opentext™

ArcSight SmartConnectors

Software Version: 24.2

Implementing ArcSight Common Event Format (CEF) - Version 27

Document Release Date: April 2024
Software Release Date: April 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Contents

What is CEF?

Common Event Format (CEF) is an extensible, text-based format designed to support multiple device types by offering the most relevant information. Message syntaxes are reduced to work with ESM normalization. CEF specifically defines a syntax for log records containing a standard header and a variable extension, formatted as key-value pairs. The CEF format can be used with on-premise devices by implementing the ArcSight Syslog SmartConnector. CEF can also be used by cloud-based service providers by implementing the SmartConnector for ArcSight Common Event Format REST.

Note: This guide describes ArcSight CEF standard only. For information about descriptions of fields or schemas related to specific ArcSight products, such as the ArcSight Manager, ArcSight Logger, or ArcSight SmartConnector, contact Customer Support.

The Case for ArcSight CEF

The central problem of any security information and event management (SIEM) environment is integration. Device vendors each have their own format for reporting event information, and such diversity can make customer site integration time consuming and expensive. The CEF standard format, developed by ArcSight, enables vendors and their customers to quickly integrate their product information into ESM.

The CEF standard format is an open log management standard that simplifies log management. CEF allows third parties to create their own device schemas that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, for later analysis by an enterprise management system.

CEF Implementation

This document defines the CEF protocol and provides details about implementing the standard. It details the header and predefined extensions used within the standard, and explains the procedure to create user-defined extensions. It also includes a list of CEF supported date formats.

Header Information

CEF uses Syslog as a transport mechanism. It uses the following format that contains a Syslog prefix, a CEF header, and one or more extensions in this format:

```
<Syslog_prefix> <CEF_header>|[Extension]
```

The CEF header consists of seven fields separated by a pipe character (|). If the pipe character (|) is used in a “value” part of a CEF header field, it must be escaped. The pipe delimiter between the header fields must not be escaped.

The CEF header is -

```
CEF:Version|Vendor|Product|Version|Message ID|Name|Severity|
```

Header Field Definitions

Header Name	Field Name	Type	Size	Description
CEF Version	CEF Version	String	N/A	**CEF Version** 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 format versions are: • 0 (CEF:0) - for CEF Specification version 0.1 • 1 (CEF:1) - for CEF Specification version 1.x For example, for CEF Specification version 1.2, the value of the **CEF Version** header field will be "**1**".
Vendor	deviceVendor	String	63	**deviceProduct** and **deviceVendor** are strings that uniquely identify the type of device that sent the message. No two products might use the same deviceVendor and deviceProduct pair. There is no central authority managing these pairs. Event producers must ensure that they assign unique name pairs.
Product	deviceProduct	String	63	
Version	deviceVersion	String	31	The **deviceVersion** is the version of the product producing the logs.

Message ID	deviceEventClassId	String	1023	**deviceEventClassId** is a unique identifier for each event-type. This can be a string or an integer. deviceEventClassId identifies the type of event reported. In the Intrusion Detection System (IDS) world, each signature or rule that detects certain activity has a unique **Signature ID** assigned. This is a requirement for other types of devices as well and helps correlation engines process the events. It is also known as Signature ID. **Note**: The '=', '%' , and '#'characters must be escaped in the vulnerability string that are mapped to **deviceEventClassId** , and if they are present in the description or name of the vulnerability. However, these characters must not be escaped when used as a delimiter.
Name	name	String	512	**name** is a string representing a human readable and understandable description of the event. The event name must not contain information that is specifically mentioned in other fields. For example: "Port scan from 10.0.0.1 targeting 20.1.1.1" is not a good event name. It must be: "Port scan". The other information is redundant and can be picked up from the rest of the fields.
Severity	agentSeverity	AgentSeverityEnumeration	N/A	**agentSeverity** is a string or integer and it reflects the importance of the event. • The valid string values are: **Unknown**, **Low**, **Medium**, **High**, and **Very-High**. • The valid integer values are: **0=Unknown**, **1-3=Low**, **4-6=Medium**, **7- 8=High**, and **9-10=Very-High**.

In which,

`CEF:Version` - is a mandatory header. The rest of the message is formatted using fields delimited by a pipe ("|") character. All of the following fields must be present and defined under "What is CEF?" on page 4.

`[Extension]` - is a placeholder for additional fields, but is not mandatory. Any additional fields are logged as key-value pairs. For a table of definitions, see ArcSight Extension Dictionary.

The following examples illustrate a CEF message using Syslog transport:

For CEF 0.x version

```
Sep 19 08:26:10 host CEF:0|Security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

For CEF 1.x version

```
Sep 29 08:26:10 host CEF:1|Security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Using CEF Without Syslog

Syslog applies a syslog prefix to each message, no matter which device it arrives from, that contains the date and hostname in the following example:

```
Jan 18 11:07:53 host CEF:Version|…
```

Even if an event producer is unable to write Syslog messages, it is possible to write the events to a file by performing the following steps:

1. Discard the syslog prefix (`Jan 18 11:07:53 host`).
2. Begin the message with the following format:

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

The Extension Field

The **Extension** field contains a collection of key-value pairs. The keys are part of a predefined set. The standard allows to include additional keys as described in the ArcSight Extension Dictionary section. An event can contain any number of key-value pairs in any order, separated by spaces (" "). If a field contains a space, such as a file name, this is valid and can be logged in exactly that manner, as shown in the following example:

```
filePath=/user/username/dir/my file name.txt
```

Note:

- If there are multiple spaces before a key, all spaces but the last space are treated as trailing spaces in the prior value in the key. If you need trailing spaces, use multiple spaces, otherwise, use one space between the end of a value and the start of the following key.
- Trailing spaces are not preserved for the final key-value pair in the extension. It is highly recommended to not utilize leading or trailing spaces in CEF events unless absolutely necessary. If that is the case, ensure the ordering of key-value pairs in the extension is such that any value with trailing spaces is not the final value. For more information on best practices for creating CEF events, see the CEF Mapping Guidelines document.
- Extension values must follow the escape character guidelines defined for encoding symbols in CEF. See, "Character Encoding" below.

Character Encoding

Because CEF uses the UTF-8 Unicode encoding method, certain symbols must use character encoding. Within this context, character encoding specifies how to represent characters that could be misinterpreted within the schema.

Ensure the following when encoding symbols in CEF:

- The entire message must be UTF-8 encoded.
- Spaces used in the header are valid. Do not encode a space character by using <space>.
- If a pipe (|) is used in the header, it must be escaped with a backslash (\). But note that the pipes in the extension do not need escaping. For example:

  ```
  Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a \| in message|10|src=10.0.0.1 act=blocked a | dst=1.1.1.1
  ```
- If a backslash (\) is used in the header or the extension, it must be escaped with another backslash (\). For example:

  ```
  Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a \\ in packet|10|src=10.0.0.1 act=blocked a \\ dst=1.1.1.1
  ```
- If an equal sign (=) is used in the extensions, it has to be escaped with a backslash (\). Equal signs in the header need no escaping. For example:

  ```
  Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a = in message|10|src=10.0.0.1 act=blocked a \= dst=1.1.1.1
  ```
- Multi-line fields can be sent by CEF by encoding the newline character as \n or \r. Note that multiple lines are only allowed in the value part of the extensions. For example:

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|Detected a
threat. No action needed.|10|src=10.0.0.1 msg=Detected a threat.\n No
action needed
```

ArcSight Extension Dictionary

The CEF Key Names For Event Producers and CEF Key Names for Event Consumers tables list the predefined names that establish usages for both event producers and event consumers. While the fields listed in both the tables are useful event consumers, the fields listed in the CEF Key Names for Event Consumers table must not be set by event producers.

Note:

- The **bytesIn** and **bytesOut** fields were containing only Integer values in CEF 0.1. However, from CEF 1.0 onwards, these fields also contain the Long values.
- All IP address fields in CEF 0.1 were containing IPv4 addresses only. However, from CEF 1.0 onwards, these fields also contain IPv6 addresses.

CEF Key Names for Event Producers

This table displays the CEF names along with the full names for each CEF key name. When sending events, the CEF key name is the proper form to use, because using the full name to send an event will fail.

CEF Key Names for Event Producers

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceAction	act	String	63	Action taken by the device.
0.1	applicationProtocol	app	String	31	Application level protocol, example: HTTP, HTTPS, SSHv2, Telnet, POP, IMPA, IMAPS, and so on.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomIPv6Address1	c6a1	IpAddress		One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.
0.1	deviceCustomIPv6Address1Label	c6a1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomIPv6Address3	c6a3	IpAddress		One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomIPv6AddressLabel	c6a3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomIPv6Address4	c6a4	IPv6 Address		One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.
0.1	deviceCustomIPv6Address4Label	c6a4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceEventCategory	cat	String	1023	Represents the category assigned by the originating device. Devices often use their own categorization schema to classify event. Example: "/Monitor/Disk/Read"

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomFloatingPoint1	cfp1	Double		One of our floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustoFloatingPoint1Label	cfp1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint2	cfp2	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustomFloatingPoint2Label	cfp2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint3	cfp3	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomFloatingPoint3Label	cfp3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint4	cfp4	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustomFloatingPoint4Label	cfp4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber1	cn1	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomNumber1Label	cn1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber2	cn2	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
0.1	deviceCustomNumber2Label	cn2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber3	cn3	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomNumber3Label	cn3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	baseEventCount	cnt	Integer		A count associated with this event. How many times was this same event observed? Count can be omitted if it is 1.
0.1	deviceCustomString1	cs1	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User- Defined Extensions.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString1Label	cs1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomString2	cs2	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.
0.1	deviceCustomString2Label	cs2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString3	cs3	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.
0.1	deviceCustomString3Label	cs3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString4	cs4	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User- Defined Extensions.
0.1	deviceCustomString4Label	cs4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString5	cs5	String	4000	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User- Defined Extensions.
0.1	deviceCustomString5Label	cs5Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomString6	cs6	String	4000	One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User- Defined Extensions.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString6Label	cs6Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	destinationDnsDomain	destinationDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).
0.1	destinationServiceName	destinationServiceName	String	1023	The service targeted by this event. Example: “sshd”
0.1	destinationTranslatedAddress	destinationTranslatedAddress	IpAddress		Identifies the translated destination that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
0.1	destinationTranslatedPort	destinationTranslatedPort	Integer		Port after it was translated; for example, a firewall. Valid port numbers are 0 to 65535.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomDate1	deviceCustomDate1	DateTime		One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User- Defined Extensions.
0.1	deviceCustomDate1Label	deviceCustomDate1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomDate2	deviceCustomDate2	DateTime		One of the two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. **TIP**: For tips on using these fields, see the guidelines defined under User-Defined Extensions.
0.1	deviceCustomDate2Label	deviceCustomDate2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceDirection	deviceDirection	DeviceDirectionEnumeration		Any information about what direction the observed communication has taken. The following values are supported: “0” for inbound or “1” for outbound
0.1	deviceDnsDomain	deviceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceExternalId	deviceExternalId	String	255	A name that uniquely identifies the device generating this event.
0.1	deviceFacility	deviceFacility	String	1023	The facility generating this event. For example, Syslog has an explicit facility associated with every event.
0.1	deviceInboundInterface	deviceInboundInterface	String	128	Interface on which the packet or data entered the device.
0.1	deviceNtDomain	deviceNtDomain	String	255	The Windows domain name of the device address.
0.1	deviceOutboundInterface	deviceOutboundInterface	String	128	Interface on which the packet or data left the device.
0.1	devicePayloadId	DevicePayloadId	String	128	Unique identifier for the payload associated with the event.
0.1	deviceProcessName	deviceProcessName	String	1023	Process name associated with the event. An example might be the process generating the syslog entry in UNIX.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceTranslatedAddress	deviceTranslatedAddress	IpAddress		Identifies the translated device address that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
0.1	destinationHostName	dhost	String	1023	Identifies the destination that an event refers to in an IP network. The format must be a fully qualified domain name (FQDN) associated with the destination node, when a node is available. Examples: “host.domain.com” or “host”.
0.1	destinationNtDomain	dntdom	String	255	The Windows domain name of the destination address.
0.1	destinationProcessId	dpid	Integer		Provides the ID of the destination process associated with the event. For example, if an event contains process ID 105, “105” is the process ID.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationUserPrivileges	dpriv	String	1023	The typical values are “Administrator”, “User”, and “Guest”. This identifies the destination user’s privileges. In UNIX, for example, activity executed on the root user would be identified with destinationUser Privileges of “Administrator”.
0.1	destinationProcessName	dproc	String	1023	The name of the event’s destination process. Example: “telnetd” or “sshd”.
0.1	destinationPort	dpt	Integer		The valid port numbers are between 0 and 65535.
0.1	destinationAddress	dst	IpAddress		Identifies the destination address that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
0.1	deviceTimeZone	dtz	String	255	The timezone for the device generating the event.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationUserId	duid	String	1023	Identifies the destination user by ID. For example, in UNIX, the root user is generally associated with user ID 0.
0.1	destinationUserName	duser	String	1023	Identifies the destination user by name. This is the user associated with the event's destination. Email addresses are often mapped into the UserName fields. The recipient is a candidate to put into this field.
0.1	deviceAddress	dvc	IpAddress		Identifies the device address that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
0.1	deviceHostName	dvchost	String	63	The format should be a fully qualified domain name (FQDN) associated with the device node, when a node is available. Example: "host.domain.com" or "host".

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationMacAddress	dmac	MacAddress		Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
0.1	deviceProcessId	dvcpid	Integer		Provides the ID of the process on the device generating the event.
0.1	endTime	end	DateTime		The time at which the activity related to the event ended. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st1970). An example would be reporting the end of a session.
0.1	externalId	externalId	String	40	The ID used by an originating device. They are usually increasing numbers, associated with events.
0.1	fileCreateTime	fileCreateTime	DateTime		Time when the file was created.
0.1	fileHash	fileHash	String	255	Hash of a file.
0.1	fileId	fileId	String	1023	An ID associated with a file could be the inode.
0.1	fileModificationTime	fileModificationTime	DateTime		Time when the file was last modified.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	filePath	filePath	String	1023	Full path to the file, including file name itself. Example: C:\Program Files \WindowsNT\Accessories\ wordpad.exe or /usr/bin/zip
0.1	filePermission	filePermission	String	1023	Permissions of the file.
0.1	fileType	fileType	String	1023	Type of file (pipe, socket, etc.)
0.1	flexDate1	flexDate1	DateTime		A timestamp field available to map a timestamp that does not apply to any other defined timestamp field in this dictionary. Use all flex fields sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
0.1	flexDate1Label	flexDate1Label	String	128	The label field is a string and describes the purpose of the flex field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	flexString1	flexString1	String	1023	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
0.1	flexString1Label	flexString1Label	String	128	The label field is a string and describes the purpose of the flex field.
0.1	flexString2	flexString2	String	1023	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	flexString2Label	flexString2Label	String	128	The label field is a string and describes the purpose of the flex field.
0.1	fileName	fname	String	1023	Name of the file only (without its path).
0.1	fileSize	fsize	Long		Size of the file.
0.1	bytesIn	in	Integer		Number of bytes transferred inbound, relative to the source to destination relationship, meaning that data was flowing from source to destination.
0.1	message	msg	String	1023	An arbitrary message giving more details about the event. Multi-line entries can be produced by using \n as the new line separator.
0.1	oldFileCreateTime	oldFileCreateTime	DateTime		Time when old file was created.
0.1	oldFileHash	oldFileHash	String	255	Hash of the old file.
0.1	oldFileId	oldFileId	String	1023	An ID associated with the old file could be the inode.
0.1	oldFileModificationTime	oldFileModificationTime	DateTime		Time when old file was last modified.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	oldFileName	oldFileName	String	1023	Name of the old file.
0.1	oldFilePath	oldFilePath	String	1023	Full path to the old file, including the file name itself. Examples: c:\Program Files\WindowsNT\Accessories\wordpad.exe or /usr/bin/zip
0.1	oldFilePermission	oldFilePermission	String	1023	Permissions of the old file.
0.1	oldFileSize	oldFileSize	Long		Size of the old file.
0.1	oldFileType	oldFileType	String	1023	Type of the old file (pipe, socket, etc.)
0.1	bytesOut	out	Integer		Number of bytes transferred outbound relative to the source to destination relationship. For example, the byte number of data flowing from the destination to the source.
0.1	eventOutcome	outcome	String	63	Displays the outcome, usually as 'success' or 'failure'.
0.1	transportProtocol	proto	String	31	Identifies the Layer-4 protocol used. The possible values are protocols such as TCP or UDP.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	reason	reason	String	1023	The reason an audit event was generated. For example “badd password” or “unknown user”. This could also be an error or return code. Example: “0x1234”
0.1	requestUrl	request	String	1023	In the case of an HTTP request, this field contains the URL accessed. The URL should contain the protocol as well. Example: “http://www/secure.com”
0.1	requestClientApplication	requestClientApplication	String	1023	The User-Agent associated with the request.
0.1	requestContext	requestContext	String	2048	Description of the content from which the request originated (for example, HTTP Referrer)
0.1	requestCookies	requestCookies	String	1023	Cookies associated with the request.
0.1	requestMethod	requestMethod	String	1023	The method used to access a URL. Possible values: “POST”, “GET”, etc.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceReceiptTime	rt	DateTime		The time at which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970)
0.1	sourceHostName	shost	String	1023	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name (FQDN) associated with the source node, when a mode is available. Examples: "host" or "host.domain.com".
0.1	sourceMacAddress	smac	MacAddress		Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
0.1	sourceNtDomain	sntdom	String	255	The Windows domain name for the source address.
0.1	sourceDnsDomain	sourceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceServiceName	sourceServiceName	String	1023	The service that is responsible for generating this event.
0.1	sourceTranslatedAddress	sourceTranslatedAddress	IpAddress		Identifies the translated source that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
0.1	sourceTranslatedPort	sourceTranslatedPort	Integer		A port number after being translated by, for example, a firewall. Valid port numbers are 0 to 65535.
0.1	sourceProcessId	spid	Integer		The ID of the source process associated with the event.
0.1	sourceUserPrivileges	spriv	String	1023	The typical values are “Administrator”, “User”, and “Guest”. It identifies the source user’s privileges. In UNIX, for example, activity executed by the root user would be identified with “Administrator”.
0.1	sourceProcessName	sproc	String	1023	The name of the event’s source process.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourcePort	spt	Integer		The valid port numbers are 0 to 65535.
0.1	sourceAddress	src	IpAddress		Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
0.1	startTime	start	DateTime		The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970)

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceUserId	suid	String	1023	Identifies the source user by ID. This is the user associated with the source of the event. For example, in UNIX, the root user is generally associated with user ID 0.
0.1	sourceUserName	suser	String	1023	Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into this field.
0.1	type	type	TypeEnumeration		0 means base event, 1 means aggregated, 2 means correlation, and 3 means action. This field can be omitted for base events (type 0).

CEF Key Names for Event Consumers

This table displays the CEF names along with the full names for each name. When sending events, the CEF key name is the proper form to use. If you use the full name to send an event, then it will fail.

CEF Key Names For Event Consumers

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	agentDnsDomain	agentDnsDomain	String	255	The DNS domain name of the ArcSight connector that processed the event.
0.1	agentNtDomain	agentNtDomain	String	255	
0.1	agentTranslatedAddress	agentTranslatedAddress	IpAddress		
0.1	agentTranslatedZoneExternalID	agentTranslatedZoneExternalID	String	200	
0.1	agentTranslatedZoneURI	agentTranslatedZoneURI	String	2048	
0.1	agentZoneExternalID	agentZoneExternalID	String	200	
0.1	agentZoneURI	agentZoneURI	String	2048	
0.1	agentAddress	agt	IpAddress		The IP address of the ArcSight connector that processed the event.
0.1	agentHostName	ahost	String	1023	The hostname of the ArcSight connector that processed the event.
0.1	agentId	aid	String	40	The agent ID of the ArcSight connector that processed the event.
0.1	agentMacAddress	amac	MacAddress		The MAC address of the ArcSight connector that processed the event.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	agentReceiptTime	art	DateTime		The time at which information about the event was received by the ArcSight connector.
0.1	agentType	at	String	63	The agent type of the ArcSight connector that processed the event
0.1	agentTimeZone	atz	String	255	The agent time zone of the ArcSight connector that processed the event.
0.1	agentVersion	av	String	31	The version of the ArcSight connector that processed the event.
0.1	customerExternalID	customerExternalID	String	200	
0.1	customerURI	customerURI	String	2048	
0.1	destinationTranslatedZoneExternalID	destinationTranslatedZoneExternalID	String	200	
0.1	destinationTranslatedZoneURI	destinationTranslatedZoneURI	String	2048	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
0.1	destinationZoneExternalID	destinationZoneExternalID	String	200	
0.1	destinationZoneURI	destinationZoneURI	String	2048	The URI for the Zone that the destination asset has been assigned to in ArcSight.
0.1	deviceTranslatedZoneExternalID	deviceTranslatedZoneExternalID	String	200	

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceTranslatedZoneURI	deviceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the device asset has been assigned to in ArcSight.
0.1	deviceZoneExternalID	deviceZoneExternalID	String	200	
0.1	deviceZoneURI	deviceZoneURI	String	2048	Thee URI for the Zone that the device asset has been assigned to in ArcSight.
0.1	destinationGeoLatitude	dlat	Double		The latitudinal value from which the destination's IP address belongs.
0.1	destinationGeoLongitude	dlong	Double		The longitudinal value from which the destination's IP address belongs.
0.1	eventId	eventId	Id		This is a unique ID that ArcSight assigns to each event.
0.1	rawEvent	rawEvent	String	4000	
0.1	sourceGeoLatitude	slat	Double		
0.1	sourceGeoLongitude	slong	Double		
0.1	sourceTranslatedZoneExternalID	sourceTranslatedZoneExternalID	String	200	
0.1	sourceTranslatedZoneURI	sourceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
0.1	sourceZoneExternalID	sourceZoneExternalID	String	200	

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceZoneURI	sourceZoneURI	String	2048	The URI for the Zone that the source asset has been assigned to in ArcSight.
1.2	agentTranslatedZoneKey	agentTranslatedZoneKey	Long	64-bit	ID of an agentTranslatedZone resource reference.
1.2	agentZoneKey	agentZoneKey	Long	64-bit	ID of an agentZone resource reference.
1.2	customerKey	customerKey	Long	64-bit	ID of a customer resource reference.
1.2	destinationTranslatedZoneKey	destinationTranslatedZoneKey	Long	64-bit	ID of a destinationTranslatedZone resource reference.
1.2	destinationZoneKey	dZoneKey	Long	64-bit	ID of a destinationZone resource reference.
1.2	deviceTranslatedZoneKey	deviceTranslatedZoneKey	Long	64-bit	ID of a deviceTranslatedZone resource reference.
1.2	deviceZoneKey	deviceZoneKey	Long	64-bit	ID of a deviceZone resource reference.
1.2	sourceTranslatedZoneKey	sTranslatedZoneKey	Long	64-bit	ID of a sourceTranslatedZone resource reference.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
1.2	sourceZoneKey	sZoneKey	Long	64-bit	ID of a sourceZone resource reference.
1.2	parserVersion	parserVersion	String	8	The release timestamp (DD-MM-YY) of the parser file that processed the event.
1.2	parserIdentifier	parserIdentifier	String	36	The parser ID of the parser file that processed the event.

Special Mappings

In some cases, the mappings between fields of the original device and those of the ArcSight Extension Dictionary are not obvious. In that case, refer to the example in the following tables.

Firewall

Original Field	Mapped to CEF Name	Mapped to Full Name
Rule Number / ACL Number	cs1	deviceCustomString1

Anti-Virus

Original Field	Mapped to CEF Name	Mapped to Full Name
Virus name	cs1	deviceCustomString1
Signature / Engine Version	cs2	deviceCustomString2
Action (Quartine, Cleaned, Deleted, …)	act	deviceAction

Email

Original Field	Mapped to CEF Name	Mapped to Full Name
Recipient (for example, user@company.com)	duser	destinationUserName
Sender (for example, user@company.com)	suser	sourceUserName
Relay	cs1	deviceCustomString1

Wireless

Original Field	Mapped to CEF Name	Mapped to Full Name
SSID	cs2	deviceCustomString2
Channel	cn1	deviceCustomNumber1

IPv6 Format

The connector code automatically sets labels for the **IPv6 address** fields if the field is set. You can set the label to the following values: **Device IPv6 Address**, **Source IPv6 Address**, and **Destination IPv6 Address**.

If the custom extension name is in IPv6 format and used to map:

- device address, then use **c6a1**. Use **Device IPv6 Address** as the label, or let the connector code set the label for you.
- source address, then use **c6a2**. Use **SourceIPv6 Address** as the label, or let the connector code set the label for you.
- destination address, then use **c6a3**. Use **Destination IPv6 Address** as the label, or let the connector code set the label for you.

User-Defined Extensions

The Extension Dictionary provides a set of predefined extension names (CEF names such as "fname" and full names such as "filetype") that must cover most event log requirements. However, vendors' devices might generate more information that can be appropriately mapped into the predefined extensions or might generate information that

does not fit the orientation of the predefined extensions. In such cases, vendors can define their own custom extensions.

Custom Extension Naming Guidelines

Ensure the following when creating custom extensions:

Format

Custom extension names must take the form:
`VendornameProductnameExplanatoryKeyName`

Requirements

Custom extension names must meet the following requirements. Custom extension name (s) must be:

- a single word, with no spaces.
- alphanumeric.
- as clear and concise as possible.
- named different than any name listed in ArcSight Extension Dictionary.

Limitations of Custom Extensions

Custom extension names are recommended for use only when no reasonable mapping of the information can be established for a predefined CEF name. While the custom extension name mechanism can be used to safely send information to CEF consumers for storage, there are certain limitations as to when and how to access the data mapped into them.

Custom extension names also have significant limitations that implementers should be aware of. These limitations can fundamentally affect the experience of ArcSight product users.

Limitations Affecting ArcSight ESM

- Data submitted to ArcSight ESM using custom name extensions is retained, but is largely inaccessible except when directly viewing events. This data shows up in a section called "Additional Data".

- Data submitted to ArcSight ESM using custom name extensions cannot be used directly for reporting, as these "Additional Data" fields are not made available in the reporting schema. Thus, any data in the "Additional Data" section of events is not available in reports.
- Data submitted to ArcSight ESM using custom name extensions cannot be used directly for event correlation (as within Rules, Data Monitors, etc.). Therefore, any data in the "Additional Data" section is not available as output for correlation activities within the ESM system.

Limitations Affecting ArcSight Logger

- Data submitted to ArcSight Logger using custom name extensions is retained in the system, but is not available for use in the Logger reporting infrastructure.
- Data submitted to ArcSight Logger using custom name extensions is available for viewing by the customer using string-based search. Event export is also available for this purpose.

Appendix A: Date Formats

CEF supports several variations on time and date formats to accurately identify the time an event occurred. These formats are as follows:

- Milliseconds since January 1, 1970 (integer).

  This time format supplies an integer with the count in milliseconds from January 1, 1970 to the time the event occurred.
- MMM dd HH:mm:ss.SSS zzz
- MMM dd HH:mm:sss.SSS
- MMM dd HH:mm:ss zzz
- MMM dd HH:mm:ss
- MMM dd yyyy HH:mm:ss.SSS zzz
- MMM dd yyyy HH:mm:ss.SSS
- MMM dd yyyy HH:mm:ss zzz
- MMM dd yyyy HH:mm:ss

For a key to the date formats shown above, refer to the SimpleDateFormat page from the API specification for the Java™ Platform, Standard Edition document.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Implementing ArcSight Common Event Format (CEF) - Version 27 (SmartConnectors 24.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!