUID=67067637-acbf-46de-a22d-be8d0
d976cd5<009>rcptMail=jeff_lovelace@trendmicro.com<009>devT
ime=May 15 2018 08:00:33 GMT+00:00<009>messageId=201805150
80033.0EE4B6834964@internalbeta.bcc.ddei<009>dvcmac=EC:F4:
```

```
BB:DE:E5:30<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>d
eviceTranslatedAddress=104.130.122.63
```

LEEF Sender Filtering/Authentication Logs

TABLE 4-10. LEEF Sender Filtering/Authentication Logs

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Description	SENDER_FILTERING
sev	Email severity	2
dvc	Appliance IP address	Examples: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)

LEEF KEY	DESCRIPTION	VALUE
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
eventType	Event type	• 1: Email reputation • 2: DHA protection • 3: Bounce attack protection • 4: SMTP traffic throttling (IP address) • 5: SMTP traffic throttling (email address) • 6: SPF • 7: DKIM • 8: DMARC
act	The action in the event	• 2: Block temporarily • 3: Block permanently
rfcResult	Sender authentication result	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	Reason for block action	Example: No DNS txt record

Log sample:

```
May 15 16:00:4 7 internalbeta LEEF:1.0|Trend Micro|Deep Di
scovery Email Inspector|3.1.0.1147|SENDER_FILTERING|sev=2<
009>deviceGUID=15129231-f1dc-4941-8014-1a1b9fbc9253<009>rf
cResult=5<009>eventType=6<009>deviceTranslatedAddress=10.2
06.155.122<009>dvchost=localhost.localdomain<009>dvc=10.20
6.155.128<009>act=2<009>duser=user1@domain.com<009>reason=
56<009>devTime=May 15 2018 08:15:31 GMT+00:00<009>suser=us
er2@domain2.com<009>dvcmac=00:0C:29:8D:2E:74<009>devTimeFo
rmat=MMM dd yyyy HH:mm:ss z
```

LEEF System Logs

TABLE 4-11. LEEF System Logs

LEEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	PRODUCT_UPDATE SYSTEM_EVENT
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00

LEEF KEY	DESCRIPTION	VALUE
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
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
operationId	Event ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
sev	Severity	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
 Email Inspector|2.5.1.1161|SYSTEM_EVENT|sev=3\0x09deviceGUID
=e57f0651-b197-42d4-a643-271c1277b5ff\0x09devTime=Apr 13 2015
 06:52:00 GMT+00:00\0x09msg=Logout: 'admin' logged off\0x09dv
cmac=B0:83:FE:DD:21:98\0x09devTimeFormat=MMM dd yyyy HH:mm:ss
 z\0x09dvchost=internalbeta.tapping.ddei\0x09dvc=10.204.253.1
63\0x09operationId=30000
```

MTA Logs

There is no syslog content mapping information for MTA logs. Deep Discovery Email Inspector sends raw MTA logs directly to syslog servers.

Log sample:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```

Chapter 5

Syslog Content Mapping - TMEF

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

TMEF Detection Logs: Email Detection Logs

TABLE 5-1. TMEF Detection Logs: Email Detection Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted

TMEF KEY	DESCRIPTION	VALUE
cn1	Email Size	Example: 30841
cn1Label	Email Size	msgSize
cs1	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs1Label	Internal email ID	msgUuid
cs2	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	Email ID	messageId
cs3	Sender email address	Example: user1@domain.com
cs3Label	Label for sender email address	senderMail
cs4	Recipient email address	Example: user2@domain.com
cs4Label	Label for recipient email address	rcptMail
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
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
mailMsgSubject	Email subject	Example: hello
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

TMEF KEY	DESCRIPTION	VALUE
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX| FRAUD_PHISHING.WRS
threatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|100130|EMAIL_DETECTION|8|rt=Apr 13 201
5 08:49:22 GMT+00:00 src=141.251.58.19 threatType=4 deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e mailMsgSubject=phishwatc
h Digest, Vol 2933, Issue 13 act=passed dvchost=internalbeta.b
cc.ddei cs2Label=messageId cs2=<20150413084922.2052D1E9A066@in
ternalbeta.bcc.ddei dvc=10.64.1.131 cs1Label=msgUuid cs1=ECBC7
B7E-1397-3005-94C5-0BA1DA0913D2 duser=user1@domain2.com suser=
user1@domain1.com dvcmac=C4:34:6B:B8:09:BC threatName=VAN_MALW
ARE.UMXX cn1Label=msgSize cn1=1204948
```

TMEF Detection Logs: Attachment Detection Logs

TABLE 5-2. TMEF Detection Logs: Attachment Detection Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Attachment severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High

TMEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted
cn1	Email severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize

TMEF KEY	DESCRIPTION	VALUE
cn3	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
cn3Label	Threat type	emailThreatType
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	emailThreats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	Email ID	messageId
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	Email recipients	Example: user1@domain2.com;test@163.com

TMEF 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
mailMsgSubject	Email subject	Example: hello
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|100131|ATTACHMENT_DETECTION|8|rt=Apr 1
3 2015 16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId
 cs3=<20150413084922.2052D1E9A066@internalbeta.bcc.ddei cn1Lab
el=emailSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2
933, Issue 13 fileHash=E07B349245FCDDB31CBF5A52012807E955D2EB7
A fileType=Directory act=passed dvchost=internalbeta.bcc.ddei
dvc=10.64.1.131 deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269
e duser=user1@domain.com cn2Label=msgSize cn2=1204948 cn3Label
=emailThreatType cn3=4 fname=JNSA%20CSIRT-%E3%82%AA%E3%83%AA%E
3%83%91%E3%83%A9.pdf suser=user2@domain.com dvcmac=C4:34:6B:B8
:09:BC cs1Label=emailThreats cs1=VAN_MALWARE.UMXX threatName=V
```

```
AN_MALWARE.UMXX cs2Label=msgUuid cs2=ECBC7B7E-1397-3005-94C5-0
BA1DA0913D2
```

TMEF Detection Logs: URL Detection Logs

TABLE 5-3. TMEF Detection Logs: URL Detection Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	URL severity	• 4: Low • 6: Medium • 8: High

TMEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized • encrypted
cn1	Email severity	• 4: Low • 6: Medium • 8: High
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize

TMEF KEY	DESCRIPTION	VALUE
cn3	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
cn3Label	Threat type	emailThreatType
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	emailThreats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	Email ID	messageId
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	Email recipients	Example: user1@domain2.com;test@163.com

TMEF 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
mailMsgSubject	Email subject	Example: hello
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+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
urlCat	Category	Example: 90:02

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|100132|URL_DETECTION|6|rt=Apr 13 2015
16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3=<2
0150413084922.2052D1E9A066@internalbeta.bcc.ddei cn1Label=emai
lSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2933, Is
sue 13 request=http://202.502.27.71:6610/ctldl.windowsupdate.c
om/msdownload/update/v3/static/trustedr/en/disallowedcertstl.c
ab?7f8b3bbc9534919b?7f8b3bbc9534919b act=passed dvchost=intern
albeta.bcc.ddei dvc=10.64.1.131 duser=user1@domain.com cn2Labe
l=msgSize cn2=1204948 cn3Label=emailThreatType cn3=4 suser=use
r2@domain.com dvcmac=C4:34:6B:B8:09:BC cs1Label=emailThreats c
s1=VAN_MALWARE.UMXX deviceGUID=034eb532-9318-40d9-b27b-d9feba7
c269e cs2Label=msgUuid cs2=ECBC7B7E-1397-3005-94C5-0BA1DA0913D
2
```

TMEF Alert Logs

TABLE 5-4. TMEF Alert Logs

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	• 2: Informational • 6: Important • 8: Critical
cn1	Alert type	• 0: System event • 1: Security event and the event severity is "High", "Medium", or "Low" • 2: Security event and the even severity is "High", or "Medium" • 3: Security event and the event severity is "High"
cn1Label	Alert type	ruleEventType

TMEF KEY	DESCRIPTION	VALUE
cs1	Description	Example: 1 or more messages detected with threats
cs1Label	Description	ruleCriteria
cs2	Triggered value	Example: 35
cs2Label	Triggered value	eventTriggeredValue

cs3	Notification content	Example:
		`The following email messages contain threats:`
		
		`Risk: Medium (Malware)`
		`Action: Quarantined`
		`Message ID: <20150619032243.5923E650365@localhost.ddei-164>`
		`Recipients: fake@test.com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263`
		`Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64)`
		`Detected: 2015-05-25 11:11:00`
		
		`Alert time: 2015-05-25 11:11:27 +0800`
		
		Note
		The maximum length is 20000 characters.

cs3Label	Notification content	ruleContent

TMEF KEY	DESCRIPTION	VALUE
deviceGUID	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
externalId	The logid in the alert database	Example: 1648
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
ruleId	Alert ID	Value between 1 and 15
ruleName	Alert name	Example: Security: Suspicious Messages Identified

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1009|300105|ALERT_EVENT|2|rt=Jun 19 2015 03
:22:58 GMT+00:00 cnt=7 deviceGUID=361a091c-addd-40cf-98e7-710e
43500a66 ruleId=10 cs2Label=ruleContent cs2=The%20number%20of%
20processed%20messages%20reached%20the%20specified%20threshold
%20%281%29.%0A%0AMessages%20processed%3A%207%0AChecking%20inte
rval%3A%200%20minutes%0A%0AAlert%20time%3A%202015-06-19%2003%3
A22%3A58%20%2B0000%0AGenerated%20by%3A%20localhost.ddei-164%20
%2810.204.253.164%29%0AManagement%20console%3A%20https%3A//10.
204.253.164/loginPage.ddei cs1Label=ruleCriteria cs1=At least
1 messages processed dvchost=localhost.ddei-164 dvc=10.204.253
.164 externalId=1694 ruleName=System: Processing Surge dvcmac=
00:50:56:01:2C:BC cn1Label=ruleEventType cn1=0
```

TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 5-5. TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200119
Header (eventName)	Description	FILE_ANALYZED
Header (severity)	Severity	3
cn1	Result of GRID/CSSS	• 0: GRID is not known good • 1: GRID is known good
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady

TMEF KEY	DESCRIPTION	VALUE
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
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+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200119|FILE_ANALYZED|3|rt=Apr 13 2015
08:58:20 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=inter
nalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID
=034eb532-9318-40d9-b27b-d9feba7c269e fname=JNSA CSIRT-example
.pdf fileHash=E07B349245FCDDB31CBF5A52012807E955D2EB7A malName
=VAN_MALWARE.UMXX fileType=Adobe Portable Document Format(PDF)
```

```
 fsize=875029 deviceOSName=win81en cn1Label=GRIDIsKnownGood cn
1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 5-6. TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL_ANALYZED
Header (severity)	Severity	3
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	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

TMEF KEY	DESCRIPTION	VALUE
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
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
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+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200126|URL_ANALYZED|3|rt=Apr 13 2015 0
8:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=intern
albeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID=
034eb532-9318-40d9-b27b-d9feba7c269e request=http://www.castel
ir.it/take/Small-9422.html fileHash=6389250B8468C46443FD775F6E
B744D6105B8DF3 deviceOSName=xpsp3en cn2Label=ROZRating cn2=3 c
n3Label=PcapReady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 5-7. TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200127
Header (eventName)	Description	NOTABLE_CHARACTERISITICS
Header (severity)	Severity	6
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
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: s1.bdstatic.com
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200127|NOTABLE_CHARACTERISTICS|6|rt=Ap
r 13 2015 08:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvc
host=internalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC
deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e fname=http://w
ww.castelir.it/take/Small-9422.html fileHash=6389250B8468C4644
3FD775F6EB744D6105B8DF3 fileType=URL fsize=0 ruleCategory=Susp
icious network or messaging activity ruleName=Queries DNS serv
er msg=s1.bdstatic.com deviceOSName=xpsp3en
```

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 5-8. TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	DENYLIST_CHANGE
Header (severity)	Severity	3
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

TMEF KEY	DESCRIPTION	VALUE
deviceExternalRiskType	Risk level	• 1: Low • 2: Medium • 3: High • 4: Confirmed Malware
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP 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+00:00
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	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|200120|DENYLIST_CHANGE|3|rt=Apr 14 201
5 10:25:24 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=int
ernalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGU
ID=034eb532-9318-40d9-b27b-d9feba7c269e cs1Label=type cs1=Deny
 List File SHA1 end=May 14 2015 09:59:20 GMT+00:00 act=Add fil
eHash=522A90D077884E880A454A4D8E1A315FCE36BB12 deviceExternalR
iskType=High
```

TMEF Message Tracking Logs

TABLE 5-9. TMEF Message Tracking Logs

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100136
Header (eventName)	Description	MESSAGE_TRACKING
Header (severity)	Email severity	• 2: Unavailable • 2: Unrated • 2: Normal • 4: Low • 6: Medium • 8: High

TMEF KEY	DESCRIPTION	VALUE
dvc	Appliance IP address	Examples: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
cs1Label	Label for Email ID	messageId
cs1	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	Label for internal email ID	msgUuid
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
mailMsgSubject	Email subject	Example: hello
reason	Reason for block action	Example: Timeout period expired
cs3Label	Latest status	latestStatus

TMEF KEY	DESCRIPTION	VALUE
cs3	Details	• Quarantined • Delivered • Delivery unsuccessful • Processing completed • Deleted
src	Source IP address	Example: 10.1.144.199
cs4Label	Label for sender email address	senderMail
cs4	Sender email address	Example: user1@domain.com
cs5Label	Label for recipient email address	rcptMail
cs5	Recipient email address	Example: user2@domain.com
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
cs6Label	Label for process history	procHistory
cs6	Process history	Example: Action taken by the device. The format: "timestamp1 act1,timestamp2 act2,…, timestampn actn"

Log sample:

```
May 15 16:08:12 internalbeta CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1154|100136|MESSAGE_TRACKING|2|rt=May
15 2018 08:02:50 GMT+00:00 src=199.59.150.74 deviceGUID=67067
637-acbf-46de-a22d-be8d0d976cd5 cs6Label=procHistory cs6=May
15 2018 08:02:50 GMT+00:00 Received,May 15 2018 08:02:51 GMT+
00:00 Sent for analysis,May 15 2018 08:07:52 GMT+00:00 Action
 set to 'pass',May 15 2018 08:07:52 GMT+00:00 Processing comp
leted  mailMsgSubject=BBC News (World)"US to open controversi
al Jerusalem embassy" deviceTranslatedAddress=199.59.150.74 d
vchost=internalbeta.bcc.ddei dvc=10.64.1.131 duser=user1@doma
```

```
in.com cs1Label=messageId cs1=20180515080250.DEDC168349EC@int
ernalbeta.bcc.ddei cs4Label=senderMail cs4=info@twitter.com c
s5Label=rcptMail cs5=user2@domain2.com suser=n066660a6ef-3786
c6192ef34d49a9435fb49c655529-user2\=\=\=domain2.com@bounce.tw
itter.com dvcmac=EC:F4:BB:DE:E5:30 cs3Label=latestStatus cs3=
Processing completed cs2Label=msgUuid cs2=105D32B1-6C3A-0705-
954B-563DDB1B5714
```

TMEF Sender Filtering/Authentication Logs

TABLE 5-10. TMEF Sender Filtering/Authentication Logs

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	CEF format version	1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100137
Header (eventName)	Description	SENDER_FILTERING
Header (severity)	Email severity	2
dvc	Appliance IP address	Examples: • IPV4:192.168.10.1 • IPv6:2620:0101:4002:0401::131
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9

TMEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00 (UTC time)
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
cn1Label	Label for event type	eventType
cn1	Event type	• 1: Email reputation • 2: DHA protection • 3: Bounce attack protection • 4: SMTP traffic throttling (IP address) • 5: SMTP traffic throttling (email address) • 6: SPF • 7: DKIM • 8: DMARC
act	The action in the event	• 2: Block temporarily • 3: Block permanently
cn2Label	Label for sender authentication result	rfcResult

TMEF KEY	DESCRIPTION	VALUE
cn2	Sender authentication result	• 1: None • 2: Pass • 3: Neutral • 4: SoftFail • 5: Fail • 6: TempError • 7: PermError
reason	Reason for block action	Example: No DNS txt record

Log sample:

```
May 15 16:08:12  internalbeta CEF:0|Trend Micro|Deep Discovery
 Email Inspector|3.1.0.1147|100137|SENDER_FILTERING|2|rt=May 1
5 2018 08:20:01 GMT+00:00 cn1Label=eventType cn1=7 cn2Label=
rfcResult cn2=5 deviceTranslatedAddress=10.206.155.122 dvchost
=localhost.localdomain dvc=10.206.155.128 act=2 duser=user1@do
main.com reason=102 deviceGUID=15129231-f1dc-4941-8014-1a1b9fb
c9253 suser=user1@domain2.com dvcmac=00:0C:29:8D:2E:74
```

TMEF System Logs

TABLE 5-11. TMEF System Logs

TMEF KEY	DESCRIPTION	VALUE
Header (timestamp)	Local time in the format: "Mmm dd hh:mm:ss"	Example: Dec 5 05:26:45
Header (host)	Hostname without the domain information	Example: internalAP1
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro

TMEF KEY	DESCRIPTION	VALUE
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)
Header (eventName)	Description	• PRODUCT_UPDATE (300102) • SYSTEM_EVENT (300999)
Header (severity)	Severity	3
cn1	Event ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
cn1Label	Event ID	operationId
deviceGUID	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
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Ema
il Inspector|2.5.1.1161|300999|SYSTEM_EVENT|3|rt=Apr 13 2015 0
```

```
9:31:08 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC deviceGUID=034eb532
-9318-40d9-b27b-d9feba7c269e cn1Label=operationId cn1=30000 ms
g=Login: 'admin' logged on from 10.204.253.21 dvchost=internal
beta.bcc.ddei dvc=10.204.253.163
```

MTA Logs

There is no syslog content mapping information for MTA logs. Deep Discovery Email Inspector sends raw MTA logs directly to syslog servers.

Log sample:

```
04-27-2018 09:57:51 Mail.Info 10.206.155.128 Apr 27 09:57:
51 localhost postfix/smtpd[19318]: proxy-accept: END-OF-ME
SSAGE: 250 2.0.0 Ok: queued as DEC594A7815; from=<user1@do
main1.com> to=<user2@domain2.com> proto=SMTP
helo=<test.com>
```

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: APEM58978/200508