



# 5.1

## TREND MICRO™ Deep Discovery™ Email Inspector

### Syslog Content Mapping Guide

Advanced Protection Against Targeted Email Threats



Endpoint Security



Network Security



Protected Cloud



Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

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

Trend Micro, the Trend Micro t-ball logo, Trend Micro Apex One, Trend Micro Apex Central, and Deep Discovery are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2021. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM59196/210115

Release Date: April 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](mailto: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 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

## **Preface**

Preface .....	v
Documentation .....	vi
Audience .....	vii
Document Conventions .....	vii
About Trend Micro .....	viii

## **Chapter 1: Introduction**

Syslog Events .....	1-2
Terminology .....	1-3

## **Chapter 2: Revision History**

## **Chapter 3: Syslog Content Mapping - CEF**

CEF Detection Logs: Email Detection Logs .....	3-3
CEF Detection Logs: Attachment Detection Logs .....	3-6
CEF Detection Logs: URL Detection Logs .....	3-8
CEF Alert Logs .....	3-9
CEF Virtual Analyzer Analysis Logs: File Analysis Events .....	3-12
CEF Virtual Analyzer Analysis Logs: URL Analysis Events .....	3-15
CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events .....	3-16
CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events .....	3-18
CEF Message Tracking Logs .....	3-20
CEF Sender Filtering/Authentication Logs .....	3-23

CEF System Logs .....	3-26
CEF Time-of-Click Protection Logs .....	3-27
MTA Logs .....	3-29

## **Chapter 4: Syslog Content Mapping - LEEF**

LEEF Detection Logs: Email Detection Logs .....	4-3
LEEF Detection Logs: Attachment Detection Logs .....	4-6
LEEF Detection Logs: URL Detection Logs .....	4-9
LEEF Alert Logs .....	4-13
LEEF Virtual Analyzer Analysis Logs: File Analysis .....	4-16
LEEF Virtual Analyzer Analysis Logs: URL Analysis .....	4-18
LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events .....	4-20
LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events .....	4-22
LEEF Message Tracking Logs .....	4-24
LEEF Sender Filtering/Authentication Logs .....	4-27
LEEF System Logs .....	4-29
LEEF Time-of-Click Protection Logs .....	4-30
MTA Logs .....	4-32

## **Chapter 5: Syslog Content Mapping - TMEF**

TMEF Detection Logs: Email Detection Logs .....	5-3
TMEF Detection Logs: Attachment Detection Logs .....	5-6
TMEF Detection Logs: URL Detection Logs .....	5-10
TMEF Alert Logs .....	5-13
TMEF Virtual Analyzer Analysis Logs: File Analysis Events ..	5-16
TMEF Virtual Analyzer Analysis Logs: URL Analysis Events .	5-18

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events .....	5-20
TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events .....	5-21
TMEF Message Tracking Logs .....	5-24
TMEF Sender Filtering/Authentication Logs .....	5-27
TMEF System Logs .....	5-29
TMEF Time-of-Click Protection Logs .....	5-30
MTA Logs .....	5-33

## **Index**

Index .....	IN-1
-------------	------





# Preface

## Preface

Learn more about the following topics:

- *Documentation on page vi*
- *Audience on page vii*
- *Document Conventions on page vii*
- *About Trend Micro on page viii*

## 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: <a href="https://success.trendmicro.com">https://success.trendmicro.com</a>

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

<https://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
<b>Bold</b>	Menus and menu commands, command buttons, tabs, and options
<i>Italics</i>	References to other documents
Monospace	Sample command lines, program code, web URLs, file names, and program output
<b>Navigation &gt; Path</b>	The navigation path to reach a particular screen  For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface
 <b>Note</b>	Configuration notes
 <b>Tip</b>	Recommendations or suggestions
 <b>Important</b>	Information regarding required or default configuration settings and product limitations
 <b>WARNING!</b>	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 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 <a href="#">Syslog Content Mapping - CEF on page 3-1</a>	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 <a href="#">Syslog Content Mapping - LEEF on page 4-1</a>	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 <a href="#">Syslog Content Mapping - TMEF on page 5-1</a>	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).



<b>EVENT</b>	<b>DESCRIPTION</b>
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.
Time-of-Click Protection Logs	These logs contain information on the detections of URLs at the time of user clicks and the actions performed.

## Terminology

<b>TERM</b>	<b>DESCRIPTION</b>
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
5.1	<ul style="list-style-type: none"> <li>• Added recipient changed event for message tracking logs</li> <li>• Added recipient changed action for email detection logs</li> <li>• Added Time-of-Click Protection logs for syslog events</li> </ul>
3.1	<ul style="list-style-type: none"> <li>• Added Unsuccessful DKIM Signing system alert</li> <li>• Added new logs for the following events:               <ul style="list-style-type: none"> <li>• Message tracing</li> <li>• Sender filtering/authentication</li> <li>• MTA</li> </ul> </li> </ul>

VERSION	DESCRIPTION
3.0	<ul style="list-style-type: none"><li>• Added the following for email detection logs:<ul style="list-style-type: none"><li>• Unavailable severity type</li><li>• deleted, delivered directly, and cleaned up action types</li><li>• Spam/Graymail, Phishing, and Content violation threat types</li></ul></li><li>• Added Unavailable severity type for attachment detection logs</li><li>• Added new system alerts:<ul style="list-style-type: none"><li>• Account Locked</li><li>• Low Free Spam Quarantine Disk Space</li><li>• Long Message Deferred Queue</li></ul></li><li>• Renamed the following system alerts:<ul style="list-style-type: none"><li>• "Quarantined Messages" to "Quarantined Messages with Detected Threats"</li><li>• "Detection Surge" to "Threat Detection Surge"</li><li>• "Low Free Quarantine Disk Space" to "Low Free Threat Quarantine Disk Space"</li></ul></li></ul>
2.6	Added High Memory Usage system alert log
2.5 SP1	<ul style="list-style-type: none"><li>• Removed Signature ID (eventid) for the following LEEF logs:<ul style="list-style-type: none"><li>• Email detection logs</li><li>• Attachment detection logs</li><li>• URL detection logs</li><li>• Alert logs</li></ul></li><li>• Added Quarantined Messages security alert log</li></ul>
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 on page 3-3*
- *CEF Detection Logs: Attachment Detection Logs on page 3-6*
- *CEF Detection Logs: URL Detection Logs on page 3-8*
- *CEF Alert Logs on page 3-9*
- *CEF Virtual Analyzer Analysis Logs: File Analysis Events on page 3-12*
- *CEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 3-15*
- *CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 3-16*
- *CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 3-18*
- *CEF Message Tracking Logs on page 3-20*
- *CEF Sender Filtering/Authentication Logs on page 3-23*
- *CEF System Logs on page 3-26*
- *CEF Time-of-Click Protection Logs on page 3-27*

- *MTA Logs on page 3-29*

## 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: 5.1.0.1110
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"><li>• 2: Unavailable</li><li>• 4: Low</li><li>• 6: Medium</li><li>• 8: High</li></ul>

CEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: <ul style="list-style-type: none"><li>• analyzed</li><li>• cleaned up</li><li>• deleted</li><li>• delivered directly</li><li>• encrypted</li><li>• file sanitized</li><li>• passed</li><li>• quarantined</li><li>• recipient changed</li><li>• stamped</li><li>• stripped</li><li>• subjectsTagged</li></ul>
cn1	Threat type	<ul style="list-style-type: none"><li>• 1: Targeted malware</li><li>• 2: Malware</li><li>• 3: Malicious URL</li><li>• 4: Suspicious file</li><li>• 5: Suspicious URL</li><li>• 6: Spam/Graymail</li><li>• 7: Phishing</li><li>• 8: Content violation</li><li>• 9: DLP incident</li></ul>
cn1Label	Threat type	threatType
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize



CEF KEY	DESCRIPTION	VALUE
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
cs5	Recipient email address	Example: user2@domain.com
cs5Label	Label for recipient email address	rcptMail
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FB8B28-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

CEF KEY	DESCRIPTION	VALUE
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.R02SC00LH14|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: 5.1.0.1110
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION

CEF KEY	DESCRIPTION	VALUE
Header (severity)	Severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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

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
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:


```
Jan 18 10:49:41 ddei5 CEF:0|Trend Micro|Deep Discovery Email
Inspector|5.1.0.1288|100132|URL_DETECTION|6|rt=Jan 18 2023
10:49:39 GMT+00:00 cs2Label=msgUuid cs2=DA1CCCE4-F287-9205-9
939-89E26E97D9E0 dvcmac=00:50:56:98:9C:99 dvchost=ddei5.1-c7
-en-140.com request=http://wrs21.winshipway.com/ deviceExter
nalId=411b541a-fa18-4bbf-8e6d-9a9c19276bf7 cs1Label=threats
cs1=TSPY_KEYLOG.GC dvc=10.64.1.140 cat=74
```

## 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

<b>CEF KEY</b>	<b>DESCRIPTION</b>	<b>VALUE</b>
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	<ul style="list-style-type: none"><li>• 2: Informational</li><li>• 6: Important</li><li>• 8: Critical</li></ul>
cs1	Alert name	Example: Security: Suspicious Messages Identified
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

CEF KEY	DESCRIPTION	VALUE
cs4	Notification content	<p>Example:</p> <pre>The following email messages contain threats:  Risk: Medium (Malware) Action: Quarantined Message ID: &lt;201506190 32243.5923E650365@loca lhost.ddei-164&gt; Recipients: fake@test. com;test@test.com Sender: test@fake.test Subject: high_4_file_ 507ECC33FA60979F6B97D 84DA47972096185C263 Attachment: 4_file_50 7ECC33FA60979F6B97D84D A47972096185C263 (MIME Base64) Detected: 2015-05-25 11:11:00  Alert time: 2015-05-25 11:11:27 +0800</pre> <hr/> <p> <b>Note</b> The maximum length is 1023 characters.</p>
cs4Label	Notification content	ruleContent
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FB28-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





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: 5.1.0.1110
Header (eventid)	Signature ID	200119
Header (eventName)	Description	Sample file sandbox analysis is finished
Header (severity)	Severity	3: Informational
cn1	Result of GRID/CSSS	<ul style="list-style-type: none"> <li>• 0: GRID is not known good</li> <li>• 1: GRID is known good</li> </ul>
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
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: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
cs3Label	Parent SHA1	ParentFileSHA1

CEF KEY	DESCRIPTION	VALUE
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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: 5.1.0.1110
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	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
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

CEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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

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: 5.1.0.1110
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: 6B593E17AFB7-40FB28-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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

CEF KEY	DESCRIPTION	VALUE
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 dvmac=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

CEF KEY	DESCRIPTION	VALUE
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3
act	The action in the event	<ul style="list-style-type: none"> <li>• Add</li> <li>• Remove</li> </ul>
cs1	Deny List type	<ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul>
cs1Label	Deny List type	type
cs2	Risk level	<ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Confirmed Malware</li> </ul>
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

CEF KEY	DESCRIPTION	VALUE
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
request	URL	Example: http://www.rainking.net/? utm_campaign=4-21-2014  http:// images.rainking.net/eloquimage
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



CEF KEY	DESCRIPTION	VALUE
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: 5.1.0.1110
Header (eventid)	Signature ID	100136
Header (eventName)	Description	MESSAGE_TRACKING
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 2: Unrated</li> <li>• 2: Normal</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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: 6B593E17AFB7-40FB28-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

CEF KEY	DESCRIPTION	VALUE
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	<ul style="list-style-type: none"><li>• Deleted</li><li>• Delivered</li><li>• Delivery unsuccessful</li><li>• Processing completed</li><li>• Quarantined</li><li>• Recipient changed</li></ul>
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

CEF KEY	DESCRIPTION	VALUE
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

<b>CEF KEY</b>	<b>DESCRIPTION</b>	<b>VALUE</b>
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: 5.1.0.1110
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)
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

CEF KEY	DESCRIPTION	VALUE
cn1	Event type	<ul style="list-style-type: none"> <li>• 1: Email reputation</li> <li>• 2: DHA protection</li> <li>• 3: Bounce attack protection</li> <li>• 4: SMTP traffic throttling (IP address)</li> <li>• 5: SMTP traffic throttling (email address)</li> <li>• 6: SPF</li> <li>• 7: DKIM</li> <li>• 8: DMARC</li> </ul>
act	The action in the event	<ul style="list-style-type: none"> <li>• 2: Block temporarily</li> <li>• 3: Block permanently</li> </ul>
cn2Label	Label for sender authentication result	rfcResult
cn2	Sender authentication result	<ul style="list-style-type: none"> <li>• 1: None</li> <li>• 2: Pass</li> <li>• 3: Neutral</li> <li>• 4: SoftFail</li> <li>• 5: Fail</li> <li>• 6: TempError</li> <li>• 7: PermError</li> </ul>
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: internalAPI
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: 5.1.0.1110
Header (eventid)	Signature ID	<ul style="list-style-type: none"> <li>• 300102 (PRODUCT_UPDATE)</li> <li>• 300999 (SYSTEM_EVENT)</li> </ul>
Header (eventName)	Description	<ul style="list-style-type: none"> <li>• PRODUCT_UPDATE (300102)</li> <li>• SYSTEM_EVENT (300999)</li> </ul>
Header (severity)	Severity	3
cn1	Event ID	<ul style="list-style-type: none"> <li>• SYSTEM_EVENT 20000-39999</li> <li>• PRODUCT_UPDATE 10000-19999</li> </ul>
cn1Label	Event ID	operationId

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
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
```

## CEF Time-of-Click Protection Logs

**TABLE 3-12. CEF: Time-of-Click Protection 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

CEF KEY	DESCRIPTION	VALUE
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	100139
Header (eventName)	Description	CTP_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 2: Unrated</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FB28-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
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT +00:00
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014  http://images.rainking.net/eloquimage
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• blocked</li> <li>• warned_and_stopped</li> <li>• warned_but_accessed</li> </ul>
msg	Email subject	Example: hello
cs1	Names of threats in the email	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>



CEF KEY	DESCRIPTION	VALUE
cs1Label	Names of threats in the email	messageId
cs2	Sender email address	Example: user1@domain.com
cs2Label	Label for sender email address	senderMail
cs3	Recipient email address	Example: user2@domain.com
cs3Label	Label for recipient email address	rcptMail
cs4	The time of URL click	Example: Mar 09 2015 17:05:21 GMT +00:00
cs4Label	Label for time of URL click	timeOfClick
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com

### Log sample:

```
Dec 16 06:32:36 ddei-172 CEF:0|Trend Micro|Deep Discovery
Email Inspector|5.1.0.1110|100139|CTP_DETECTION|8|rt=Dec
16 2020 06:30:08 GMT+00:00 cs2Label=senderMail cs2=tarek@
test.com request=http://g9yxzah7yu23n.com suser=tarek@tes
t.com dvchost=ddei-172 dvc=10.204.63.172 deviceExternalId
=2bcbcc98-3f99-40e3-864f-e5f102511631 duser=ddei_test1@de
mo.com msg=syslog - ctp cs3Label=rcptMail cs3=ddei_test1@
demo.com cs1Label=messageId cs1=2020121613571222594383@te
st.com act=blocked dvcmac=00:50:56:A7:D9:FD cs4Label=time
OfClick cs4=Dec 16 2020 06:30:36 GMT+00:00
```

## 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:

- *LEEF Detection Logs: Email Detection Logs on page 4-3*
- *LEEF Detection Logs: Attachment Detection Logs on page 4-6*
- *LEEF Detection Logs: URL Detection Logs on page 4-9*
- *LEEF Alert Logs on page 4-13*
- *LEEF Virtual Analyzer Analysis Logs: File Analysis on page 4-16*
- *LEEF Virtual Analyzer Analysis Logs: URL Analysis on page 4-18*
- *LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 4-20*
- *LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 4-22*
- *LEEF Message Tracking Logs on page 4-24*
- *LEEF Sender Filtering/Authentication Logs on page 4-27*
- *LEEF System Logs on page 4-29*
- *LEEF Time-of-Click Protection Logs on page 4-30*

- [MTA Logs on page 3-29](#)



**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: 5.1.0.1110
Header (eventName)	Event Name	EMAIL_DETECTION
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• analyzed</li> <li>• cleaned up</li> <li>• deleted</li> <li>• delivered directly</li> <li>• encrypted</li> <li>• file sanitized</li> <li>• passed</li> <li>• quarantined</li> <li>• recipient changed</li> <li>• stamped</li> <li>• stripped</li> <li>• subjectsTagged</li> </ul>
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
messageld	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	<ul style="list-style-type: none"><li>• 2: Unavailable</li><li>• 4: Low</li><li>• 6: Medium</li><li>• 8: High</li></ul>
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.JMXX FRAUD_PHISHING.WRS

LEEF KEY	DESCRIPTION	VALUE
threatType	Threat type	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>

**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: 5.1.0.1110
Header (eventName)	Event Name	ATTACHMENT_DETECTION
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• analyzed</li> <li>• cleaned up</li> <li>• deleted</li> <li>• delivered directly</li> <li>• encrypted</li> <li>• file sanitized</li> <li>• passed</li> <li>• quarantined</li> <li>• recipient changed</li> <li>• stamped</li> <li>• stripped</li> <li>• subjectsTagged</li> </ul>
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
emailSeverity	Email severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX  FRAUD_PHISHING.WRS
emailThreatType	Threat type	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

LEEF Key	DESCRIPTION	VALUE
mailMsgSubject	Email subject	Example: hello
messageld	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	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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
id=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: 5.1.0.1110
Header (eventName)	Event Name	URL_DETECTION

LEEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: <ul style="list-style-type: none"><li>analyzed</li><li>cleaned up</li><li>deleted</li><li>delivered directly</li><li>encrypted</li><li>file sanitized</li><li>passed</li><li>quarantined</li><li>recipient changed</li><li>stamped</li><li>stripped</li><li>subjectsTagged</li></ul>
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
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	<ul style="list-style-type: none"> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX FRAUD_PHISHING.WRS
emailThreatType	Threat type	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>
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	<ul style="list-style-type: none"> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
src	Source IP address	Example: 10.1.144.199

LEEF KEY	DESCRIPTION	VALUE
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.ddei\0x09dvc=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: 5.1.0.1110
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	<p>Example:</p> <pre>The following email messages contain threats:  Risk: Medium (Malware) Action: Quarantined Message ID: &lt;201506190 32243.5923E650365@loca lhost.ddei-164&gt; 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</pre> <hr/> <p> <b>Note</b> The maximum length is 20000 characters.</p>
ruleCriteria	Description	Example: 1 or more messages detected with threats



LEEF KEY	DESCRIPTION	VALUE
ruleEventType	Alert type	<ul style="list-style-type: none"> <li>0: System event</li> <li>1: Security event and the event severity is "High", "Medium", or "Low"</li> <li>2: Security event and the even severity is "High", or "Medium"</li> <li>3: Security event and the event severity is "High"</li> </ul>
ruleId	Alert ID	Value between 1 and 15
ruleName	Alert name	Example: Security: Suspicious Messages Identified
sev	Severity	<ul style="list-style-type: none"> <li>2: Informational</li> <li>6: Important</li> <li>8: Critical</li> </ul>

**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: 5.1.0.1110
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: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
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

LEEF KEY	DESCRIPTION	VALUE
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
gridIsKnownGood	Result of GRID/CSSS	<ul style="list-style-type: none"> <li>• 0: GRID is not known good</li> <li>• 1: GRID is known good</li> </ul>
malName	Malware name	Example: HEUR_NAMETRICK.A
pcapReady	PCAP ready	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
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 DLL
L\0x09fsSize=482816\0x09deviceOSName=win81en\0x09gridIsKnownGood=-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: 5.1.0.1110
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: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
pcapReady	PCAP ready	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
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
alpha.bcc.ddei\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09dev
iceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fileHash=BF68
52C834224BD2C26AC4BE20E7E08930B39FEF\0x09deviceOSName=win7sp1e
n\0x09url=http://climorg.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: 5.1.0.1110
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
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
fileType	True file type	Example: RIFF bitmap file

LEEF KEY	DESCRIPTION	VALUE
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\{D78424A0E1AA-11E4-B7C5-7CC9C8DA4AD2}.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: 5.1.0.1110
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	<ul style="list-style-type: none"> <li>• Add</li> <li>• Remove</li> </ul>
deviceExternalRiskType	Risk level	<ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Confirmed Malware</li> </ul>
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57



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
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
pComp	Detection engine / component	Sandbox
sev	Severity	3
type	Deny List type	<ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul>
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\x09devTimeFormat=MMM dd yyyy HH:mm:ss \
0x09sev=3\x09pComp=Sandbox\x09dvc=10.64.1.131\x09dvchost=in
ternalbeta.bcc.ddei\x09deviceMacAddress=C4:34:6B:B8:09:BC\x0
9deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\x09end=May 1
3 2015 07:44:37 GMT+00:00\x09act=Add\x09dst=200.98.168.34\x
09dpt=80\x09deviceExternalRiskType=Medium\x09type=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: 5.1.0.1110
Header (eventName)	Event Name	MESSAGE_TRACKING
sev	Email severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 2: Unrated</li> <li>• 2: Normal</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>

LEEF KEY	DESCRIPTION	VALUE
dvc	Appliance IP address	Examples: <ul style="list-style-type: none"> <li>• IPV4:192.168.10.1</li> <li>• IPV6:2620:0101:4002:0401::131</li> </ul>
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
messageld	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
reason	Reason for block action	Example: Timeout period expired
latestStatus	Latest status	<ul style="list-style-type: none"> <li>• Deleted</li> <li>• Delivered</li> <li>• Delivery unsuccessful</li> <li>• Processing completed</li> <li>• Quarantined</li> <li>• Recipient changed</li> </ul>

LEEF KEY	DESCRIPTION	VALUE
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 16:00:47 internalbeta LEEF:1.0|Trend Micro|Deep Discovery 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 GMT+00:00 Action set to 'pass',May 15 2018 08:00:33 GMT+00:00 Processing completed<009>msgUuid=46252714-6C39-FF05-98F4-5C63BCB20569<009>mailMsgSubject=Time is running out: New data privacy permissions<009>src=104.130.122.63<009>senderMail=sap@mailsap.com<009>sender=bounce+814a73.7ecda73-jeff_lovelace@trendmicro.com@mailsap.com<009>dvchost=internalbeta.bcc.ddei<009>dvc=10.64.1.131<009>duser=jeff_lovelace@trendmicro.com<009>deviceGUID=67067637-acbf-46de-a22d-be8d0d976cd5<009>rcptMail=jeff_lovelace@trendmicro.com<009>devTime=May 15 2018 08:00:33 GMT+00:00<009>messageId=20180515080033.0EE4B6834964@internalbeta.bcc.ddei<009>dvcmac=EC:F4:BB:DE:E5:30<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>deviceTranslatedAddress=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: 5.1.0.1110
Header (eventName)	Description	SENDER_FILTERING
sev	Email severity	2
dvc	Appliance IP address	Examples: <ul style="list-style-type: none"> <li>• IPV4:192.168.10.1</li> <li>• IPV6:2620:0101:4002:0401::131</li> </ul>
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
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
suser	Email sender	Example: user2@domain.com

LEEF KEY	DESCRIPTION	VALUE
duser	Email recipients	Example: user1@domain2.com;test@163.com
eventType	Event type	<ul style="list-style-type: none"> <li>• 1: Email reputation</li> <li>• 2: DHA protection</li> <li>• 3: Bounce attack protection</li> <li>• 4: SMTP traffic throttling (IP address)</li> <li>• 5: SMTP traffic throttling (email address)</li> <li>• 6: SPF</li> <li>• 7: DKIM</li> <li>• 8: DMARC</li> </ul>
act	The action in the event	<ul style="list-style-type: none"> <li>• 2: Block temporarily</li> <li>• 3: Block permanently</li> </ul>
rfcResult	Sender authentication result	<ul style="list-style-type: none"> <li>• 1: None</li> <li>• 2: Pass</li> <li>• 3: Neutral</li> <li>• 4: SoftFail</li> <li>• 5: Fail</li> <li>• 6: TempError</li> <li>• 7: PermError</li> </ul>
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 Discovery Email Inspector|3.1.0.1147|SENDER_FILTERING|sev=2<009>deviceGUID=15129231-f1dc-4941-8014-1a1b9fbc9253<009>rfcResult=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: 5.1.0.1110
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
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

LEEF KEY	DESCRIPTION	VALUE
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
operationId	Event ID	<ul style="list-style-type: none"> <li>SYSTEM_EVENT 20000-39999</li> <li>PRODUCT_UPDATE 10000-19999</li> </ul>
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
```

## LEEF Time-of-Click Protection Logs

**TABLE 4-12. LEEF: Time-of-Click Protection 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



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: 5.1.0.1110
Header (eventName)	Description	CTP_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 2: Unrated</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT +00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
url	URL	Example: http://1.2.3.4/query?term=value
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• blocked</li> <li>• warned_and_stopped</li> <li>• warned_but_accessed</li> </ul>
mailMsgSubject	Email subject	Example: hello

LEEF KEY	DESCRIPTION	VALUE
messageld	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
senderMail	Sender email address	Example: user1@domain.com
rcptMail	Recipient email address	Example: user2@domain.com
timeOfClick	The time of URL click	Example: Mar 09 2015 17:05:21 GMT +00:00
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com

#### Log sample:

```
Dec 16 06:38:57 ddei-172 LEEF:1.0|Trend Micro|Deep Discovery
Email Inspector|5.1.0.1110|CTP_DETECTION|deviceGUID=2bcbcc9
8-3f99-40e3-864f-e5f102511631<009>mailMsgSubject=syslog - ct
p<009>url=http://g9yxzah7yu23n.com<009>dvcHost=ddei-172<009>
messageId=2020121613571222594383@test.com<009>senderMail=tarek@test.com<009>dvc=10.204.63.172<009>act=blocked<009>duser=ddei_test1@demo.com<009>rcptMail=ddei_test1@demo.com<009>devTime=Dec 16 2020 06:30:08 GMT+00:00<009>timeOfClick=Dec 16 2020 06:36:56 GMT+00:00<009>dvcMac=00:50:56:A7:D9:FD<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>suser=tarek@test.com
```

## 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 on page 5-3*
- *TMEF Detection Logs: Attachment Detection Logs on page 5-6*
- *TMEF Detection Logs: URL Detection Logs on page 5-10*
- *TMEF Alert Logs on page 5-13*
- *TMEF Virtual Analyzer Analysis Logs: File Analysis Events on page 5-16*
- *TMEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 5-18*
- *TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 5-20*
- *TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 5-21*
- *TMEF Message Tracking Logs on page 5-24*
- *TMEF Sender Filtering/Authentication Logs on page 5-27*
- *TMEF System Logs on page 5-29*
- *TMEF Time-of-Click Protection Logs on page 5-30*

- *MTA Logs on page 3-29*

## 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: 5.1.0.1110
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"><li>• 2: Unavailable</li><li>• 4: Low</li><li>• 6: Medium</li><li>• 8: High</li></ul>

TMEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>analyzed</li> <li>cleaned up</li> <li>deleted</li> <li>delivered directly</li> <li>encrypted</li> <li>file sanitized</li> <li>passed</li> <li>quarantined</li> <li>recipient changed</li> <li>stamped</li> <li>stripped</li> <li>subjectsTagged</li> </ul>
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



TMEF KEY	DESCRIPTION	VALUE
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
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	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Email Inspector|2.5.1.1161|100130|EMAIL_DETECTION|8|rt=Apr 13 2015 08:49:22 GMT+00:00 src=141.251.58.19 threatType=4 deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e mailMsgSubject=phishwatch Digest, Vol 2933, Issue 13 act=passed dvchost=internalbeta.bcc.ddei cs2Label=messageId cs2=<20150413084922.2052D1E9A066@internalbeta.bcc.ddei dvc=10.64.1.131 cs1Label=msgUuid cs1=ECBC7B7E-1397-3005-94C5-0BA1DA0913D2 duser=user1@domain2.com suser=user1@domain1.com dvcmac=C4:34:6B:B8:09:BC threatName=VAN_MALWARE.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: 5.1.0.1110
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Attachment severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>

TMEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• analyzed</li> <li>• cleaned up</li> <li>• deleted</li> <li>• delivered directly</li> <li>• encrypted</li> <li>• file sanitized</li> <li>• passed</li> <li>• quarantined</li> <li>• recipient changed</li> <li>• stamped</li> <li>• stripped</li> <li>• subjectsTagged</li> </ul>
cn1	Email severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize

TMEF KEY	DESCRIPTION	VALUE
cn3	Threat type	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>
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
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

TMEF KEY	DESCRIPTION	VALUE
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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 Email Inspector|2.5.1.1161|100131|ATTACHMENT_DETECTION|8|rt=Apr 13 2015 16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3=<20150413084922.2052D1E9A066@internalbeta.bcc.ddei cn1Label=emailSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2 933, Issue 13 fileHash=E07B349245FCDD31CBF5A52012807E955D2EB7A fileType=Directory act=passed dvchost=internalbeta.bcc.ddei dvc=10.64.1.131 deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e duser=user1@domain.com cn2Label=msgSize cn2=1204948 cn3Label=emailThreatType cn3=4 fname=JNSA%20CSIRT-%E3%82%AA%E3%83%AA%E3%83%91%E3%83%A9.pdf suser=user2@domain.com dvcmac=C4:34:6B:B8:09:BC cs1Label=emailThreats cs1=VAN_MALWARE.UMXX threatName=VAN_MALWARE.UMXX cs2Label=msgUuid cs2=ECBC7B7E-1397-3005-94C5-0BA1DA0913D2
```

## 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: 5.1.0.1110
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	URL severity	<ul style="list-style-type: none"> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
act	The action in the event	<p>Examples:</p> <ul style="list-style-type: none"> <li>• analyzed</li> <li>• cleaned up</li> <li>• deleted</li> <li>• delivered directly</li> <li>• encrypted</li> <li>• file sanitized</li> <li>• passed</li> <li>• quarantined</li> <li>• recipient changed</li> <li>• stamped</li> <li>• stripped</li> <li>• subjectsTagged</li> </ul>

<b>TMEF KEY</b>	<b>DESCRIPTION</b>	<b>VALUE</b>
cn1	Email severity	<ul style="list-style-type: none"> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize
cn3	Threat type	<ul style="list-style-type: none"> <li>• 1: Targeted malware</li> <li>• 2: Malware</li> <li>• 3: Malicious URL</li> <li>• 4: Suspicious file</li> <li>• 5: Suspicious URL</li> <li>• 6: Spam/Graymail</li> <li>• 7: Phishing</li> <li>• 8: Content violation</li> <li>• 9: DLP incident</li> </ul>
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>

TMEF KEY	DESCRIPTION	VALUE
cs3Label	Email ID	messageId
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
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 http://images.rainking.net/elouquimage
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:

```
Jan 18 10:59:21 ddei5 CEF:0|Trend Micro|Deep Discovery Email Inspector|5.1.0.1288|100132|URL_DETECTION|6|rt=Jan 18 2023 10:59:20 GMT+00:00 src=10.64.1.201 deviceGUID=411b541a-fa18-4bbf-8e6d-9a9c19276bf7 cn1Label=emailSeverity cn1=6 mailMsgSubject=test url detection urlCat=74 request=http://wrs21.winshipway.com/ cs3Label=messageId cs3=<2023021017391312383819@imsstest.com> dvchost=ddei5.1-c7-en-140.com dvc=10.64.1.140 act=quarantined duser=floyd_recipient@imsstest.com cs2Label=msgUuid cs2=24FA1D28-F287-B105-BA7E-CB16F55712F2 cn3Label=emailThreatType cn3=3 suser=f
```




```
loyd_sender@imsstest.com dvcmac=00:50:56:98:9C:99 cn2Label=msgSize cn2=2286
```

## 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: 5.1.0.1110
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	<ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 6: Important</li> <li>• 8: Critical</li> </ul>
cn1	Alert type	<ul style="list-style-type: none"> <li>• 0: System event</li> <li>• 1: Security event and the event severity is "High", "Medium", or "Low"</li> <li>• 2: Security event and the even severity is "High", or "Medium"</li> <li>• 3: Security event and the event severity is "High"</li> </ul>

TMEF KEY	DESCRIPTION	VALUE
cn1Label	Alert type	ruleEventType
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	<p>Example:</p> <pre>The following email messages contain threats:  Risk: Medium (Malware) Action: Quarantined Message ID: &lt;201506190 32243.5923E650365@loca lhost.ddei-164&gt; Recipients: fake@test. com;test@test.com Sender: test@fake.test Subject: high_4_file_ 507ECC33FA60979F6B97D 84DA47972096185C263 Attachment: 4_file_50 7ECC33FA60979F6B97D84 DA47972096185C263 (MIME Base64) Detected: 2015-05-25 11:11:00  Alert time: 2015-05-25 11:11:27 +0800</pre> <hr/> <p> <b>Note</b> The maximum length is 20000 characters.</p>
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 Email 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-98e7-710e43500a66 ruleId=10 cs2Label=ruleContent cs2=The%20number%20of%20processed%20messages%20reached%20the%20specified%20threshold%20%281%29.%0A%0AMessages%20processed%3A%207%0AChecking%20interval%3A%200%20minutes%0A%0AAlert%20time%3A%202015-06-19%2003%3A22%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: 5.1.0.1110
Header (eventid)	Signature ID	200119
Header (eventName)	Description	FILE_ANALYZED
Header (severity)	Severity	3
cn1	Result of GRID/CSSS	<ul style="list-style-type: none"> <li>• 0: GRID is not known good</li> <li>• 1: GRID is known good</li> </ul>
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
cn3Label	PCAP ready	PcapReady
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FB8B28-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: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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 Email 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=internalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e fname=JNSA CSIRT-example.pdf fileHash=E07B349245FCDDDB31CBF5A52012807E955D2EB7A malName=VAN_MALWARE.UMXX fileType=Adobe Portable Document Format(PDF) fsize=875029 deviceOSName=win81en cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRrating 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: 5.1.0.1110
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	<ul style="list-style-type: none"> <li>• 0: PCAP is not ready</li> <li>• 1: PCAP is ready</li> </ul>
cn3Label	PCAP ready	PcapReady
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

TMEF KEY	DESCRIPTION	VALUE
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B 6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
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 Email Inspector|2.5.1.1161|200126|URL_ANALYZED|3|rt=Apr 13 2015 08:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=internalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e request=http://www.castelir.it/take/Small-9422.html fileHash=6389250B8468C46443FD775F6EB744D6105B8DF3 deviceOSName=xpsp3en cn2Label=ROZRating cn2=3 cn3Label=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: 5.1.0.1110
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar



TMEF KEY	DESCRIPTION	VALUE
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 Email Inspector|2.5.1.1161|200127|NOTABLE_CHARACTERISTICS|6|rt=Apr 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://www.castelir.it/take/Small-9422.html fileHash=6389250B8468C46443FD775F6EB744D6105B8DF3 fileType=URL fsize=0 ruleCategory=Suspicious network or messaging activity ruleName=Queries DNS server 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

<b>TMEF KEY</b>	<b>DESCRIPTION</b>	<b>VALUE</b>
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: 5.1.0.1110
Header (eventid)	Signature ID	200120
Header (eventName)	Description	DENYLIST_CHANGE
Header (severity)	Severity	3
act	The action in the event	<ul style="list-style-type: none"> <li>• Add</li> <li>• Remove</li> </ul>
cs1	Deny List type	<ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul>
cs1Label	Deny List type	type
deviceExternalRiskType	Risk level	<ul style="list-style-type: none"> <li>• 1: Low</li> <li>• 2: Medium</li> <li>• 3: High</li> <li>• 4: Confirmed Malware</li> </ul>
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

TMEF KEY	DESCRIPTION	VALUE
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: 1EDD5B38DE4729545767088C5CAB 395E4197C8F3
pComp	Detection engine / component	Sandbox
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014  http://images.rainking.net/eloquimage
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|2.5.1.1161|200120|DENYLIST_CHANGE|3|rt=Apr 14 2015 10:25:24 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=internalbeta.bcc.ddei deviceMacAddress=C4:34:6B:B8:09:BC deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e cs1Label=type cs1=Deny List File SHA1 end=May 14 2015 09:59:20 GMT+00:00 act=Add fileHash=522A90D077884E880A454A4D8E1A315FCE36BB12 deviceExternalRiskType=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: 5.1.0.1110
Header (eventid)	Signature ID	100136
Header (eventName)	Description	MESSAGE_TRACKING
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 2: Unavailable</li> <li>• 2: Unrated</li> <li>• 2: Normal</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
dvc	Appliance IP address	Examples: <ul style="list-style-type: none"> <li>• IPV4:192.168.10.1</li> <li>• IPV6:2620:0101:4002:0401::131</li> </ul>
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost

TMEF KEY	DESCRIPTION	VALUE
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
cs3	Details	<ul style="list-style-type: none"> <li>• Deleted</li> <li>• Delivered</li> <li>• Delivery unsuccessful</li> <li>• Processing completed</li> <li>• Quarantined</li> <li>• Recipient changed</li> </ul>
src	Source IP address	Example: 10.1.144.199
cs4Label	Label for sender email address	senderMail

TMEF KEY	DESCRIPTION	VALUE
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: 5.1.0.1110
Header (eventid)	Signature ID	100137
Header (eventName)	Description	SENDER_FILTERING
Header (severity)	Email severity	2
dvc	Appliance IP address	Examples: <ul style="list-style-type: none"> <li>• IPV4:192.168.10.1</li> <li>• IPV6:2620:0101:4002:0401::131</li> </ul>
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)
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
suser	Email sender	Example: user2@domain.com

TMEF KEY	DESCRIPTION	VALUE
duser	Email recipients	Example: user1@domain2.com;test@163.com
cn1Label	Label for event type	eventType
cn1	Event type	<ul style="list-style-type: none"> <li>• 1: Email reputation</li> <li>• 2: DHA protection</li> <li>• 3: Bounce attack protection</li> <li>• 4: SMTP traffic throttling (IP address)</li> <li>• 5: SMTP traffic throttling (email address)</li> <li>• 6: SPF</li> <li>• 7: DKIM</li> <li>• 8: DMARC</li> </ul>
act	The action in the event	<ul style="list-style-type: none"> <li>• 2: Block temporarily</li> <li>• 3: Block permanently</li> </ul>
cn2Label	Label for sender authentication result	rfcResult
cn2	Sender authentication result	<ul style="list-style-type: none"> <li>• 1: None</li> <li>• 2: Pass</li> <li>• 3: Neutral</li> <li>• 4: SoftFail</li> <li>• 5: Fail</li> <li>• 6: TempError</li> <li>• 7: PermError</li> </ul>
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
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	<ul style="list-style-type: none"> <li>• 300102 (PRODUCT_UPDATE)</li> <li>• 300999 (SYSTEM_EVENT)</li> </ul>
Header (eventName)	Description	<ul style="list-style-type: none"> <li>• PRODUCT_UPDATE (300102)</li> <li>• SYSTEM_EVENT (300999)</li> </ul>
Header (severity)	Severity	3
cn1	Event ID	<ul style="list-style-type: none"> <li>• SYSTEM_EVENT 20000-39999</li> <li>• PRODUCT_UPDATE 10000-19999</li> </ul>

TMEF KEY	DESCRIPTION	VALUE
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 Email Inspector|2.5.1.1161|300999|SYSTEM_EVENT|3|rt=Apr 13 2015 09:31:08 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e cn1Label=operationId cn1=30000 msg>Login: 'admin' logged on from 10.204.253.21 dvchost=internal.beta.bcc.ddei dvc=10.204.253.163
```

## TMEF Time-of-Click Protection Logs

**TABLE 5-12. TMEF: Time-of-Click Protection 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

<b>TMEF KEY</b>	<b>DESCRIPTION</b>	<b>VALUE</b>
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Email Inspector
Header (pver)	Appliance version	Example: 5.1.0.1110
Header (eventid)	Signature ID	100139
Header (eventName)	Description	CTP_DETECTION
Header (severity)	Email severity	<ul style="list-style-type: none"> <li>• 2: Unrated</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>
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
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT +00:00
request	URL	Example: <a href="http://www.rainking.net/?utm_campaign=4-21-2014">http://www.rainking.net/?utm_campaign=4-21-2014</a>   <a href="http://images.rainking.net/eloquaimage">http://images.rainking.net/eloquaimage</a>
act	The action in the event	Examples: <ul style="list-style-type: none"> <li>• blocked</li> <li>• warned_and_stopped</li> <li>• warned_but_accessed</li> </ul>
mailMsgSubject	Email subject	Example: hello

TMEF KEY	DESCRIPTION	VALUE
cs1	Message ID in the email	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs1Label	Label for the message ID in the email	messageId
cs2	Sender email address	Example: user1@domain.com
cs2Label	Label for sender email address	senderMail
cs3	Recipient email address	Example: user2@domain.com
cs3Label	Label for recipient email address	rcptMail
cs4	The time of URL click	Example: Mar 09 2015 17:05:21 GMT +00:00
cs4Label	Label for time of URL click	timeOfClick
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com

### Log sample:

```
Dec 16 06:42:06 ddei-172 CEF:0|Trend Micro|Deep Discovery
Email Inspector|5.1.0.1110|100139|CTP_DETECTION|8|rt=Dec
16 2020 06:30:08 GMT+00:00 cs2Label=senderMail cs2=tarek
@test.com deviceGUID=2bcbcc98-3f99-40e3-864f-e5f102511631
mailMsgSubject=syslog - ctp request=http://g9yxzah7yu23n
.com suser=tarek@test.com dvchost=ddei-172 dvc=10.204.63.
172 duser=ddei_test1@demo.com cs3Label=rcptMail cs3=ddei_
test1@demo.com cs1Label=messageId cs1=2020121613571222594
383@test.com act=blocked dvcmac=00:50:56:A7:D9:FD cs4Labe
l=timeOfClick cs4=Dec 16 2020 06:40:11 GMT+00:00
```

## 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](http://www.trendmicro.com)

Item Code: APEM59196/210115