Common Event Format (CEF) Logs

Technical Note

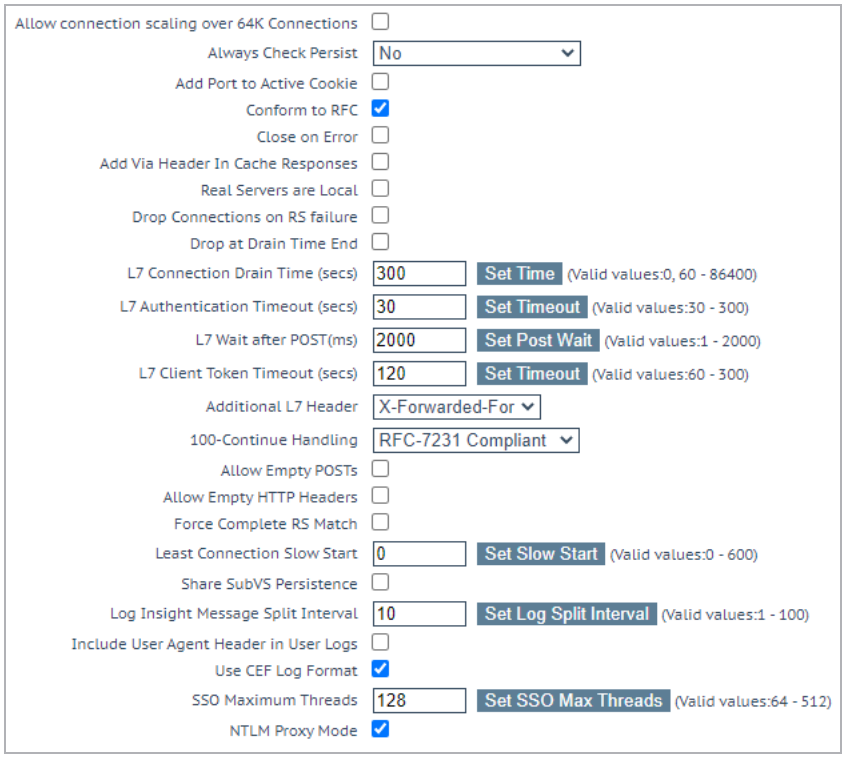
UPDATED: 19 March 2021

Copyright Notices

Table of Contents

1 Common Event Format (CEF) Logs

This document outlines the details of the Kemp 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.

CEF is an open log management standard that improves 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]
```

1.1 Related Firmware Version

This document was published with LoadMaster Operating System (LMOS) version 7.2.53. This document has not required substantial changes since 7.2.53. However, the content is in sync with the latest LoadMaster Generally Available (GA) firmware.

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

> 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 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.

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	Request	1 (Low)
12	Attempt	2 (Low)
13	Attempted XSS attack	9 (Very High)
14	SMTP parse failure	7 (High)
15	SMTP Blocked	6 (Medium)
16	Blocked access to directory	6 (Medium)
17	Blocked access to host	6 (Medium)

3 CEF Extension

The Kemp Technologies 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.

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

```
CEF:0|Kemp|LM|1.0|0|Accept|0|vs=10.35.56.32:80 event=Accept srcip=10.0.30.127
srcport=6045 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=10.0.70.142:80 event=Slave accept
srcip=10.35.2.94 srcport=56838 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=10.0.70.141:80 event=SSL accept
srcip=10.35.2.94 srcport=65431 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=10.0.70.141:80 event=Connection
timed out srcip=10.0.71.104 srcport=61956 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=10.35.56.32:80 event=Connected
srcip=10.0.30.127 srcport=8454 dstip=10.35.9.11 dstport=80
```

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
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=172.16.151.21:80 event=Connection failed srcip=192.168.10.67 srcport=17548 dstip=172.16.128.37 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=172.16.151.50:443 event=Logged off user=aduser1@kpauto.net srcip=192.168.10.67
```

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
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 'Accept' message with 'Device Event Class ID' of '7':

```
CEF:0|Kemp|LM|1.0|7|User Interaction|2|vs=10.0.70.141:443 event=User
Interaction srcip=10.35.2.94 srcport=6045 msg=User Interaction
```

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 a 'Logged On' message with 'Device Event Class ID' of '8':

```
CEF:0|Kemp|LM|1.0|8|Logged on|1|vs=10.0.70.141:80 event=Logged on
srcip=10.0.11.113 user=ruth 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=10.35.56.32:80 event=Access Denied
srcip=10.0.30.127 user=ExampleUser 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
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=10.0.70.141:443 event=Access Blocked
srcip=10.35.2.94 user=administrator 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 a 'Request' message with 'Device Event Class ID' of '11':

```
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.35.56.32:80 event=Request
srcip=10.0.30.127 srcport=8454 method=GET url=http://10.35.56.32/
user=peter@street.com
```

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.

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

```
CEF:0|Kemp|LM|1.0|12|Attempt|2|vs=172.16.151.21:80 event=Attempt
srcip=192.168.10.67 srcport=17946 method=GET url=http://172.16.151.21/
user=test.030@kpauto.net
```

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.
user	The user making the request.

The following example shows an 'Attempted XSS attack' message with 'Device Event Class ID' of '13':

```
CEF:0|Kemp|LM||1.0|13|Attempted XSS attack|9|vs=10.0.70.141:80 event=Attempted
XSS attack srcip=10.0.71.104 srcport=62098 dtcode=7
```

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
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 '14':

```
2020-06-24T15:51:08+00:00 lb100 l7log: CEF:0|Kemp|LM|1.0|14|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 '15':

```
2020-06-24T15:49:20+00:00 lb100 l7log: CEF:0|Kemp|LM|1.0|15|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
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 '16':

```
CEF:0|Kemp|LM|1.0|16|Blocked access to directory|6|vs=10.0.70.141:80
event=Blocked access to directory srcip=10.35.2.94 srcport=62951 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 that someone is trying to access.

The following example shows a 'Blocked access to host' message with 'Device Event Class ID' of '17':

```
CEF:0|Kemp|LM|1.0|17|Blocked access to host|6|vs=10.0.70.141:80 event=Blocked
access to host srcip=10.35.2.94 srcport=63054 resource=10.0.70.141
```

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 address that someone is trying to access.

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

Last Updated Date

This document was last updated on 19 March 2021.