JUNIPER NETWORKS | Engineering Simplicity

CEF, LEEF & Syslog Support for SIEM User's Guide

Published
2025-09-17

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

CEF, LEEF & Syslog Support for SIEM User's Guide
Copyright © 2025 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | v

1 CEF, LEEF & Syslog Support for SIEM User's Guide

SIEM Syslog, LEEF and CEF Logging | 2

- To create a new SIEM notification: | 4
- Using CEF Alert event_id or incident_id to Display Details in Web UI | 5
- To display, delete or edit an Active SIEM connector configuration: | 5
- Alert notification configuration options | 5
- Syslog Trap Sink Server | 7
- CEF, LEEF and Syslog Format | 7
- LEEF FORMAT | 7
- CEF FORMAT | 8
- CEF Field Definitions | 9
- Juniper ATP Appliance CEF Notification Example | 10

Sample CEF and Syslog Notifications | 11

- Example 1: Email with Both Malicious URL and Attachment | 12
- Example 2: Email Sent to Multiple Recipients with Malicious Attachment | 12
- Example 3: Email Sent to Multiple Recipients with Multiple Bad URLs (Separated by Space) and Attachment | 13
- Example 4: Infection Event for which Identity Information is Obtained from Active Directory | 13
- CEF Download (DL) Malware Event Notification Examples | 14
- Syslog Download (DL) Malware Event Notification Examples | 15
- LEEF Event Examples | 15

Syslog Malware Event Infection Notification Example | 16

- Using CEF Alert eventID or incidentID to Display Details in the Juniper ATP Appliance Web UI | 20

CEF Extension Field Key=Value Pair Definitions | **21**

Installing the QRadar Juniper ATP Appliance DSM for LEEF Alerts | 37

Support for QRadar SIEM LEEF Alert Format | **37**

To Install the QRadar DSM Juniper ATP Appliance Extension Plugin | **38**

About This Guide

Use this guide to learn about ATP Appliance incident and event details that can be sent to connected SIEM platforms in CEF, LEEF or Syslog formats.

1

CHAPTER

CEF, LEEF & Syslog Support for SIEM User's Guide

IN THIS CHAPTER

- SIEM Syslog, LEEF and CEF Logging | **2**
- Sample CEF and Syslog Notifications | **11**
- Syslog Malware Event Infection Notification Example | **16**
- Installing the QRadar Juniper ATP Appliance DSM for LEEF Alerts | **37**

SIEM Syslog, LEEF and CEF Logging

IN THIS SECTION

- To create a new SIEM notification: | 4
- Using CEF Alert event_id or incident_id to Display Details in Web UI | 5
- To display, delete or edit an Active SIEM connector configuration: | 5
- Alert notification configuration options | 5
- Syslog Trap Sink Server | 7
- CEF, LEEF and Syslog Format | 7
- LEEF FORMAT | 7
- CEF FORMAT | 8
- CEF Field Definitions | 9
- Juniper ATP Appliance CEF Notification Example | 10

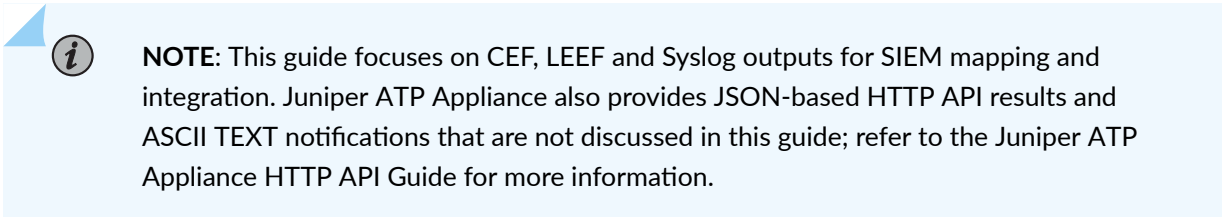
The Juniper ATP Appliance platform collects, inspects and analyzes advanced and stealthy web, file, and email-based threats that exploit and infiltrate client browsers, operating systems, emails and applications. Juniper ATP Appliance's detection of malicious attacks generates incident and event details that can be sent to connected SIEM platforms in CEF, LEEF or Syslog formats. This guide provides information about incident and event collection using these formats.

Juniper ATP Appliance generates LEEF or CEF logs for Download (DL) and Infection (IN) incidents, including phishing (PHS, DL + PHS), for the following event types.

- http | email | cnc | submission | exploit | data theft

NOTE: DL (Download)-based CEF Logs contain the hash and file type of the downloaded malware file. IN (Infection)-based CEF Logs do not provide a hash and file type.

Identity information is also sent as part of SIEM. Refer to Active Directory integration information, external collector options, and other Advanced Threat Analytics and Anti-SIEM filtering options available from the Operator's Guide.



NOTE: This guide focuses on CEF, LEEF and Syslog outputs for SIEM mapping and integration. Juniper ATP Appliance also provides JSON-based HTTP API results and ASCII TEXT notifications that are not discussed in this guide; refer to the Juniper ATP Appliance HTTP API Guide for more information.

In addition, Juniper ATP Appliance extended Syslog functionality in a previous release and added more details to Syslog messaging. Syslog alerts are sent for the following Incident and event types:

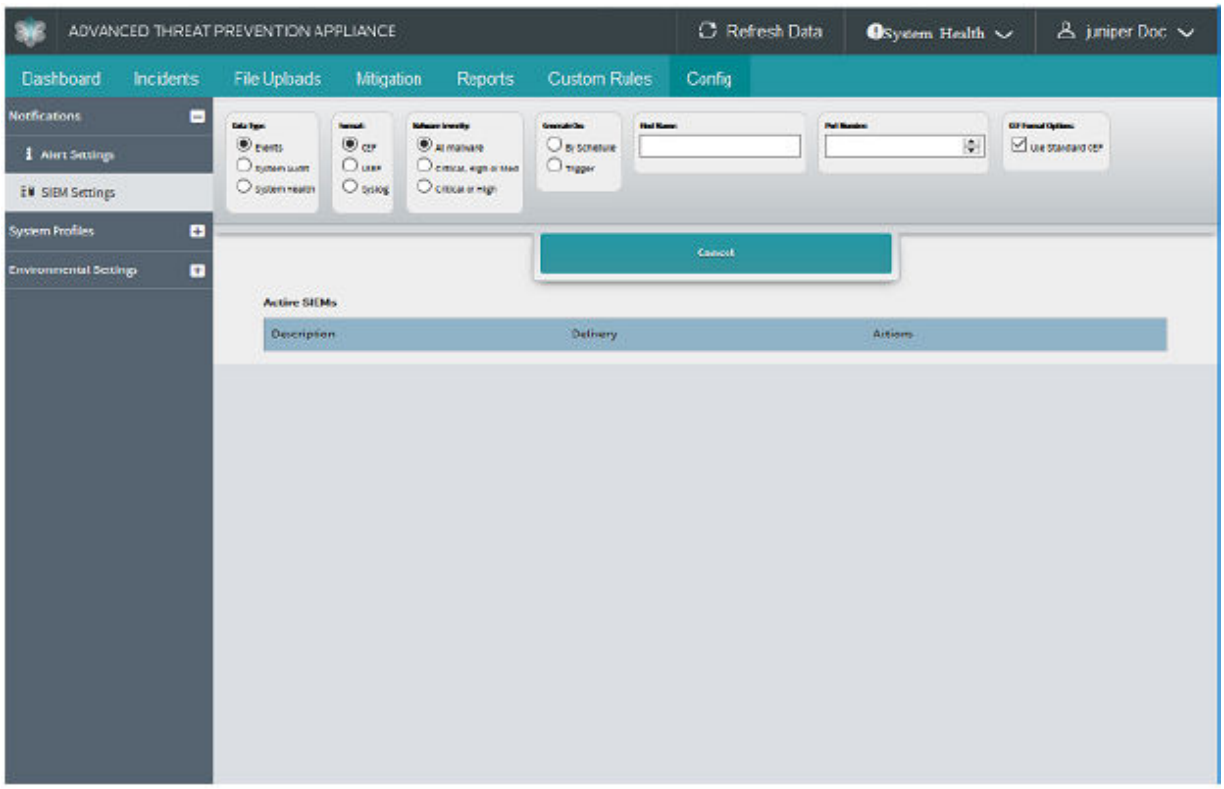
- Downloads
- Infections
- Exploits
- Email Downloads
- Phishing
- File Uploads (malware analysis)
- Data Theft
- Endpoint Identity information

Juniper ATP Appliance has added extra fields to the Syslog output such as externalId (Incident ID), eventID (Event ID), and so on. All extra fields are included in this document.

The Juniper ATP Appliance Central Manager WebUI Config> Notifications> SIEM Settings provides the option to configure event and system audit notifications for CEF-format, LEEF-format, or SYSLOG SIEM servers. The servers, in turn, must be configured to receive the Juniper ATP Appliance notifications in CEF, LEEF and Syslog formats (provide hostname and port number for Syslog).

Configure SIEM Settings in order to have Events or System Audit notifications sent to designated hosts aslogs in either CEF, LEEF or Syslog format.

Figure 1: Setting SIEM Notification



Note that if selecting Syslog as the SIEM setting when configuring System Health alerts, you can choose to include the Hostname or Process name in the Syslog messages that are sent from the Juniper ATP Appliance: Show Hostname and Show Process Name:

To create a new SIEM notification:

1. Navigate to the Config>Notifications page and select SIEM Settings from the left panel menu.
2. Click Add New SIEM Connector to set up a new Events, System Audit or System Health log notification in CEF, LEEF or Syslog format.
3. Select from the available options and click Add to complete the configuration and add the new SIEM connector configuration to the Active SIEMS list.

Using CEF Alert event_id or incident_id to Display Details in Web UI

Given an incident_id or event_id, you can use the following URLs to display relative details in the Juniper ATP Appliance Web UI.

Replace “JATP_HOSTNAME_HERE” with your Juniper ATP Appliance host name, and replace “0000000” with the event_id or incident_id.

- https://JATP_HOSTNAME_HERE/admin/index.html?incident_id=0000000
- https://JATP_HOSTNAME_HERE/admin/index.html?event_id=0000000

NOTE: The system will prompt for login/password if no login session is currently active.

To display, delete or edit an Active SIEM connector configuration:

1. To display a recent report, or delete or edit an existing SIEM configuration, click Display, Delete or Edit, respectively, in the Active SIEM table for a selected configuration row.
2. Edit, modify or delete the current settings and fields as desired, then click Save.

Alert notification configuration options

Alert notifications for SIEM events or system audits are available only if Outgoing Mail Settings are configured from the Config>System Settings menu.

Descriptions of Events alert settings are provided in the following tables.

Table 1: Events SIEM Settings

Type	Select the type of SIEM connector notification to be configured: Event
Format	Select CEF or Syslog as the notification output format.

Malware Severity	To filter the log notification by malware severity results, choose either: All Malware | Critical, High or Med | Critical or High
Generate On	Select Trigger or By Schedule to set the method by which a SIEM Events log is generated. If “By Schedule” is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.
Host Name	Enter the host name of the CEF or Syslog server.
Port Number	Enter the port number of the CEF or Syslog server.

Table 2: System Audit SIEM Settings

Type	Select the type of SIEM notification to be configured: System Audit
Format	Select CEF or Syslog as the notification output format.
Event Type	Select the event type(s) to include in the alert notification: Login/Logout | Failed logins | Add/Update Users | System Settings | Restarts
Format	Select CEF or Syslog as the log output format.
Generate On	Select Trigger or By Schedule to set the method by which a SIEM System Audit log is generated. If “By Schedule” is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.

Table 3: System Health SIEM Settings

Type	Select the type of SIEM connector log to be configured: System Health

Health	Select the health report type(s) to include in the SIEM log: Overall Health | Processing Delay
Format	Select CEF or Syslog as the log output format. Note that if selecting Syslog as the SIEM setting when configuring System Health alerts, you can choose to show or hide the Hostname or Process name in the Syslog messages that are sent from the Juniper ATP Appliance: show Hostname and Show Process Name.
Generate On	Select Trigger or By Schedule to set the method by which a SIEM System Audit log is generated. If “By Schedule” is selected, then select a Day, then enter a Time in the format 00:00 am or pm to set the day(s) and time at which the alert is to be generated.

Syslog Trap Sink Server

When configuring a Juniper ATP Appliance to generate alert notifications in CEF or Syslog format, an administrator must confirm that the rsyslog trap-sink SIEM server supports CEF. The CEF output is accessible for parsing only on the rsyslog server and cannot be viewed from the Juniper ATP Appliance CLI or Web UI.

CEF, LEEF and Syslog Format

Common Event Format (CEF)and Log Event Extended Format (LEEF) are open standard syslog formats for log management and interoperabily of security related information from different devices, network appliances and applications. This open log format is adopted by Juniper ATP Appliance for sending Juniper ATP Appliance malware event , system audit and system health notifications to the configured channel.

LEEF FORMAT

As LEEF events are received, QRadar performs traffic analysis and inspects event traffic to identify the sending device or appliance traffic. When traffic analysis identifies an event source, the first 25 events are categorized as SIM Generic Log DSM events with the event name set as Unknown Log Event. After

the event traffic is identified, QRadar creates a log source to categorize and label events that have been forwarded from the sending appliance or software. Events sent from the sending device are viewable in QRadar on the Log Activity tab.

Refer to the QRadar Log Event Extended Format (LEEF) Guide at https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/b_Leef_format_guide.pdf for more information.

NOTE: For information about installing the Juniper ATP Appliance DSM plugin, refer to "Installing the QRadar Juniper ATP Appliance DSM for LEEF Alerts" on page 37.

CEF FORMAT

The standard CEF format is:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

The Juniper ATP Appliance CEF format is as follows:

```
CEF:0|JATP|Cortex|<JATP version 5.0>|<event type:
http,email,datatheft...>|<malware name>|<incident risk mapping to 0- 10>|externalId=<JATP
Incident ID> eventId=<JATP event ID> <ExtensionField=value...>...
```

The CEF format contains the most relevant malware event, system audit or system health information, making it available for event consumers to parse and to use the data interoperably. To integrate events, the syslog message format is used as a transport mechanism. This mechanism is structured to include a common prefix applied to each message, and contains the date and hostname as shown below:

```
<timestamp in UTC> host <message>
where message=<header>|<extension>
```

Here is the common prefix as shown in Splunk:

```
<Timestamp in UTC> <server-fully-qualified domain name of the Juniper ATP box> <CEF format>
```

Here is the priority header format for Syslog:

```
<Syslog Priority> Timestamp Hostname Processname: SyslogContent
```

Syslog Priority is 134.

Syslog Facility is User-level and Syslog Severity is Notice. Hostname and Processname are configured from the SIEM Settings configuration page by checking the Show Hostname and Show Process Name options (see figure above).

Definitions for the primary CEF fields as well as the "CEF Extension Field Key=Value Pair Definitions" on page 21 are provided in the following sections.

CEF Field Definitions

Table 4: Field Definitions

Definition	Definition
Version	An integer that identifies the version of the CEF format. This information is used to determine what the following fields represent. Example: 0
Device Vendor Device Product Device Version	Strings that uniquely identify the type of sending device. No two products Dec use the same device-vendor and device-product pair, although there is no central authority that manages these pairs. Be sure to assign unique name pairs. Example: JATP|Cortex|3.6.0.12
Signature ID/ Event Class ID	A unique identifier in CEF format that identifies the event-type. This can be a string or an integer. The Event Class ID identifies the type of event reported. Example (one of these types): http |email| cnc| submission| exploit| datatheft
Malware Name	A string indicating the malware name. Example: TROJAN_FAREIT.DC

Table 4: Field Definitions *(Continued)*

Definition	Definition
Severity/Incident Risk Mapping	An integer that reflects the severity of the event. For the Juniper ATP Appliance CEF, the severity value is an incident risk mapping range from 0-10 Example: 9.
External ID	The Juniper ATP Appliance incident number. Example: externalId=1003
Event ID	The Juniper ATP Appliance Event ID number. Example: eventId=13405
Extension	A collection of key-value pairs; the keys are part of a predefined set. An event can contain any number of key- value pairs in any order, separated by spaces. **NOTE**: Review the definitions for these extension field labels provided in the section: "CEF Extension Field Key=Value Pair Definitions" on page 21.

TIP: Timestamp format for Syslog is M D H:i:s

Juniper ATP Appliance CEF Notification Example

The following CEF example is defined per field and label:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension
```

The Juniper ATP Appliance CEF format is as follows:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|cnc|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10 malwareSeverity=0.5
```

```
    malwareCategory=Trojan_DataTheft cncServers=50.154.149.189
    Nov 23 17:36:39 10-3 : Timestamp in UTC 2016-01-23 17:36:39.841+00
    tap00.test.JATP.net : Server-fully-qualified domain name of the JATP box
    CEF:0 : CEF version is 0
    JATP : Device vendor is Juniper
    Cortex : Device product is Cortex
    5.0 : Device version (Version number as shown in the GUI)
    cnc : Type of event
    TROJAN_Zemot.CY : Name of the malware
    7 : Severity (range between 0-10)
    995 : External ID
    123 : Event ID
    2016-01-23 17:36:39.841+00 : Last Activity Time stamp
    50.154.149.189 : Source IP Address
    192.168.1.10 : Destination IP Address
    0.5 : Malware Severity Rating
    Trojan_DataTheft : Malware Category
31.170.165.131 : CnC server IP Address
```

SEE ALSO

Sample CEF and Syslog Notifications | 11

Sample CEF and Syslog Notifications

IN THIS SECTION

- Example 1: Email with Both Malicious URL and Attachment | 12
- Example 2: Email Sent to Multiple Recipients with Malicious Attachment | 12
- Example 3: Email Sent to Multiple Recipients with Multiple Bad URLs (Separated by Space) and Attachment | 13
- Example 4: Infection Event for which Identity Information is Obtained from Active Directory | 13
- CEF Download (DL) Malware Event Notification Examples | 14
- Syslog Download (DL) Malware Event Notification Examples | 15

LEEF Event Examples | 15

Sample CEF, LEEF, and Syslog notification examples are shown for various event types in this section.

The definitions for each of the <extension> field keys per event type are provided in the section "CEF Extension Field Key=Value Pair Definitions" on page 21

NOTE: Be aware that if a value is null, the label will still display in the notification; for example, dst= and filename remain blank in the CEF message:

```
eventId=13423 lastActivityTime=2016-7-26 21:50:50+00 dst=
fileHash=c01e057e6b7115057d9465311346f198a7fed574 fileName= fileType=PE32 executable
```

CEF Phishing Event Examples:

Phishing events are included in CEF/Syslog. Here are few examples:

Example 1: Email with Both Malicious URL and Attachment

```
Dec 6 16:52:22 IP Dec 06 16:51:38 hostname
    CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|externalId=1504
    eventId=14067 lastActivityTime=2016-12-06 23:51:38+00 src= dst=
    src_hostname= dst_hostname= src_username= dst_username=
    mailto:src_email_id=src@abc.comdst_email_id={mailto:test@abc.com} startTime=2016-12- 06
23:51:38+00 url=http://greatfilesarey.asia/QA/files_to_pcaps/74280968a4917da52b5555351eeda969.bin
    fileHash=bce00351cfc559afec5beb90ea387b03788e4af5 fileType=PE32
executable (GUI) Intel 80386, for MS Windows
```

Example 2: Email Sent to Multiple Recipients with Malicious Attachment

```
Dec 9 19:47:19 IP Dec 09 19:49:36 hostname
    CEF:0|JATP|Cortex|3.6.0.1444|email|TROJAN_GIPPERS.DC|8|externalId=1505
    eventId=14068 lastActivityTime=2016-05-10 02:49:36+00 src= dst=
    src_hostname= dst_hostname= src_username= dst_username=
```

```
    mailto:src_email_id=src@abc.com
    dst_email_id={mailto:test1@abc.com,mailto:test2@abc.com,mailto:test3@abc.com}
    fileHash=bce00351cfc559afec5beb90ea387b03788e4af5 fileType=PE32
    executable (GUI) Intel 80386, for MS Windows startTime=2016-05-10
02:49:36.000000+00
```

Example 3: Email Sent to Multiple Recipients with Multiple Bad URLs (Separated by Space) and Attachment

```
Dec 3 16:42:24 IP Dec 03 16:42:54 hostname
    CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|externalId=1499
    eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src= dst=
    src_hostname= dst_hostname= src_username= dst_username=
    mailto:src_email_id=src@abc.com
    dst_email_id={mailto:test1@abc.com,mailto:test2@abc.com,mailto:test3@abc.com} startTime=2016-
    05-03 23:42:54+00 url=http://greatfilesarey.asia/QA/files_to_pcaps/
    74280968a4917da52b5555351eeda969.bin http://greatfilesarey.asia/QA/
    files_to_pcaps/1813791bcecf3a3af699337723a30882.bin
    fileHash=bce00351cfc559afec5beb90ea387b03788e4af5 fileType=PE32
executable (GUI) Intel 80386, for MS Windows
```

Example 4: Infection Event for which Identity Information is Obtained from Active Directory

```
Dec 2 17:17:25 IP Dec 02 17:08:08 hostname
    CEF:0|JATP|Cortex|3.6.0.1444|cnc|TROJAN_DUSVEXT.CY|10|externalId=1489
    eventId=14046 lastActivityTime=2016-05-03 00:08:08.349+00
    src=31.170.165.131 dst=172.20.1.201 src_hostname=
    dsthostname=emailuser-host src_username= dst_username=emailuser
    malwareSeverity=0.75 malwareCategory=Trojan_Generic
cncServers=31.170.165.131
```

CEF System Health Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.3|3|services-health|5|desc=Behavior Engine is
    not running json={"status": "0", "service": "Behavior Engine"}
source = udp:514 sourcetype = syslog
```

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.3|3|appliance-connect-health|5|desc=Lost
    connection to web_collector upgrade (10.2.11.107) for 10 minutes
    json={"ip": "10.2.11.107", "age": 10.3804142, "type": "web_collector",
 "appliance": "upgrade", "pretty_age": "10 minutes"}
```

Syslog System Health Notification Example:

```
<134>Nov 24 17:22:56 tap54.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|3|traffic-health|5|desc=10.2.20.54
    (10.2.20.54) received 0 KB of monitor traffic over last 10 minutes
    json={"pretty_age": "10 minutes", "ip": "10.2.20.54", "age": 10,
 "appliance": "10.2.20.54", "sample_size": 2, "traffic": "0”}
```

NOTE: The priority value in syslog headers from pcaps is “134”. The Juniper ATP Appliance mirrors the output of CEF for the fields supported by Syslog to generate Syslog output

CEF Download (DL) Malware Event Notification Examples

```
2016-7-11 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.12|http|TROJAN_Zemot.CY|5|eventId=123
    src=50.154.149.189 dst=192.168.1.10 startTime=2016-6-30
    01:05:16.001+00fileHash=1d81e21db086a2c385696f17f17bdde6d4be04d
    fileName=ccaed7c3c6e58a2844c9896246997f62.bin fileType=PE32 executable
(GUI) Intel 80386, for MS Windows startTime=2016-08-11 17:36:39.841+00
```

Syslog Download (DL) Malware Event Notification Examples

```
<134>Nov 23 21:58:05 tap54.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|http|TROJAN_GIPPERS.DC|8|externalId=374
    eventId=13348 lastActivityTime=2016-02-24 05:58:05.151123+00
    src=172.16.0.1 dst=10.1.1.26
    fileHash=acf69d292d2928c5ddfe5e6af562cd482e6812dc
    fileName=79ea1163c0844a2d2b6884a31fc32cc4.bin fileType=PE32 executable
    (GUI) Intel 80386, for MS Windows startTime=2016-02-24
05:58:05.151123+00
```

CEF HTTP Malware Event Notification Example

```
Dec 31 16:43:47 10-3 2016-12-26 18:06:52.333023+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.12|http|TROJAN_FAREIT.DC|10|13405
    lastActivityTime=2016-12-26 18:06:52.333023+00 src=172.16.0.1
    dst=10.1.1.44 fileHash=6ff61bec9baa970df54c69fbef1209004a01f068
    fileName=e309ea0c7271f3845d86621717220479.bin fileType=PE32 executable
    (GUI) Intel 80386, for MS Windows startTime=2016-12-26
18:06:52.333023+00
```

LEEF Event Examples

LEEF log for Download

```
<134>Sep 24 16:23:36 ovf-core.eng.ovf-core.com LEEF:1.0|Cyphort|Cortex|5.0.4.16|http|
src=172.16.1.101    dst=172.16.1.105    usrName=    devTime=2018-09-24 16:23:36 PDT
cat=malware    devTimeFormat=yyyy-MM-dd HH:mm:ss z    sev=10    dst_hostname=
src_hostname=    src_username=    incidentId=2614    eventId=80543
fileHash=a1e6d991e4464e7c018182951faa468c42ca3937    fileType=Composite Document File V2
Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Author: Jonh Deddi, Last
Saved By: Jonh Deddi, Name of Creating Application: Microsoft Excel, Create Time/Date: Mon Aug
24 23:23:16 2015, Last Saved Time/Date: Tue Aug 25 11:54:39 2015, Security: 0
fileName=61646e7802b449ee02f7269129079829b5eae37c0b934b40475f1f0e94409ad4
malwareName=HEUR_MACRO    fileHashMd5=7aeea812c00fcf77d4214f430078e3c4

LEEF log for 3rd party log ingestion (Virus scan log from Symantec)
```

LEEF log for 3rd party log ingestion (Virus scan log from Symantec)

```
<134>Sep 24 14:23:41 ovf-core.eng.ovf-core.com LEEF:1.0|Cyphort|Cortex|5.0.4.16|third_party|
src=    dst=169.254.31.242    usrName=Administrator    devTime=2018-09-24 14:23:41 PDT
cat=malware    devTimeFormat=yyyy-MM-dd HH:mm:ss z    sev=3    dst_hostname=    src_hostname=
src_username=    incidentId=2613    eventId=80517    malwareName=Virus Scan
```

LEEF for email with both phishing links and also a malicious attachment

```
<134>Sep 12 12:27:24 ovf-core.eng.ovf-core.com LEEF:1.0|Cyphort|Cortex|5.0.4.12|email|src=
dst=    usrName=    devTime=2018-09-12 12:27:24 PDT    cat=malware    devTimeFormat=yyyy-MM-dd
HH:mm:ss z    sev=10    url=http://www.two-of-us.at/images/W.exe http://lm.beilequ.com/update/
365/365weatherIns_61.rar http://abc.adamoads.com/fda    dst_hostname=    src_hostname=
src_username=    src_email_id=kalyan@cyphort.com    dst_email_id=jane.doe@cydevel.com
incidentId=2531    eventId=78703    fileHash=1f0b0376c0f39b33673363d61294abfaab9fb837
fileType=Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.1, Code
page: 936, Title: PowerPoint Presentation, Last Saved By: MC SYSTEM, Revision Number: 5, Name of
Creating Application: Microsoft PowerPoint, Total Editing Time: 01:28, Last Saved Time/Date: Sat
Sep 29 04:42:55 2007, Number of Words: 2    malwareName=EXPLOIT_OFFICE_XDS
email_msg_id=CABo8cN_mCTN5XAL+G=C4OcVXry7eiKm4uctkguf2Lqvv_KfWrg@mail.gmail.com
fileHashMd5=17e9e5a4c807f3d2d50ba512542c982c
```

RELATED DOCUMENTATION

Syslog Malware Event Infection Notification Example | 16

Syslog Malware Event Infection Notification Example

IN THIS SECTION

Using CEF Alert eventID or incidentID to Display Details in the Juniper ATP Appliance Web UI | 20

- CEF Extension Field Key=Value Pair Definitions | **21**

```
<134>Nov 23 21:58:05 tap54.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|cnc|TROJAN_Vertexbot.CY|5|externalId=353
    eventId=13321 lastActivityTime=2016-02-24 02:17:25.638+00
    src=31.170.165.131 dst=10.1.1.48 malwareSeverity=0.5
malwareCategory=Unknown cncServers=31.170.165.131
```

CEF Email Malware Event Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|email|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10
    fileHash=d93216633bf6f86bc3076530b6e9ca6443fc75b5 fileName=abc.bin
fileType=Zip archive data, at least v2.0 to extract startTime=2016-01-23 17:36:39.841+00
```

Syslog Email Malware Event Notification Example:

```
<134> Nov 23 18:50:00 tap0.test.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|email|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10
    fileHash=d93216633bf6f86bc3076530b6e9ca6443fc75b5 fileName=abc.bin
fileType=Zip archive data, at least v2.0 to extract startTime=2016-01-23 17:36:39.841+00
```

CEF CnC Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|cnc|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10
malwareSeverity=0.5 malwareCategory=Trojan_DataTheft cncServers=50.154.149.189
```

Syslog CnC Notification Example:

```
<134> Nov 23 18:50:00 tap0.test.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|cnc|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10 malwareSeverity=0.5
malwareCategory=Trojan_DataTheft cncServers=50.154.149.189
```

CEF File Submission Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|submission|TROJAN_Zemot.CY|7|externalId=995
    eventId=123 lastActivityTime=2016-01-23 17:36:39.841+00
    src=50.154.149.189 dst=192.168.1.10
    fileHash=d93216633bf6f86bc3076530b6e9ca6443fc75b5 fileName=abc.bin
fileType=Zip archive data, at least v2.0 to extract submissionTime=2016- 01-23 17:36:39.841+00
```

Syslog File Upload Notification Example:

```
<134>Nov 23 21:58:05 tap54.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|submission|VIRUS_NABUCUR.DC|5|externalId=354
    eventId=13322 lastActivityTime=2016-02-24 02:25:05.163039+00src= dst=
    fileHash=12b1777e451ef24bcc940bc79cdd7a0ffb181d78 fileName=
     fileType=PE32 executable (GUI) Intel 80386, for MS Windows
submissionTime=2016-02-24 02:25:05.163039+00
```

CEF Exploit Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|exploit|Exploit|7|externalId=995 eventId=123
    lastActivityTime=2016-01-23 17:36:39.841+00 src=50.154.149.189
    dst=192.168.1.10 reqReferer=http://forums.govteen.com/content.php
url=http://64.202.116.151/nzrems2/1
```

Syslog Exploit Notification Example:

```
<134>Nov 23 21:58:05 tap54.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|exploit|Exploit|3|externalId=352
    eventId=13319 lastActivityTime=2016-02-24 02:18:21.105811+00
```

```
    src=64.202.116.124 dst=192.168.50.203 reqReferer=http:// www.christianforums.com/
url=http://64.202.116.124/5butqfk/?2
```

CEF Data Theft Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|datatheft|2ND_ORDER_DLP_CUSTOMIZED :
    CreditCard_Rule|7|externalId=995 eventId=123 lastActivityTime=2016-01-23
    17:36:39.841+00 src=50.154.149.189 dst=192.168.1.10
    description=2ND_ORDER_DLP_CUSTOMIZED : CreditCard_Rule port=80
protocol=HTTP startTime=2016-01-23 17:36:39.841+00
```

Syslog Data Theft Notification Example:

```
<134> Nov 23 18:50:00 tap0.test.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|datatheft|2ND_ORDER_DLP_CUSTOMIZED :
    CreditCard_Rule|7|externalId=995 eventId=123 lastActivityTime=2016-01-23
    17:36:39.841+00 src=50.154.149.189 dst=192.168.1.10 description=2ND_ORDER_DLP_CUSTOMIZED :
CreditCard_Rule port=80
protocol=HTTP startTime=2016-01-23 17:36:39.841+00
```

CEF System Health Notification Example:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|3|traffic-health|5|desc=10.2.20.54
    (10.2.20.54) received 0 KB of monitor traffic over last 10 minutes
    json={"pretty_age": "10 minutes", "ip": "10.2.20.54", "age": 10,
"appliance": "10.2.20.54", "sample_size": 2, "traffic": "0”}
```

Syslog System Health Notification Example:

```
<134>Nov 24 17:12:55 tap0.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|3|link-health|5|desc=Link eth1 on 10.2.20.54
    (10.2.20.54) is down json={"interface": "eth1", "ip": "10.2.20.54",
    "appliance": "10.2.20.54", "app_id": "467dea60-d7da-11dd-83c7-
10bf48d79a6e", "up": false}
```

CEF System Audit Notification Examples:

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|2|update-system-config|5|desc=descriptio
     json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" :
"test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
```

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|2|update-smtp|5|desc=description json={
     "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" :
 "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
```

```
2016-01-23 17:36:39.841+00 tap0.test.JATP.net
    CEF:0|JATP|Cortex|3.6.0.15|2|reboot|5|desc=description json={ "user_id"
    : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP",
 "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
```

Syslog System Audit Notification Examples:

```
<134>Nov 24 14:32:59 tap0.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|2|add-user|5|username=admin desc=Delete user
     'jane' with id 'f263f0b1-353e-046c-1577-6adc1c96cb62' json={ "user_id" :
    "f263f0b1-353e-046c-1577-6adc1c96cb62", "user_name" : "jane"}
    <134>Nov 24 14:31:20 tap0.eng.JATP.net JATP:
    CEF:0|JATP|Cortex|3.6.0.15|2|update-user|5|username=admin desc=Updated
    user id '27ee212e-855d-08d4-953f-6b9cea46a679': name 'john', is admin:
     yes, has debug: yes, reset password: no json={ "user_id" : "27ee212e-
    855d-08d4-953f-6b9cea46a679", "user_name" : "john", "is_admin" : 1,
"has_debug": 1 , "reset_password" : 0}
```

Using CEF Alert eventID or incidentID to Display Details in the Juniper ATP Appliance Web UI

Given an incidentID or eventID, you can use the following URLs to display relative details in the Juniper ATP Appliance Web UI.

Replace “JATP_HOSTNAME_HERE” with your Juniper ATP Appliance host name, and replace “0000000” with the event_id or incident_id.

- https://JATP_HOSTNAME_HERE/admin/index.html?incident_id=0000000
- https://JATP_HOSTNAME_HERE/admin/index.html?event_id=0000000

NOTE: The system will prompt for login/password if no login session is currently active.

CEF Extension Field Key=Value Pair Definitions

Juniper ATP Appliance uses the following parameters in its CEF extension field key=value pairs. The keys in extension have "=" sign; for example:. cncServers=a.b.c.d eventId=123. The fields before extensions are surrounded by pipes ("|"); for example: |login|, |cnc|, |JATP|.

The following table defines each extension field key in CEF and/or Syslog messages.

Table 5: Extension field keys in CEF and/or Syslog messages

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
description= Only for System Audit	description desc is the description of the system audit event	Audit	String 1023 characters	description=update-user

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
json=	json output sends different data depending on what kind of System Audit event is referenced. The following sample json= is for update-user: json = { "user_id" : "2721f188-682e-03d0-6dfa-5d5d688047b6", "username" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 0}	Audit	String 1023 characters	json= This json= field is for login: <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|login|5|username=admin desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
login	Login	Audit	String	login <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|login|5|username=admin desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
login-fail	Login failure	Audit	String	login-fail <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|loginfail| 5| username=admin desc=description json={ "user_id" : "8d7c450edf6a-0ab6-193d- 143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
logout	Lockout	Audit	String	logout <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|logout|5|username= admin desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
add-user	Add User	Audit	String	add-user <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|adduser| 5| username=admin desc=description json={ "user_id" : "8d7c450edf6a-0ab6-193d- 143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
update-user	Update User	Audit	String	update-user <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|updateuser| 5| username=admin desc=description json={ "user_id" : "8d7c450edf6a-0ab6-193d- 143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
update-system-config	System Config Update	Audit	String	update-system-config <134>Nov 24 14:35:48 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|update-systemconfig| 5|username=adm in desc=Updated update settings: software auto update: 'yes', Set hostname: 'tap0', Set server_fqdn : 'tap0.eng.JATP.net', Set ivp_format : 'application/ zip' remote shell enabled: yes json={ "do_auto_update" : 1, "hostname" : "tap0", "server_fqdn" : "tap0.eng.JATP.net", "ivp_format" : "application/zip", "remote_shell_enabled : 1
reboot	Reboot	Audit	String	reboot <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|reboot|5|username =admin desc=description json={ "user_id" : "8d7c450edf6a-0ab6-193d- 143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
appliance-connecthealth	health of appliance connection	Audit	String	appliance-connecthealth <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|appliance-connecthealth| 5|username=adm in desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
link-health	Link health			link-health <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|linkhealth| 5| username=adm in desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
traffic-health	Traffic health			traffic-health <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|trafficchealth| 5| username=adm in desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
clear-db	Clear DB	Audit	String	clear-db <134>Nov 24 16:32:03 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|cleardb| 5| username=admin desc=Clear event database json={ "status" : 0}
restart-services	Restart Services	Audit	String	restart-services <134>Nov 24 14:37:07 tap54.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|restartservices| 5| username=ad min desc=Restart services json={ "status" : 0}
add-report	Add Report	Audit	String	add-report <134>Nov 24 14:37:32 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|addreport| 5| username=adm in desc=Add report (id '300BF9F1-973B-4523- 8BEB-B82B70B78925') json={ "report_id" : "300BF9F1-973B-4523- 8BEB-B82B70B78925”}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
delete-report	Delete Report	Audit	String	delete-report <134>Nov 24 14:37:41 tap0.eng.JATP.netJATP JATP: CEF:0| JATP|Cortex|3.6.0. 15|2|deletereport| 5| username=adm in desc=Delete report (id 'CF411F54-EB45-0C41- 654A-AFA1B9FF9DEB') json={ "report_id" : "CF411F54-EB45-0C41- 654A-AFA1B9FF9DEB”}
add-notification	Add Notification	Audit	String	add-notification <134>Nov 24 14:35:04 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|addnotification| 5| username =admin desc=Add notification (id 'AD5D3D6C-6A51-4BB5- 958A-A1B392D3DFDA') json={ "report_id" : "AD5D3D6C-6A51-4BB5-958AA1B392D3DFDA”}
delete-notification	Delete Notification	Audit	String	delete-notification <134>Nov 24 14:38:13 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|deletenotification| 5| username =admin desc=Delete notification (id '26EC53CA-B1A7-4DBAA111- 013CD2548FFD') json={ "report_id" : "26EC53CA-B1A7-4DBAA111- 013CD2548FFD”}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
add-siem	Add SIEM	Audit	String	add-siem <134>Nov 24 14:29:08 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|addsiem| 5| username=admin desc=Add SIEM upload to 'splunktest. eng.JATP.net' (id '768687F7-4A81-42AF-897A-6814A48D4155') json={ "report_id" : "768687F7-4A81-42AF-897A-6814A48D4155", "host_name": "splunktest. eng.JATP.net”}
delete-siem	Delete SIEM	Audit	String	delete-siem <134>Nov 24 14:38:57 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|deletesiem| 5| username=admin desc=Delete SIEM upload to '10.9.8.7' (id '8165C17F-F375-4226- 8E7A-BC8E690E3370') json={ "report_id" : "8165C17F-F375-4226- 8E7A-BC8E690E3370", "host_name": "10.9.8.7”}
add-email-collector	Add Email Collector	Audit	String	add-email-collector <134>Nov 24 14:39:35 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|add-emailcollector| 5| username=a dmin desc=Add email collector from '10.2.10.3' (id '5FB8FFDC-7024- 467A-8AC8-6CD68CA8781D') json={ "report_id" : "5FB8FFDC-7024-467A-8AC8- 6CD68CA8781D", "host_name": "10.2.10.3”}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
delete-email-collector	Delete Email Collector	Audit	String	delete-email-collector <134>Nov 24 14:39:09 tap0.eng.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|delete-emailcollector| 5|username=a dmin desc=Delete email collector from '10.2.10.7' (id '6C36F94A-3CF2- 45D8-83B9-CDF50BE0490B') json={ "report_id" : "6C36F94A-3CF2-45D8-83B9- CDF50BE0490B", "host_name": "10.2.10.7”}
dst=	destinationIPAddress dst represents the IP address of the destination when any communication to an external host is observed within the detection engine.	Events	IPv4 and IPv6 Addresses	dst=128.12.38.6 **NOTE**: Note: This could also be the destination IP address from which the user downloaded malware; this extension is not specific to infection only.
lastActivityTime=	Time stamp of the last activity associated with this event.	Events	string 1023 characters	lastActivityTime=2016- 12-26 18:06:52.333023+00
fileHash=	fileHash represents the checksum of the malware object from a Juniper ATP Appliance detection engine	Events	255 characters	filehash=3174990d783f4 a1bd5e99db60176b920

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
fileName=	fileName represents the name of the object file analyzed by Juniper ATP Appliance detection engine	Events	255 characters	fileName=Trojan.Generic
fileType=	fileType represents the analyzed object type.	Events	255 characters	fileType=pdf
startTime=	startTime represents the date and time of the initial malware event in the Juniper ATP Appliance detection system.	Event	string 1023 characters	startTime=2016-08-11 18:22:19
malwareSeverity=	Severity risk in the range 0-10	Event	integer	malwareSeverity=0.75
malwareCategory=	Juniper ATP Appliance malware category determination	Event	string 1023 characters	malwareCategory=
cncServers=	IP address of the CnC server associated with this event	Event	IPv4 and IPv6 Addresses	cncServers=31.170.165.131
submissionTime=	Date and time of user File Submit option from the CM Web UI	Event	data	submissionTime=2016- 12-26 17:54:46.04875+00

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
src=	The source address associated with this malware event.	Event	IPv4 and IPv6 Addresses	src=64.202.116.124
dst=	The source address associated with this malware event.	Event	IPv4 and IPv6 Addresses	dst=10.1.1.1
reqReferer=	The URL of the HTTP address that triggered or with which the malware exploit is associated	Event	URL	reqReferer=http:// www.christianforums.com/
url=	The URL associated with an exploit malware event.	Event	URL	url=http:// 64.202.116.124/5butqfk/ ?2
ExternalId=	The Juniper ATP Appliance incident number. Example: externalId=1003	External ID	The Juniper ATP Appliance incident number.	Example: externalId=1003
EventId=	The Juniper ATP Appliance Event ID number. Example: eventId=13405	Event ID	The Juniper ATP Appliance Event ID number.	Example: eventId=13405

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
username=	The admin or user's username Username is included in System Audit Syslogs.	Event	string	Example: username="s_roberts"
port=	Port number associated with the event	Event	integer	port=22
protocol=	Protocol associated with the event	Event	integer	protocol=http
appliance-connecthealth	Connection health between Web Collectors and Secondary Cores.	Health	String	<134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|appliance-connecthealth| 5|username=adm in desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
traffic-health	Traffic health	Health	String	traffic-health <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|trafficchealth| 5| desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
link-health	Link health	Health	String	link-health <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|linkhealth| 5| desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
services-health	Services health	Health	String	services-health <134> Nov 23 18:50:00 tap0.test.JATP.net JATP: CEF:0|JATP| Cortex|3.6.0. 15|2|serviceshealth| 5| desc=description json={ "user_id" : "8d7c450e-df6a-0ab6-193d-143bfc6f7cac", "user_name" : "test.JATP", "is_admin" : 0, "has_debug": 1 , "reset_password" : 1}
src_hostname	Hostname of the threat source. Information is obtained from Active Directory (applicable to SMB Lateral detection where host details of threat source are obtained from Active Directory)	Event	String	Dec 2 17:17:25 IP Dec 02 17:08:08 hostname CEF:0|JATP|Cortex|3.6.0. 1444|cnc|TROJAN_DUSV EXT.|10| externalId=1489 eventId=14046 lastActivityTime=2016- 05-03 00:08:08.349+00 src=31.170.165.131 dst=172.20.1.201 src_hostname= dst_hostname=emailuse r-host src_username= dst_username=emailuse r malwareSeverity=0.75 malwareCategory=Troja n_Generic cncServers=31.170.165.131

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
dst_hostname	Endpoint hostname (threat target); information is obtained from Active Directory	Event	String	Dec 6 16:52:22 IP Dec 06 16:51:38 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1504 eventId=14067 lastActivityTime=2016-12-06 23:51:38+00 src= dst= src_hostname= dst_hostname= src_username= dst_username=src_email_id=src@abc.com dst_email_id={test@abc.com} startTime=2016- 12-06 23:51:38+00 url=http:// greatfilesarey.asia/QA/files_to_pcaps/ 74280968a4917da52b5555351eeda969.bin fileHash=bce00351cfc559afec5beb90ea387b037 88e4af5 fileType=PE32 executable (GUI) Intel 80386, for MS Windows
src_username	Username of the person logged in into the threat source host. Information is obtained from Active Directory (applicable to Lateral spread because only then we will get the host details of threat source from Active Directory)	Event	String	Dec 3 16:42:24 IP Dec 03 16:42:54 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1499 eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src= dst= src_hostname= dst_hostname= src_username= dst_username=src_email_id=src@abc.com dst_email_id={test1@abc.com,test2@abc.com,test3@abc.com,} url=http:/ /greatfilesarey.asia/QA/ fileType=PE32 executable (GUI) Intel 80386, for MS Windows

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
dst_username: Username of the person logged in into the threat target host. Information is obtained from Active Directory.				Dec 3 16:42:24 IP Dec 03 16:42:54 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1499 eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src= dst= src_hostname= dst_hostname= src_username= dst_username=src_email_id=src@abc.com dst_email_id={test1@ab c.com,test2@abc.com,test3@abc.com,} url=http:/ /greatfilesarey.asia/QA/ fileType=PE32 executable (GUI) Intel 80386, for MS Windows
src_email_id	Email ID of the sender of the email	Event	String	Dec 3 16:42:24 IP Dec 03 16:42:54 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1499 eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src_email_id=src@abc.com dst_email_id={test1@ab c.com,test2@ab c.com,test3@ab c.com,} startTime=2016-05-03 23:42:54+00 url=http:// greatfilesarey.asia/QA/ files_to_pcaps/ 74280968a4917da52b5 555351eeda969.bin fileType=PE32 executable (GUI) Intel 80386, for MS Windows

Table 5: Extension field keys in CEF and/or Syslog messages *(Continued)*

Extension Field Key	Full Name & Description	Event Type	Data Type & Length	CEF or Syslog Key Value (Example)
dst_email_id	Email IDs of recipients	Event	String	Dec 3 16:42:24 IP Dec 03 16:42:54 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1499 eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src_email_id=src@abc.com dst_email_id={test1@ab c.com,test2@ab c.com,test3@ab c.com,} startTime=2016-05-03 23:42:54+00 url=http:// greatfilesarey.asia/QA/files_to_pcaps/ 74280968a4917da52b5555351eeda969.bin fileType=PE32 executable (GUI) Intel 80386, for MS Windows
url	Bad URLs sent in email (In CEF/Syslog, the maximum number of bad URLs Juniper ATP Appliance sends is 5, separated by a character space)	Event	String	Dec 3 16:42:24 IP Dec 03 16:42:54 hostname CEF:0|JATP|Cortex|3.6.0.1444|email|Phishing|8|e xternalId=1499 eventId=14058 lastActivityTime=2016-05-03 23:42:54+00 src_email_id=src@abc.com dst_email_id={test1@ab c.com,test2@ab c.com,test3@ab c.com,} startTime=2016-05-03 23:42:54+00 url=http:// greatfilesarey.asia/QA/files_to_pcaps/ 74280968a4917da52b5555351eeda969.bin fileType=PE32 executable (GUI) Intel 80386, for MS Windows

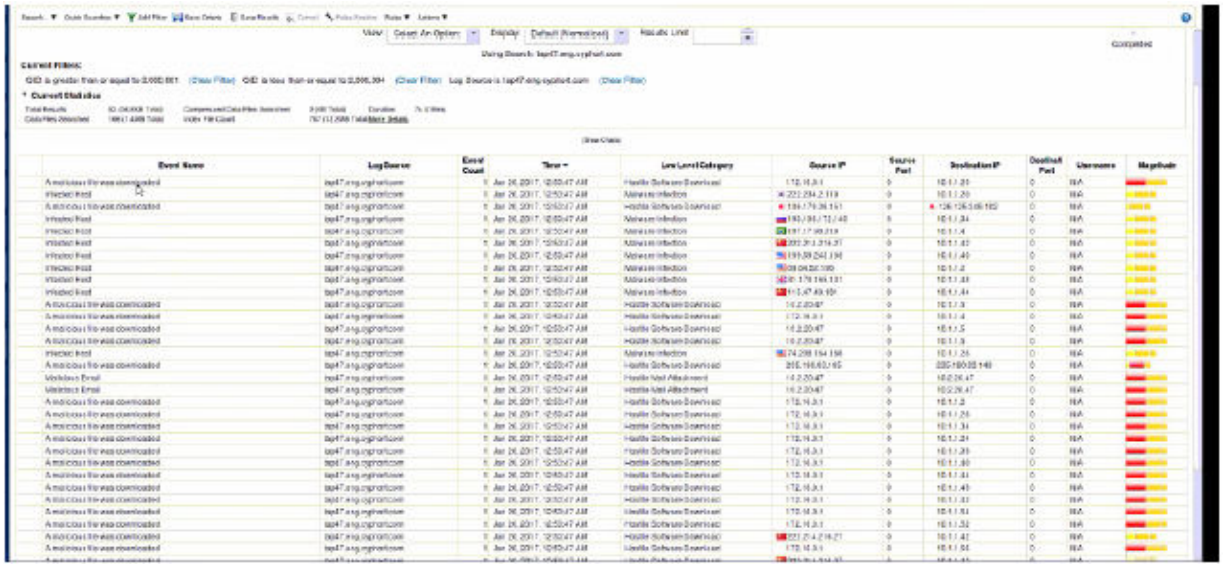
Installing the QRadar Juniper ATP Appliance DSM for LEEF Alerts

IN THIS SECTION

- Support for QRadar SIEM LEEF Alert Format | 37
- To Install the QRadar DSM Juniper ATP Appliance Extension Plugin | 38

Support for QRadar SIEM LEEF Alert Format

The Log Event Extended Format (LEEF) is a customized event format for IBM®Security QRadar®.

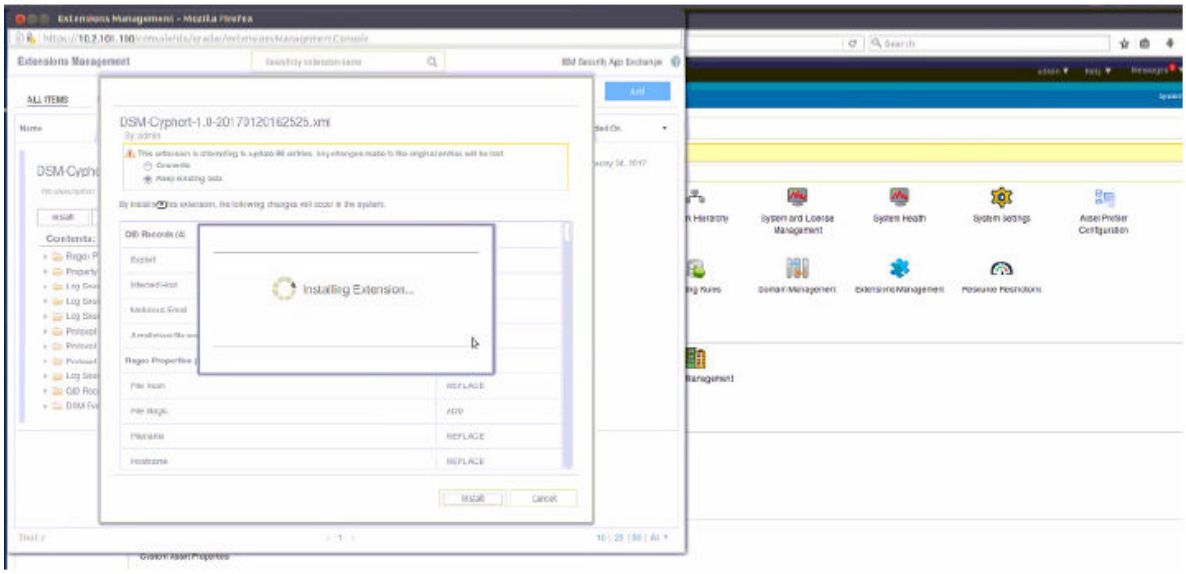


NOTE: Installation of the DSM-Juniper ATP Appliance extension plugin on the QRadar server is required.You can download the DSM-Juniper ATP Appliance extension plugin from https://webdownload.juniper.net/swdl/dl/secure/site/1/record/138167.html.

For configuration information, refer to the Juniper ATP Appliance Operator's Guide.

To Install the QRadar DSM Juniper ATP Appliance Extension Plugin

1. Enable the LEEF options per data type from the Juniper ATP Appliance Central Manager Web UI Config>Notifications>SIEM Settings pages.
2. On the QRadar device, use the Extension Management tab install the Juniper ATP Appliance plugin file.



3. Download the DSM-Juniper ATP Appliance extension plugin file to the Juniper ATP Appliance.

SEE ALSO

SIEM Syslog, LEEF and CEF Logging | 2