Micro Focus Security ArcSight Common Event Format

Implementing ArcSight Common Event Format (CEF)

Version 25

September 28, 2017

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Phone	A list of phone numbers is available on the Micro Focus Security ArcSight Technical Support Page: https://softwaresupport.softwaregrp.com/
Support Web Site	https://softwaresupport.softwaregrp.com/
Protect 724 Community	https://community.softwaregrp.com/t5/ArcSight-Connectors/tkb-p/connector-documentation.

Revision History

Date	Description
09/28/2017	Moved cat field from Event Consumer table to Event Producer table.
08/22/2017	Added explanation of preservation of trailing spaces to the section “The Extension Field.”.

Contents

Chapter 1: What is CEF?

CEF is an extensible, text-based format designed to support multiple device types by offerring the most relevant information. Message syntaxes are reduced to work with ESM normalization. Specifically, CEF defines a syntax for log records comprised of 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 and does not include descriptions of fields or schemas related to ArcSight products, such as the ArcSight Manager, ArcSight Logger, or ArcSight SmartConnectors. If you need that type of information, 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 Common Event Format (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 Certification

The Enterprise Security Products Technology Alliance Program assists technology companies that want to adopt, test, and certify their compatibility with the CEF standard and by extension ArcSight interoperability. The CEF Technology Alliance Program provides a process that includes documentation, event categorization assistance, technical and marketing support along with access to a hosted ArcSight ESM solution for testing. For more information, see the Micro Focus Security Products Program Guide on Protect724.

CEF Implementation

This document defines the CEF protocol and provides details on how to implement the standard. It details the header and predefined extensions used within the standard, as well as how 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, comprised of a `syslog prefix,` a `header` and an `extension`, as shown below:

```
Jan 18 11:07:53 host CEF:Version|Device Vendor|Device Product|Device
Version|Device Event Class ID|Name|Severity|[Extension]
```

The `CEF:Version` portion of the message is a mandatory header. The remainder of the message is formatted using fields delimited by a pipe ("|") character. All of these remaining fields should be present and are defined under “Header Field Definitions” on the next page.

The `extension` portion of the message is a placeholder for additional fields, but is not mandatory. Any additional fields are logged as key-value pairs. See "ArcSight Extension Dictionary" for a table of definitions.

The following example illustrates a CEF message using Syslog transport:

```
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
```

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, as shown below.

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

However, if an event producer is unable to write syslog messages, it is still possible to write the events to a file.

To do so:

1. Omit the syslog prefix (Jan 18 11:07:53 host).
2. Begin the message with the format shown below:

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

Header Field Definitions

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 version is 0 (`CEF:0`).

Device Vendor, **Device Product** and **Device Version** 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.

Device Event Class ID is a unique identifier per event-type. This can be a string or an integer. 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 as well, and helps correlation engines process the events. Also known as Signature ID.

Name 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. For example: "Port scan from 10.0.0.1 targeting 20.1.1.1" is not a good event name. It should be: "Port scan". The other information is redundant and can be picked up from the other fields.

Severity 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 Extension Field

The **Extension** field contains a collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys as outlined in “ArcSight Extension Directory” later in this document. 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 below:

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

Notes:

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.

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.

Note the following when encoding symbols in CEF:

The entire message should 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 has to be escaped with a backslash (\). But note that 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 has to 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.
```

Chapter 2: ArcSight Extension Dictionary

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

CEF Key Names for Event Producers

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; using the full name to send an event will fail.

CEF Key Names for Event Producers

CEF Key Name	Full Name	Data Type	Length	Meaning
act	deviceAction	String	63	Action taken by the device.
app	applicationProtocol	String	31	Application level protocol, example values are HTTP, HTTPS, SSHv2, Telnet, POP, IMPA, IMAPS, and so on.
c6a1	deviceCustomIPv6Address1	IPv6 address		One of four IPv6 address fields available to map fields that do not apply to any other in this dictionary. TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
c6a1Label	deviceCustomIPv6 Address1Label	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.
c6a3	deviceCustomIPv6Address3	IPv6 address		One of four IPv6 address fields available to map fields that do not apply to any other in this dictionary. TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
c6a3Label	deviceCustomIPv6Address3 Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and

CEF Key Name	Full Name	Data Type	Length	Meaning
				describes the purpose of the custom field.
c6a4	deviceCustomIPv6 Address4	IPv6 address		One of four IPv6 address fields available to map fields that do not apply to any other in this dictionary. TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
C6a4Label	deviceCustomIPv6 Address4Label	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.
cat	deviceEventCategory	String	1023	Represents the category assigned by the originating device. Devices often use their own categorization schema to classify event. Example: "/Monitor/Disk/Read"
cfp1	deviceCustomFloatingPoint1	Floating Point		One of four floating point fields available to map fields that do not apply to any other in this dictionary.
cfp1Label	deviceCustom FloatingPoint1Label	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.
cfp2	deviceCustomFloatingPoint2	Floating Point		One of four floating point fields available to map fields that do not apply to any other in this dictionary.
cfp2Label	deviceCustomFloatingPoint2 Label	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.
cfp3	deviceCustomFloatingPoint3	Floating Point		One of four floating point fields available to map fields that do not apply to any other in this dictionary.

CEF Key Name	Full Name	Data Type	Length	Meaning
cfp3Label	deviceCustom FloatingPoint3Label	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.
cfp4	deviceCustomFloatingPoint4	Floating Point		One of four floating point fields available to map fields that do not apply to any other in this dictionary.
cfp4Label	deviceCustom FloatingPoint4Label	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.
cn1	deviceCustomNumber1	Long		One of 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.
cn1Label	deviceCustomNumber1Label	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.
cn2	DeviceCustomNumber2	Long		One of 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.
cn2Label	deviceCustomNumber2Label	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.
cn3	deviceCustomNumber3	Long		One of 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 Key Name	Full Name	Data Type	Length	Meaning
cn3Label	deviceCustomNumber3Label	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.
cnt	baseEventCount	Integer		A count associated with this event. How many times was this same event observed? Count can be omitted if it is 1.
cs1	deviceCustomString1	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: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs1Label	deviceCustomString1Label	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.
cs2	deviceCustomString2	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: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs2Label	deviceCustomString2Label	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.
cs3	deviceCustomString3	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.

CEF Key Name	Full Name	Data Type	Length	Meaning
				TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs3Label	deviceCustomString3Label	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.
cs4	deviceCustomString4	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: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs4Label	deviceCustomString4Label	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.
cs5	deviceCustomString5	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: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs5Label	deviceCustomString5Label	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.
cs6	deviceCustomString6	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.

CEF Key Name	Full Name	Data Type	Length	Meaning
				TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
cs6Label	deviceCustomString6Label	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.
destination DnsDomain	destinationDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).
destination ServiceName	destinationServiceName	String	1023	The service targeted by this event. Example: "sshd"
destination Translated Address	destinationTranslated Address	IPv4 Address		Identifies the translated destination that the event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
destination TranslatedPort	destinationTranslatedPort	Integer		Port after it was translated; for example, a firewall. Valid port numbers are 0 to 65535.
deviceCustom Date1	deviceCustomDate1	TimeStamp		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: See the guidelines under "User-Defined Extensions" for tips on using these fields.
deviceCustom Date1Label	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.
deviceCustom Date2	deviceCustomDate2	TimeStamp		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.

CEF Key Name	Full Name	Data Type	Length	Meaning
				TIP: See the guidelines under "User-Defined Extensions" for tips on using these fields.
deviceCustom Date2Label	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.
deviceDirection	deviceDirection	Integer		Any information about what direction the observed communication has taken. The following values are supported: "0" for inbound or "1" for outbound
deviceDns Domain	deviceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).
device ExternalId	deviceExternalId	String	255	A name that uniquely identifies the device generating this event.
deviceFacility	deviceFacility	Stirng	1023	The facility generating this event. For example, Syslog has an explicit facility associated with every event.
deviceInbound Interface	deviceInboundInterface	String	128	Interface on which the packet or data entered the device.
deviceNt Domain	deviceNtDomain	String	255	The Windows domain name of the device address.
Device Outbound Interface	deviceOutboundInterface	String	128	Interface on which the packet or data left the device.
Device PayloadId	devicePayloadId	String	128	Unique identifier for the payload associated with the event.
deviceProcess Name	deviceProcessName	String	1023	Process name associated with the event. An example might be the process generating the syslog entry in UNIX.
device Translated Address	deviceTranslatedAddress	IPv4 Address		Identifies the translated device address that the event refers to in an IP network. The format is an

CEF Key Name	Full Name	Data Type	Length	Meaning
				IPv4 address. Example: “192.168.10.1”
dhost	destinationHostName	String	1023	Identifies the destination that an event refers to in an IP network. The format should be a fully qualified domain name (FQDN) associated with the destination node, when a node is available. Examples: “host.domain.com” or “host”.
dmac	destinationMacAddress	MAC Address		Six colon-seperated hexadecimal numbers. Example: “00:0D:60:AF:1B:61”
dntdom	destinationNtDomain	String	255	The Windows domain name of the destination address.
dpid	destinationProcessId	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.
dpriv	destinationUserPrivileges	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”.
dproc	destinationProcessName	String	1023	The name of the event’s destination process. Example: “telnetd” or “sshd”.
dpt	destinationPort	Integer		The valid port numbers are between 0 and 65535.
dst	destinationAddress	IPv4 Address		Identifies the destination address that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
dtz	deviceTimeZone	String	255	The timezone for the device generating the event.

CEF Key Name	Full Name	Data Type	Length	Meaning
duid	destinationUserId	String	1023	Identifies the destination user by ID. For example, in UNIX, the root user is generally associated with user ID 0.
duser	destinationUserName	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.
dvc	deviceAddress	IPv4 Address		Identifies the device address that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
dvchost	deviceHostName	String	100	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".
dvcmac	deviceMacAddress	MAC Address		Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
dvcpid	deviceProcessId	Integer		Provides the ID of the process on the device generating the event.
end	endTime	Time Stamp		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.
externalId	externalId	String	40	The ID used by an originating device. They are usually increasing numbers, associated with events.
fileCreateTime	fileCreateTime	Time Stamp		Time when the file was created.
fileHash	fileHash	String	255	Hash of a file.
fileId	fileId	String	1023	An ID associated with a file could be the inode.

CEF Key Name	Full Name	Data Type	Length	Meaning
fileModification Time	fileModificationTime	Time Stamp		Time when the file was last modified.
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
filePermission	filePermission	String	1023	Permissions of the file.
fileType	fileType	String	1023	Type of file (pipe, socket, etc.)
flexDate1	flexDate1	Time Stamp		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.
flexDate1Label	flexDate1Label	String	128	The label field is a string and describes the purpose of the flex field.
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.
flexString1 Label	flexString2Label	String	128	The label field is a string and describes the purpose of the flex field.
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

CEF Key Name	Full Name	Data Type	Length	Meaning
				be set by vendors unless necessary.
flex String2Label	flexString2Label	String	128	The label field is a string and describes the purpose of the flex field.
fname	filename	Stirng	1023	Name of the file only (without its path).
fsize	fileSize	Integer		Size of the file.
in	bytesIn	Integer		Number of bytes transferred inbound, relative to the source to destination relationship, meaning that data was flowing from source to destination.
msg	message	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.
oldFileCreate Time	oldFileCreateTime	Time Stamp		Time when old file was created.
oldFileHash	oldFileHash	String	255	Hash of the old file.
oldFileId	oldFileId	String	1023	An ID associated with the old file could be the inode.
oldFile Modification Time	oldFileModificationTime	Time Stamp		Time when old file was last modified.
oldFileName	oldFileName	String	1023	Name of the old file.
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
oldFile Permission	oldFilePermission	String	1023	Permissions of the old file.
oldFileSize	oldFileSize	Integer		Size of the old file.
oldFileType	oldFileType	String	1023	Type of the old file (pipe, socket, etc.)

CEF Key Name	Full Name	Data Type	Length	Meaning
out	bytesOut	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.
outcome	eventOutcome	String	63	Displays the outcome, usually as 'success' or 'failure'.
proto	transportProtocol	String	31	Identifies the Layer-4 protocol used. The possible values are protocols such as TCP or UDP.
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"
request	requestUrl	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"
requestClient Application	requestClientApplication	String	1023	The User-Agent associated with the request.
requestContext	requestContext	String	2048	Description of the content from which the request originated (for example, HTTP Referrer)
requestCookies	requestCookies	String	1023	Cookies associated with the request.
requestMethod	requestMethod	String	1023	The method used to access a URL. Possible values: "POST", "GET", etc.
rt	deviceReceiptTime	Time Stamp		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)
shost	sourceHostName	String	1023	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name (DQDN) associated with the source node, when a

CEF Key Name	Full Name	Data Type	Length	Meaning
				mode is available. Examples: “host” or “host.domain.com”.
smac	sourceMacAddress	MAC address		Six colon-separated hexadecimal numbers. Example: “00:0D:60:AF:1B:61”
sntdom	sourceNtDomain	String	255	The Windows domain name for the source address.
sourceDns Domain	sourceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).
source ServiceName	sourceServiceName	String	1023	The service that is responsible for generating this event.
source Translated Address	sourceTranslatedAddress	IPv4 Address		Identifies the translated source that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
source TranslatedPort	sourceTranslatedPort	Integer		A port number after being translated by, for example, a firewall. Valid port numbers are 0 to 65535.
spid	sourceProcessId	Integer		The ID of the source process associated with the event.
spriv	sourceUserPrivileges	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”.
sproc	sourceProcessName	String	1023	The name of the event’s source process.
spt	sourcePort	Integer		The valid port numbers are 0 to 65535.
src	sourceAddress	IPv4 Address		Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”.
start	startTime	Time Stamp		The time when the activity the event referred to started. The

CEF Key Name	Full Name	Data Type	Length	Meaning
				format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1st 1970)
suid	sourceUserId	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.
suser	sourceUserName	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.
type	type	Integer		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; using the full name to send an event will fail.

CEF Key Names For Event Consumers

CEF Key Name	Full Name	Data Type	Length	Meaning
agentDns Domain	agentDnsDomain	String	255	The DNS domain name of the ArcSight connector that processed the event.
agentNtDomain	agentNtDomain	String	255	
agentTranslated Address	agentTranslatedAddress	IP Address		
agentTranslated ZoneExternalID	agentTranslatedZone ExternalID	String	200	
agentTranslated Zone URI	agentTranslatedZoneURI	String	2048	

CEF Key Name	Full Name	Data Type	Length	Meaning
agentZone ExternalID	agentZoneExternalID	String	200	
agentZoneURI	agentZoneURI	String	2048	
agt	agentAddress	IP Address		The IP address of the ArcSight connector that processed the event.
ahost	agentHostName	String	1023	The hostname of the ArcSight connector that processed the event.
aid	agentId	String	40	The agent ID of the ArcSight connector that processed the event.
amac	agentMacAddress	MAC Address		The MAC address of the ArcSight connector that processed the event.
art	agentReceiptTime	Time Stamp		The time at which information about the event was received by the ArcSight connector.
at	agentType	String	63	The agent type of the ArcSight connector that processed the event
atz	agentTimeZone	String	255	The agent time zone of the ArcSight connector that processed the event.
av	agentVersion	String	31	The version of the ArcSight connector that processed the event.
customer ExternalID	customerExternalID	String	200	
customerURI	customerURI	String	2048	
destination TranslatedZone ExternalID	destinationTranslated ZoneExternalID	String	200	
destination Translated ZoneURI	destinationTranslated ZoneURI	String	2048	The URI for the Translated Zone that the destination asset has

CEF Key Name	Full Name	Data Type	Length	Meaning
				been assigned to in ArcSight.
destinationZone ExternalID	destinationZoneExternalID	String	200	
destinationZone URI	destinationZoneURI	String	2048	The URI for the Zone that the destination asset has been assigned to in ArcSight.
device TranslatedZone ExternalID	deviceTranslatedZone ExternalID	String	200	
device TranslatedZone URI	deviceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the device asset has been assigned to in ArcSight.
deviceZone ExternalID	deviceZoneExternalID	String	200	
deviceZoneURI	deviceZoneURI	String	2048	Thee URI for the Zone that the device asset has been assigned to in ArcSight.
dlat	destinationGeoLatitude	Double		The latitudinal value from which the destination's IP address belongs.
dlong	destinationGeoLongitude	Double		The longitudinal value from which the destination's IP address belongs.
eventId	eventId	Long		This is a unique ID that ArcSight assigns to each event.
rawEvent	rawEvent	String	4000	
slat	sourceGeoLatitude	Double		
slong	sourceGeoLongitude	Double		
source TranslatedZone ExternalID	sourceTranslatedZone ExternalID	String	200	

CEF Key Name	Full Name	Data Type	Length	Meaning
source TranslatedZone URI	sourceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
sourceZone ExternalID	sourceZoneExternalID	String	200	
sourceZoneURI	sourceZoneURI	String	2048	The URI for the Zone that the source asset has been assigned to in ArcSight.

Chapter 3: 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 and the label is not. If you want to set the label explicitly, the correct values are "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, use **c6a1**. Use “Device IPv6 Address” as the label, or let the connector code set the label for you.

source address, use **c6a2**. Use “SourceIPv6 Address” as the label, or let the connector code set the label for you.

destination address, use **c6a3**. Use “Destination IPv6 Address” as the label, or let the connector code set the label for you.

Chapter 4: 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 should cover most event log requirements. However, vendors' devices may generate more information than can be appropriately mapped into the predefined extensions or may 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

Note the following when creating custom extensions.

Format

Custom extension names should take the form `VendornameProductnameExplanatoryKeyName`

Requirements

Custom extension names should meet the following requirements. Custom extension nam(s):

- Must be made up of a single word, with no spaces.
- Must be alphanumeric
- Should be as clear and concise as possible.
- May not be named the same as 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 EXM

- Data submitted to ArcSight ESM using custom name extensions is retained; however, it 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.). Thus, 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; however, it 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/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, visit the SimpleDateFormat page at http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html .