Progress®
Kemp® LoadMaster®

Technical Note Common Event Format (CEF) Logs

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Common Event Format (CEF) Logs 4

Chapter 2: CEF Header 7

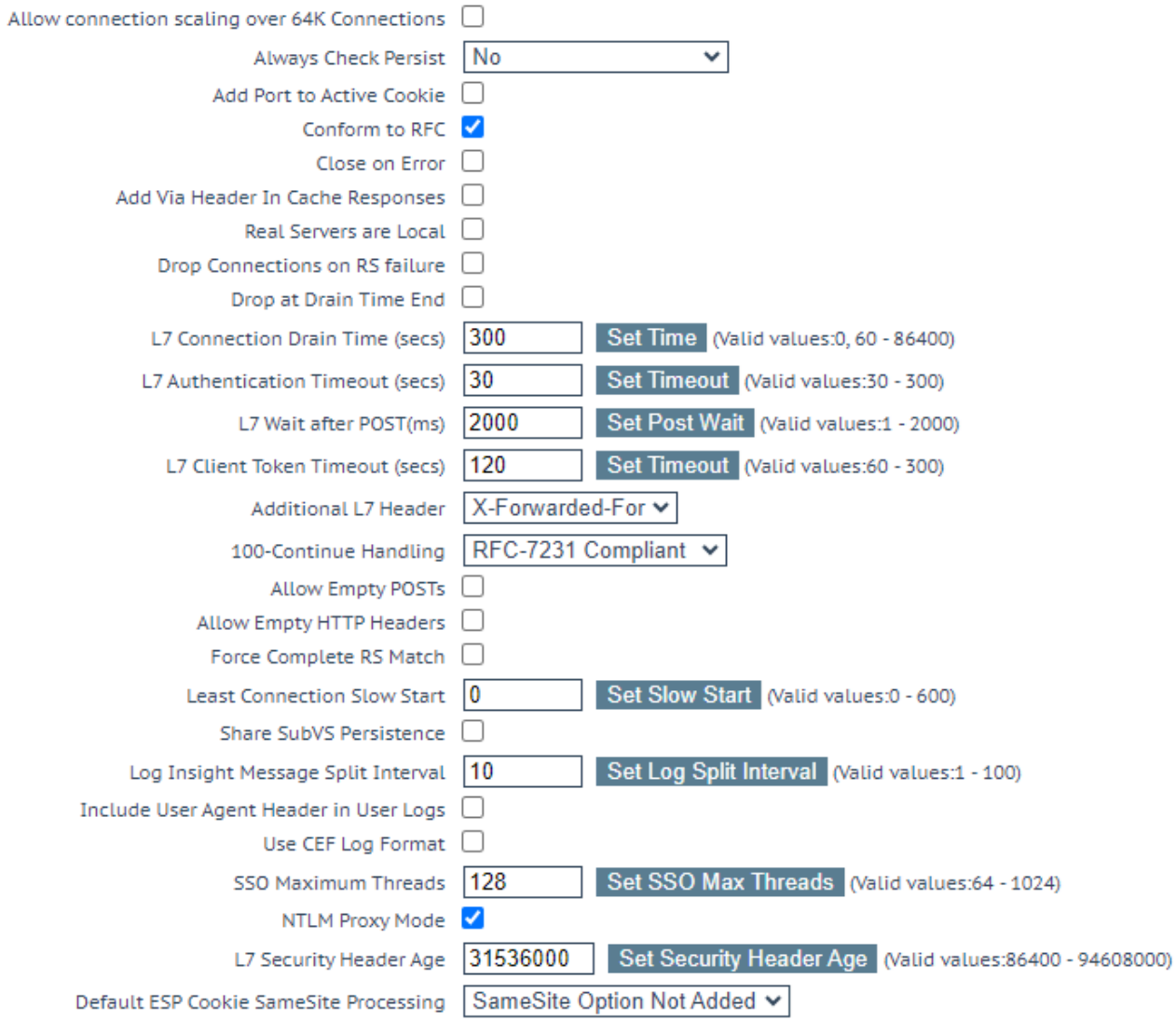
Chapter 3: CEF Extension 10

Chapter 4: References 23

1

Common Event Format (CEF) Logs

This document outlines the details of the Common Event Format (CEF) logs for the Edge Security Pack (ESP) feature. CEF logs were introduced in LoadMaster firmware version 7.2.50.



To enable the CEF log format, go to **System Configuration > Miscellaneous Options > L7 Configuration** and select the **Use CEF Log Format** check box. The **Use CEF Log Format** check box is disabled by default.

Once enabled, all the logs in the **System Configuration > Logging Options > Extended Log Files** page are recorded in CEF format. To export these logs, set the parameters in the **System Configuration > Logging Options > Syslog Options** page to point at your log collector/analyzer.

Note: The CEF log format is only available for ESP logs. It is not available for system, audit, GEO, WAF logs, and so on.

CEF is a widely used log message format that provides a standard format. In CEF format logs, data points are clearly labeled and this makes the overall message easier to read by people and third-party log collectors and analyzers. When used as a source format for monitored devices, CEF allows for easier overall log storage and analysis across a network of different devices. CEF logs also improve the interoperability of security-related information from different security and network devices and applications. CEF was developed by ArcSight and uses UTF-8 Unicode.

The CEF logs are composed of a header and an extension. The header is well-defined within the specification and the extension is a key-value pair vendor-specific segment. The format of the logs is as follows:

```
CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class
ID|Name|Severity|[Extension]
```

2

CEF Header

The CEF header comprises of everything bar the [Extension]. ArcSight describes the CEF Header as follows:

Version

This is an integer and identifies the version of the CEF format. Event consumers use this information to determine what the following fields represent. The current CEF version is 0 (CEF:0).

The Progress Kemp Version is '0'.

Device Vendor, Device Product, and Device Version

These are strings that uniquely identify the type of sending device. No two products may use the same device-vendor and device-product pair. There is no central authority managing these pairs. Event producers must ensure that they assign unique name pairs.

The Progress Kemp Device Vendor is 'Kemp', the Device Product is 'LM' and the Device Version is '0'.

Note: LM is an abbreviation for LoadMaster.

Device Event Class ID

This is a unique identifier per event-type. This can be a string or an integer. The Device Event Class ID identifies the type of event reported. In the Intrusion Detection System (IDS) world, each signature or rule that detects certain activity has a unique Device Event Class ID assigned. This is a requirement for other types of devices too, and helps correlation engines to process the events. This is also known as the Signature ID.

Name

This is a string representing a human-readable and understandable description of the event. The event name should not contain information that is specifically mentioned in other fields.

Severity

This is a string or integer and reflects the importance of the event.

The valid string values are Unknown, Low, Medium, High, and Very-High.

The valid integer values are 0-3=Low, 4-6=Medium, 7-8=High, and 9-10=Very-High.

The Progress Kemp Device Event Class ID, Name, and Severity are outlined in the table below. These all correlate together to provide a full understanding of the type and severity of the CEF log.

L7 ESP CEF Logs

Device Event Class ID	Name	Severity
0	Accept	0 (Low)
1	Slave accept	0 (Low)
2	SSL accept	0 (Low)
3	Connection timed out	1 (Low)
4	Connected	1 (Low)
5	Connection failed	3 (Low)
6	Logged off	1 (Low)
7	User interaction	2 (Low)
8	Logged on	1 (Low)
9	Access Denied	6 (Medium)
10	Access Blocked	6 (Medium)
11	Access Locked	
12	Access Disabled	6 (Medium)
13	Password Expired	6 (Medium)
14	Request	1 (Low)
15	Attempt	2 (Low)
16	Attempted XSS attack	9 (Very High)

Device Event Class ID	Name	Severity
17	SMTP parse failure	7 (High)
18	SMTP Blocked	6 (Medium)
19	Blocked access to directory	6 (Medium)
20	Blocked access to host	6 (Medium)

SSOMGR CEF Logs

Device Event Class ID	Name	Severity
100	User AAA	0 (Low)
101	User session timeout	0 (Low)
102	User session kill	0 (Low)
103	Kill all sessions	0 (Low)
104	Flush SSO cache	1 (Low)

3

CEF Extension

The Progress Kemp CEF Extension is a key-value pairing of information providing extra details based on the 'Device Event Class ID'. This is clarified through the use of examples below.

L7 ESP CEF Logs

The following example shows an 'Accept' message with 'Device Event Class ID' of '0'.

```
CEF:0|Kemp|LM|1.0|0|Accept|0|vs=10.35.46.238:80 event=Accept srcip=10.35.2.98
srcport=61518 msg=Accept
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
msg	This is a free-form string providing extra details

The following example shows a 'Slave Accept' message with 'Device Event Class ID' of '1':

```
CEF:0|Kemp|LM|1.0|1|Slave accept|0|vs=10.35.46.238:80 event=Slave accept
srcip=10.35.2.98 srcport=57432 msg=Slave accept
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
msg	This is a free-form string providing extra details

The following example shows an 'SSL Accept' message with 'Device Event Class ID' of '2':

```
CEF:0|Kemp|LM|1.0|2|SSL accept|0|vs=10.35.46.238:443 event=SSL accept
srcip=10.35.2.98 srcport=51639 msg=SSL accept
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request

The following example shows a 'Connection Timed Out' message with 'Device Event Class ID' of '3':

```
CEF:0|Kemp|LM|1.0|3|Connection timed out|1|vs=10.35.46.235:443 event=Connection
timed out srcip=10.35.2.98 srcport=51723 msg=waiting for initial client request
await_remaddr=0
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
msg	This is a free-form string providing extra details
await_remaddr	Internal flag - likely to be zero

The following example shows an 'Connected' message with 'Device Event Class ID' of '4':

```
CEF:0|Kemp|LM|1.0|4|Connected|1|vs=10.35.46.235:443 event=Connected
srcip=10.35.2.98 srcport=51675 dstip=172.20.0.129 dstport=80
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
dstip	This is the destination IP address for this connection
dstport	This is the destination port for this connection

The following example shows a 'Connection Failed' message with 'Device Event Class ID' of '5':

```
CEF:0|Kemp|LM|1.0|5|Connection failed|3|vs=10.35.46.238:80 event=Connection
failed srcip=10.35.2.98 srcport=57378 dstip=172.20.0.129 dstport=82
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
dstip	This is the destination IP address for this connection
dstport	This is the destination port for this connection

The following example shows a 'Logged off' message with 'Device Event Class ID' of '6':

```
CEF:0|Kemp|LM|1.0|6|Logged off|1|vs=10.35.46.238:443 event=Logged off
user=mohit@kpauto.net srcip=10.35.2.98
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
user	The user that was entered in the ESP form and logged on
srcip	This is the source IP address that originated the request

The following example shows an 'User Interaction' message with 'Device Event Class ID' of '7':

```
CEF:0|Kemp|LM|1.0|7|User interaction|2|vs=10.35.46.238:443 event=User
interaction srcip=10.35.2.98 user=mohit@kpauto.net msg=requires password reset
```

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the

Extension key-value pair	Description
	same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
msg	This is a free form string providing extra details

The following example shows a 'Logged On' message with 'Device Event Class ID' of '8':

```
CEF:0|Kemp|LM|1.0|8|Logged on|1|vs=10.35.46.157:443 event=Logged on
srcip=10.35.2.45 user=mgupta@kempqaesp.net msg=logged on
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
user	The username of the user who attempted to log on
msg	This is a free-form string providing extra details

The following example shows an 'Access Denied' message with 'Device Event Class ID' of '9':

```
CEF:0|Kemp|LM|1.0|9|Access Denied|6|vs=10.35.46.252:443 event=Access Denied
srcip=10.35.8.8 user=mohit@kempqaesp.net msg=denied access
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request

Extension key-value pair	Description
user	The username of the user who attempted to log on
msg	This is a free-form string providing extra details

The following example shows an 'Access Blocked' message with 'Device Event Class ID' of '10':

```
CEF:0|Kemp|LM|1.0|10|Access Blocked|6|vs=10.35.46.242:443 event=Access Blocked
srcip=10.35.2.98 user=mohit msg=blocked access
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
user	The user that was entered into the ESP form and logged on
msg	This is a free-form string providing extra details

The following example shows an 'Access Locked' message with 'Device Event Class ID' of '11':

```
TBD
```

The following example shows an 'Access Disabled' message with 'Device Event Class ID' of '12':

```
CEF:0|Kemp|LM|1.0|12|Access Disabled|6|vs=10.35.46.252:443 event=Access
Disabled srcip=10.35.2.45 user=mohit@kempqaesp.net msg=account disabled
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header

Extension key-value pair	Description
srcip	This is the source IP address that originated the request
user	The user that was entered into the ESP form and logged on
msg	This is a free-form string providing extra details

The following example shows an 'Password Expired' message with 'Device Event Class ID' of '13':

```
CEF:0|Kemp|LM|1.0|13|Password Expired|6|vs=10.35.46.252:443 event=Password
Expired srcip=10.35.8.8 user=mohit@kempqaesp.net msg=password expired
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
user	The user that was entered into the ESP form and logged on
msg	This is a free-form string providing extra details

The following example shows a 'Request' message with 'Device Event Class ID' of '14':

```
CEF:0|Kemp|LM|1.0|14|Request|1|vs=10.35.46.157:443 event=Request
srcip=10.35.2.45 srcport=54548 method=GET url=https://10.35.46.157/
user=mgupta@kempqaesp.net useragent=Mozilla/5.0
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header

Extension key-value pair	Description
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
method	The HTML method, for example GET or POST.
URL	The URL that the user is trying to access.
user	The user making the request.
useragent	The user agent that process the user request

The following example shows an 'Attempt' message with 'Device Event Class ID' of '15':

```
CEF:0|Kemp|LM|1.0|15|Attempt|2|vs=10.35.46.252:443 event=Attempt
srcip=10.35.2.98 srcport=56593 method=GET url=https://10.35.46.252/owa/
useragent=Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101
Firefox/91.0
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
method	The HTML method, for example GET or POST.
URL	The URL that the user is trying to access.
useragent	The user agent that process the user request.

The following example shows an 'Attempted XSS attack' message with 'Device Event Class ID' of '16':

```
CEF:0|Kemp|LM|1.0|16|Attempted XSS attack|9|vs=10.35.46.238:443 event=Attempted
XSS attack srcip=10.35.2.98 srcport=61038 dtcode=6
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
dtcode	This only appears if someone is trying to access an ESP Virtual Service in a way that suggests they are trying to hack the system (for example, there are missing fields or bad characters in the request)

The following example shows an 'SMTP Parse Failure' message with 'Device Event Class ID' of '17':

```
CEF:0|Kemp|LM|1.0|17|SMTP parse failure|7|vs=10.1.133.11:25 event=SMTP parse
failure src=10.0.71.175:61401
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
src	This is the Source IP address: Port that originated the request

The following example shows an 'SMTP Blocked' message with 'Device Event Class ID' of '18':

```
CEF:0|Kemp|LM|1.0|18|SMTP Blocked|6|vs=10.1.133.11:25 event=SMTP Blocked
src=10.0.71.175:61401 resource=ktest.com
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination

Extension key-value pair	Description
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
src	This is the Source IP address: Port that originated the request
resource	The URL that someone is trying to access.

The following example shows a 'Blocked access to directory' message with 'Device Event Class ID' of '19':

```
CEF:0|Kemp|LM|1.0|19|Blocked access to directory|6|vs=10.35.46.238:443
event=Blocked access to directory srcip=10.35.2.98 srcport=61108 resource=/
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request
srcport	This is the source port that originated the request
resource	The URL or IP that someone is trying to access.

The following example shows a 'Blocked access to host' message with 'Device Event Class ID' of '20':

```
CEF:0|Kemp|LM|1.0|20|Blocked access to host|6|vs=10.35.46.238:443 event=Blocked
access to host srcip=10.35.2.98 srcport=61096 resource=10.35.46.238
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
srcip	This is the source IP address that originated the request

Extension key-value pair	Description
srcport	This is the source port that originated the request
resource	The URL or IP address that someone is trying to access.

SSOMGR CEF Logs

The following example shows a 'User AAA' message with 'Device Event Class ID' of '100':

```
CEF:0|Kemp|LM|1.0|100|User AAA|0|vs=10.35.46.235:443 event=User AAA
user=mohit@parent.net domain=parent.net server=172.21.135.103 protocol=LDAP
Unencrypted result=0:Success
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
user	The username of the user who attempted to log on
domain	The name of the domain to be used
server	This is the address of the server
protocol	This is the type of selected protocol
result	This is the result for this connection

The following example shows a 'User session timeout' message with 'Device Event Class ID' of '101':

```
CEF:0|Kemp|LM|1.0|101|User session timeout|0|vs=10.35.46.242:443 event=User
session timeout user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted expired
user session, start time:1629182393 duration:69 seconds
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination

Extension key-value pair	Description
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
user	The username of the user who attempted to log on
domain	The name of the domain to be used
msg	This is a free-form string providing extra details

The following example shows a 'User session kill' message with 'Device Event Class ID' of '102':

```
CEF:0|Kemp|LM|1.0|102|User session kill|0|vs=10.35.46.235:443 event=User
session kill user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted user
session, start time:1629378587 duration:8 seconds
```

The CEF Extension comprises of:

Extension key-value pair	Description
vs	This is the Virtual Service IP address: Port combination
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
user	The username of the user who attempted to log on
domain	The name of the domain to be used
msg	This is a free-form string providing extra details

The following example shows a 'Kill all sessions' message with 'Device Event Class ID' of '103':

CEF:0|Kemp|LM|1.0|103|Kill all sessions|0|event=Kill all sessions domain=MULLTIDOMAIN msg=Deleted 1 user session(s) associated with domain

The CEF Extension comprises of:

Extension key-value pair	Description
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
domain	The name of the domain to be used
msg	This is a free-form string providing extra details

The following example shows a 'Flush SSO cache' message with 'Device Event Class ID' of '104':

CEF:0|Kemp|LM|1.0|104|Flush SSO cache|1|event=Flush SSO cache msg=SSO cache being flushed user sessions:1 cookie sessions:1

The CEF Extension comprises of:

Extension key-value pair	Description
event	This is a string describing the event type; typically, the same as the 'Name' field in the CEF header
msg	This is a free-form string providing extra details

4

References

The following document provides further details about CEF logs:

https://community.microfocus.com/t5/ArcSight-Connectors/ArcSight-Common-Event-Format-CEF-Implementation-Standard/ta-p/1645557?attachment-id=68077