ArcSight

Imperva
SecureSphere
January 3, 2018

IMPERVA®

CEF Connector Configuration Guide

Imperva SecureSphere

January 3, 2018

Revision History

Version	Date	Description
1.0	04/26/2009	First edition of this Configuration Guide.
2.0	07/26/2009	Certified and new cover page.
3.0	03/01/2011	Updated version numbers.
3.0	03/24/2011	Updated version numbers.
4.0	01/3/2018	Updated version numbers and logo on cover page.

SecureSphere Configuration Guide

This guide provides information for configuring Imperva SecureSphere appliances for syslog event collection. SecureSphere versions 6.2 through 8.5 are supported.

Overview

The integration of ArcSight into SecureSphere is based on the sending of syslog messages specially formatted with placeholders. These placeholders are used to define a syslog based event using the ArcSight Common Event Format.

Syslog Integration

Syslog is the most common and straightforward SecureSphere SIM/SEIM integration interface since all SIM/SIEM products incorporate syslog servers. The syslog interface can be applied to integrate SecureSphere security alerts and system events with those of other systems for event correlation, identification of blended threats, and recording of alerts to a centralized repository. Syslog is not recommended for full audit data integration as not all SecureSphere audit data is available via syslog and the volume of audit data often exceeds SIM/SIEM syslog data length limitations.

Common Event Format (CEF) Integration

The ArcSight Common Event Format (CEF) defines a syslog based event format to be used by other vendors. The CEF standard addresses the need to define core fields for event correlation for all vendors integrating with ArcSight.

SecureSphere versions 6.2 through 8.5 have the ability to integrate with ArcSight using the CEF standard. Administrators can set the system to send a syslog event when an alert or system event occurs. SecureSphere versions 6.2 through 8.5 can send syslog messages based on the CEF standard.

SecureSphere Placeholders

SecureSphere offers a list of placeholders to be used when syslog messages are sent. The placeholders provide detailed information about the security or system event occurred. The SecureSphere administrator has the ability to configure the entire syslog message. When integrating with Arcsight, the administrator configures the message based on the CEF standard.

Configuration

The following section describes how to set SecureSphere to send syslog messages, based on the CEF standard, when an alert or system event occurs. SecureSphere offers four different events, each requiring slightly different configuration. They include:

- Security Event
- Custom Security Event
- Firewall Security Event
- System Event

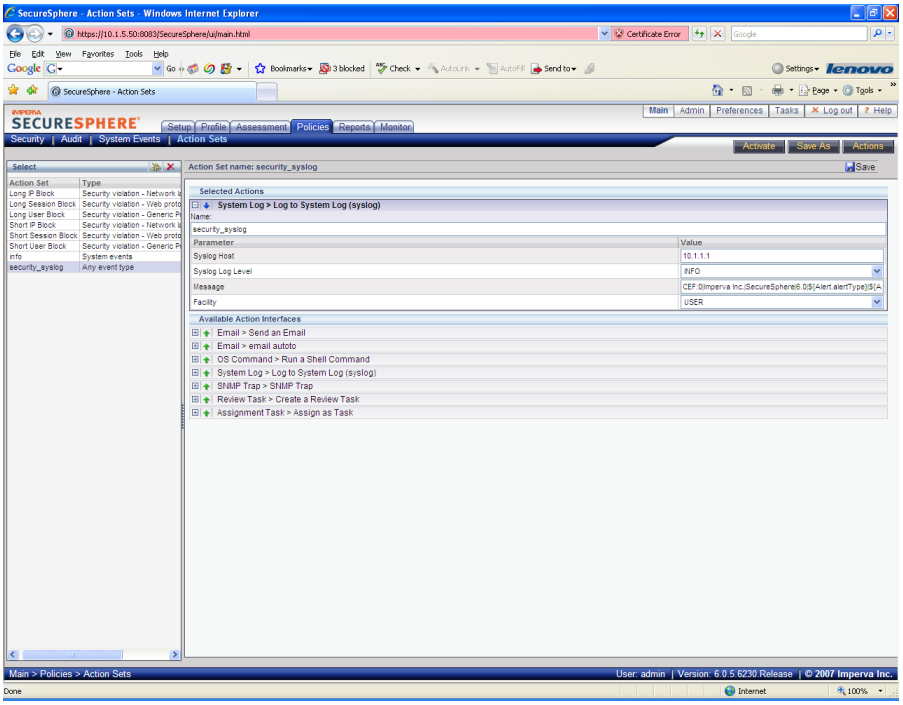
Configuring a Security Event

To set SecureSphere to send syslog messages based on the CEF standard when a security event occurs:

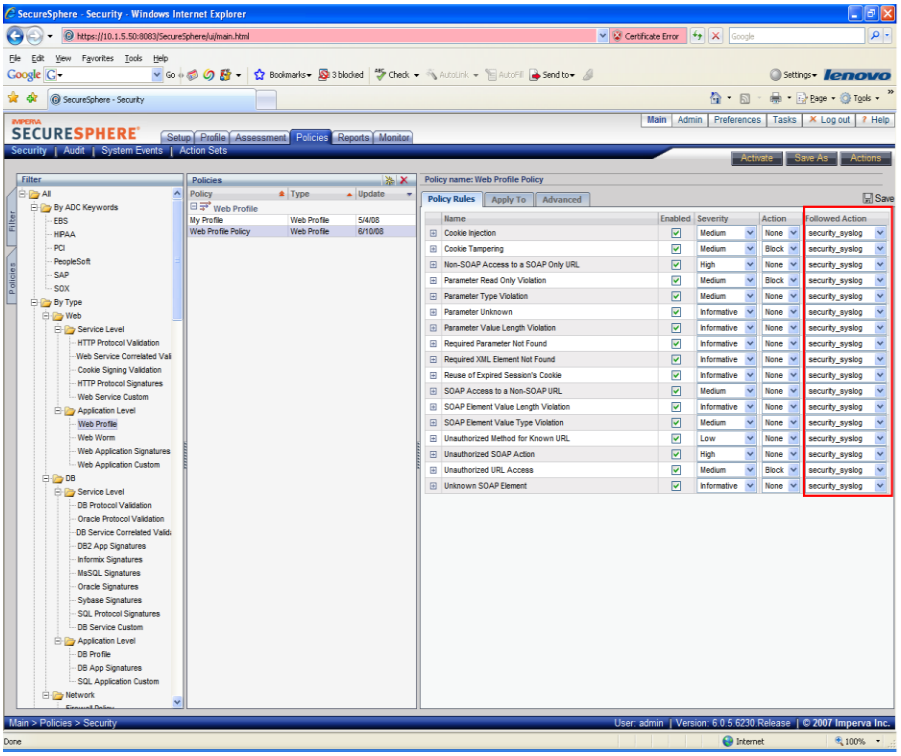
1. Define a new Action Set and configure the parameters as follows:
   a. **Name:** The action set name, for example, security_syslog.
   b. **Syslog Host:** The IP or host name of the Syslog server.
   c. **Syslog Log Level**: The Syslog log level.
   d. **Message**: The CEF message for a security event (alert).

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Alert.alertType}|${Alert.alertMetadata.alertName}|${Alert.severity}|act=${Alert.immediateAction}
dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort} duser=${Alert.username}
src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort} proto=${Event.sourceInfo.ipProtocol}
rt=#arcsightDate (${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy
cs2=${Alert.serverGroupName} cs2Label=ServerGroup cs3=${Alert.serviceName} cs3Label=ServiceName
cs4=${Alert.applicationName} cs4Label=ApplicationName cs5=${Alert.description} cs5Label=Description
```

2. **Facility**: The facility name that you want.



3 Set the security policies followed action that you want to send to Syslog when a violation occurs. Use the action set defined for security events in step 1.



4 When a security violation occurs, an alert is generated and a Syslog message is sent.

Configuring a Custom Policy Security Event

To set SecureSphere to send syslog messages based on the CEF standard when a custom policy event occurs:

1. Define a new Action Set and configure the parameters as follows:
   a. **Name**: The action set name, for example, custom_secutiy_syslog.
   b. **Syslog Host**: The IP or host name of the Syslog server.
   c. **Syslog Log Level**: The Syslog log level.
   d. **Message**: The CEF message for a custom policy security event (alert).

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Rule.parent.displayName}|${Rule.parent.displayName}|${Alert.severity}|act=${Alert.immediateAc
tion} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort} duser=${Alert.username}
src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort}
proto=${Event.sourceInfo.ipProtocol} rt=#arcsightDate
(${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy
cs2=${Alert.serverGroupName}
cs2Label=ServerGroup cs3=${Alert.serviceName} cs3Label=ServiceName
cs4=${Alert.applicationName} cs4Label=ApplicationName cs5=${Alert.description}
cs5Label=Description
```

   e. **Facility**: The facility name that you want.

2. Set the custom security policies followed action that you want to send to Syslog when a violation occurs. Use the action set defined for security events in step 1.

Configuring a Firewall Security Event

To set SecureSphere to send syslog messages based on the CEF standard when a firewall security event occurs:

1. Define a new Action Set and configure the parameters as follows:
   a. **Name**: The action set name, for example, firewall_secutiy_syslog.
   b. **Syslog Host: The IP or host name of the Syslog server.**
   c. **Syslog Log Level: The Syslog log level.**

d **Message:** The CEF message for a custom policy security event (alert).

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Alert.alertType}|${Alert.alertMetadata.alertName}|${Alert.severity}|act=${Alert.immediateAction}
dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort} duser=${Alert.username}
src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort}
proto=${Event.sourceInfo.ipProtocol} rt=#arcsightDate (${Alert.createTime}) cat=Alert
cs1=${Rule.parent.displayName} cs1Label=Policy cs2=${Alert.serverGroupName}
cs2Label=ServerGroup cs3=${Alert.description} cs3Label=Description
```

e **Facility**: The facility name that you want.

2 Set the firewall security policies followed action that you want to send to Syslog when a violation occurs. Use the action set defined for security events in step 1.

Configuring a System Event

To set SecureSphere to send syslog messages based on the CEF standard when a system event occurs:

1 Define a new Action Set and configure the parameters as follows:

a **Name**: The action set name, for example, system_syslog.

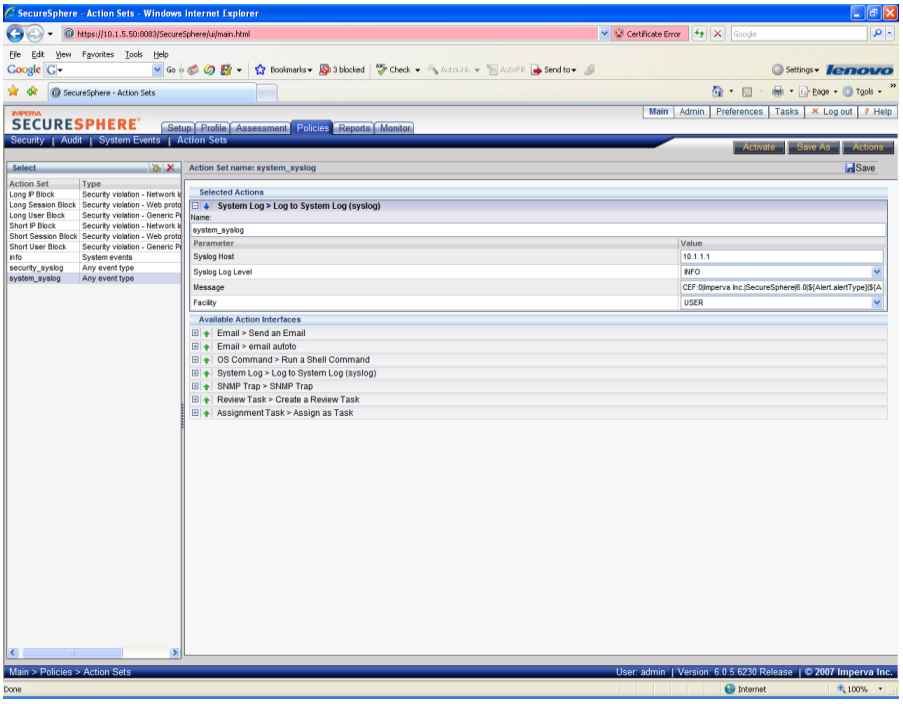
b **Syslog Host**: The IP or host name of the Syslog server.

c **Syslog Log Level**: The Syslog log level.

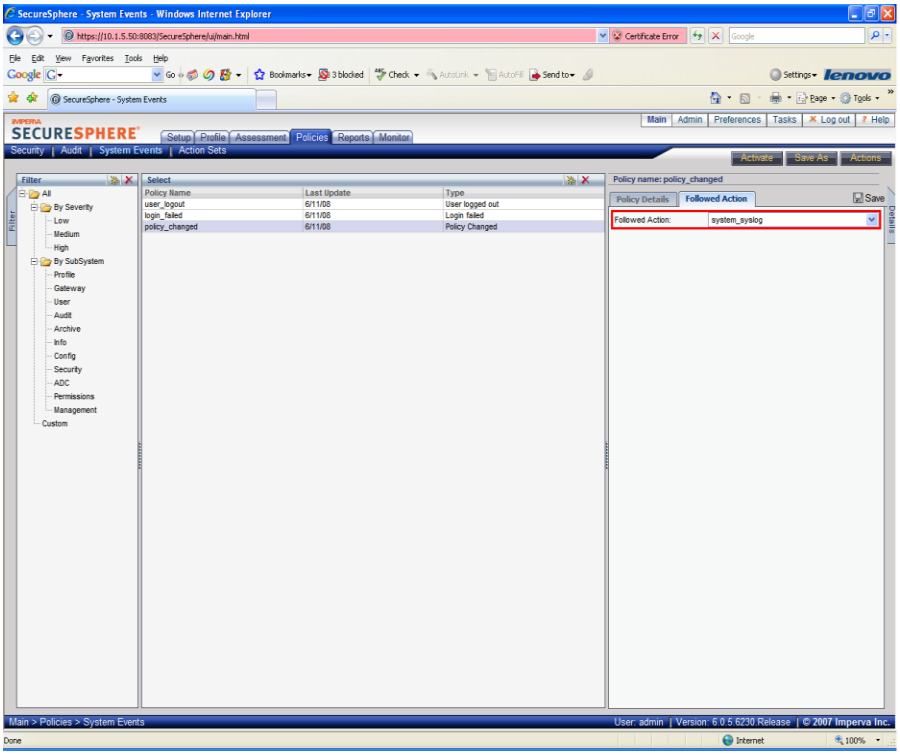
d **Message**: The CEF message for a system event.

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Event.eventType}|${Event.message}|${Event.severity.displayName}| suser=${Event.username}
rt=# (${Event.createTime}) cat=SystemEvent
```

2 **Facility**: The facility name that you want.



3 Create the system event policy and set the followed action to send a Syslog message when the event occurs. Use the action set defined for system events in step 1.



4 When the system event occurs, a Syslog message is sent.

Syslog Messages in SecureSphere

The format of the syslog message should be as follows:

CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|deviceEventClassId|Name|Severity|Extension

Example Messages in SecureSphere

SecureSphere supports four types of Syslog Messages that integrate with Arcsight. These include:

- Security Event
- Custom Security Event
- Firewall Security Event
- System Event

Example Security Event

Security events indicate that a security policy violation has taken place. The following is an example of syntax used to build a syslog message for reporting a regular security event to ArcSight.

CEF:0|Imperva Inc.|SecureSphere|*[SecureSphere version #]*
|${Alert.alertType}|${Alert.alertMetadata.alertName}|${Alert.severity}
|act=${Alert.immediateAction} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort}
duser=${Alert.username}
src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort} proto=${Event.sourceInfo.ipProtocol}
rt=#arcsightDate
(${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy cs2=${Alert.serverGroupName}
cs2Label=ServerGroup cs3=${Alert.serviceName} cs3Label=ServiceName cs4=${Alert.applicationName}
cs4Label=ApplicationName
cs5=${Alert.description} cs5Label=Description

Example Custom Security Event

Security events indicate that a security policy violation has taken place. The following is an example of syntax used to build a syslog message for reporting a custom security event to ArcSight.

CEF:0|Imperva Inc.|SecureSphere|*[SecureSphere version #]*
|${Rule.parent.displayName}|${Rule.parent.displayName}|${Alert.severity}
|act=${Alert.immediateAction} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort}
duser=${Alert.username} src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort}
proto=${Event.sourceInfo.ipProtocol} rt=#arcsightDate${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName}
cs1Label=Policy cs2=${Alert.serverGroupName} cs2Label=ServerGroup cs3=${Alert.serviceName} cs3Label=ServiceName
cs4=${Alert.applicationName} cs4Label=ApplicationName cs5=${Alert.description} cs5Label=Description

Example Firewall Security Event

Firewall Security events indicate a Firewall related issue has occurred. The following is an example of syntax used to build a syslog message for reporting a firewall event to ArcSight.

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Alert.alertType}|${Alert.alertMetadata.alertName}|${Alert.severity}
|act=${Alert.immediateAction} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort}
duser=${Alert.username}
src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort} proto=${Event.sourceInfo.ipProtocol}
rt=#arcsightDate
(${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy cs2=${Alert.serverGroupName}
cs2Label=ServerGroup cs3=${Alert.description} cs3Label=Description
```

Example System Event

System events indicate a system related issue has occurred. The following is an example of syntax used to build a syslog message for reporting a system event to ArcSight.

```
CEF:0|Imperva Inc.|SecureSphere|[SecureSphere version #]
|${Event.eventType}|${Event.message}|${Event.severity.displayName}|suser=${Event.username}
rt=#arcsightDate(${Event.createTime}) cat=SystemEvent
```

Screen Shot

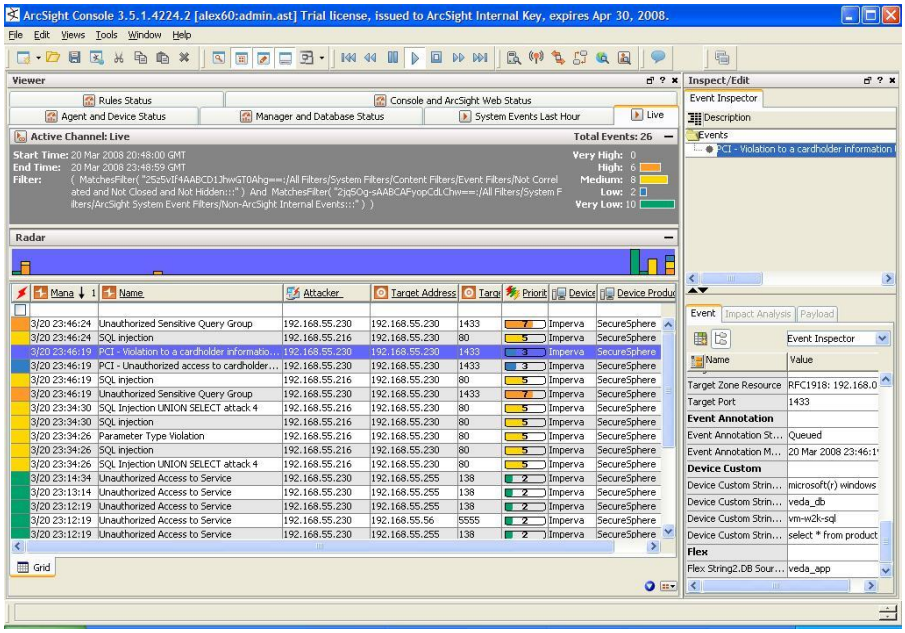


Figure 1: ArcSight Console showing SecureSphere V6 Alert

Events

CEF fields are added in the message field of System Log properties. These fields are used to create a syslog message that can be read by ArcSoft. There are two categories of CEF fields that can be used in syslog messages:

- Standard Fields
- Extended Fields

Standard Event Fields

The following are the supported CEF standard event fields and the corresponding values to configure in SecureSphere:

CEF Field Name	Version
CEF Definition	Version is an integer that identifies the version of the CEF format. Event consumers use this information to determine the following fields. Currently only version 0 (zero) is established in the CEF format. The other fields might need to be added to the "prefix" and therefore require a version number change. Adding new formats is handled through the standards body.
Configuration in SecureSphere	0
SecureSphere Definition	N/R

CEF Field Name	DeviceVendor
CEF Definition	Device Vendor, Device Product, and Device Version are strings that uniquely identify the type of device that sends events. Two products cannot use the same device-vendor and device product pair. There is no central authority managing these pairs. Event producers have to ensure that they assign a unique name to each pair.
Configuration in SecureSphere	Imperva Inc.
SecureSphere Definition	Company Name

CEF Field Name	DeviceProduct
CEF Definition	Device Vendor, Device Product, and Device Version are strings that uniquely identify the type of device that sends events. Two products cannot use the same device-vendor and device product pair. There is no central authority managing these pairs. Event producers have to ensure that they assign a unique name to each pair.
Configuration in SecureSphere	SecureSphere
SecureSphere Definition	Product Name

CEF Field Name	DeviceVersion
CEF Definition	Device Vendor, Device Product and Device Version are strings that identify the type of device that sends events. Two products cannot use the same device-vendor and device product pair. There is no central authority managing these pairs. Event producers have to ensure that they assign a unique name to each pair.
Configuration in SecureSphere	Versions 6.2 through 8.5
SecureSphere Definition	Product Version

CEF Field Name	deviceEventClassId
CEF Definition	DeviceEventClassId is a unique identifier for each event type. This can be a string or an integer. DeviceEventClassId represents the type of event reported. In the intrusion detection system (IDS) world, each signature or rule that detects certain activity has a unique deviceEventClassId assigned. This is a requirement for other types of devices as well, and helps correlation engines deal with the events.
Configuration in SecureSphere	${Alert.alertType} for security alerts other than custom policy alerts ${Rule.parent.displayName} for custom policy security alerts ${Event.eventType} for system events
SecureSphere Definition	${Alert.alertType} is the alert type (firewall, signature, protocol, profile, or correlation) ${Rule.parent.displayName} is the name of the custom policy ${Event.eventType} is the type of system event

CEF Field Name	Name
CEF Definition	Name is a string that represents 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. The name should be: "Port scan". The rest of information is redundant and can be picked up from the other fields.
Configuration in SecureSphere	${Alert.alertMetadata.alertName} for security alerts other than custom policy alerts ${Rule.parent.displayName} for custom policy security alerts ${Event.message} for system events
SecureSphere Definition	${Alert.alertMetadata.alertName} is the alert name ${Event.message} is the message of the event$ {Rule.parent.displayName} is the name of the custom policy

CEF Field Name	Severity
CEF Definition as appears in CEF documentation	Severity reflects the importance of the event.
Configuration in SecureSphere	${Alert. severity} for alerts ${Event.severity.displayName} for system events
SecureSphere Definition	${Alert.severity} is the severity of the alert in text format: Low, Medium, High. ${Event.severity.displayName} is the severity of the event in text format: Low, Medium, High. Severity should not be set to Informative when CEF is used. Use Low instead.

CEF Field Name	Extension
CEF Definition as appears in CEF documentation	Extension is a collection of key-value pairs. Each key is a part of a predefined set. The standard allows including additional keys as outlined later. An event can contain any number of key-value pairs in any order separated by spaces (" "). A field can include spaces, i.e. in case of file name.
Configuration in SecureSphere	Security Event (Alert): act=${Alert.immediateAction} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort} duser=${Alert.username} src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort} proto=${Event.sourceInfo.ipProtocol} rt=#arcsightDate (${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy cs2=${Alert.serverGroupName} cs2Label=ServerGroup cs3=${Alert.serviceName} cs3Label=ServiceName cs4=${Alert.applicationName} cs4Label=ApplicationName cs5=${Alert.description} cs5Label=Description Firewall Event (Alert): act=${Alert.immediateAction} dst=${Event.destInfo.serverIp} dpt=${Event.destInfo.serverPort} duser=${Alert.username} src=${Event.sourceInfo.sourceIp} spt=${Event.sourceInfo.sourcePort} proto=${Event.sourceInfo.ipProtocol} rt=#arcsightDate (${Alert.createTime}) cat=Alert cs1=${Rule.parent.displayName} cs1Label=Policy cs2=${Alert.serverGroupName} cs2Label=ServerGroup cs3=${Alert.description} cs3Label=Description System Event: User: ${Event.username} Creation Time: #arcsightDate (${Event.createTime}) cat=SystemEvent
SecureSphere Definition	The definition of each placeholder is listed under the Extension Field Dictionary.

Extended Event Fields

The extension field provides the ability to use the CEF key-value pairs for additional information on the event. The following table details a CEF key and its corresponding SecureSphere placeholder:

CEF Key	deviceFacility
CEF Definition	The facility generating the event.
SecureSphere Placeholder	N/R
SecureSphere Definition	Choose the desired facility.
SecureSphere Event Type	All events

CEF Key	act
CEF Definition	Action mentioned in the event.
SecureSphere Placeholder	${Alert.immediateAction}
SecureSphere Definition	The immediate action performed, either block transaction (event) or no action.
SecureSphere Event Type	Security event.

CEF Key	dst
CEF Definition	Identifies destination an event refers to in an IP network in IPv4 format. For example: "192.168.10.1".
SecureSphere Placeholder	${Event.destInfo.serverIp}
SecureSphere Definition	The destination IP address.
SecureSphere Event Type	Security events.

CEF Key	dpt
CEF Definition	The valid port numbers are between 0 and 65535.
SecureSphere Placeholder	${Event.destInfo.serverPort}
SecureSphere Definition	The destination port.
SecureSphere Event Type	Security events.

CEF Key	duser
CEF Definition	Identifies the destination user by name. This parameter represents the user associated with event's destination.
SecureSphere Placeholder	${Alert.username}
SecureSphere Definition	The destination user. In web applications it refers to the application user logged into the application. In database applications it refers to the database user.
SecureSphere Event Type	Security events.

CEF Key	src
CEF Definition	Identifies source an event refers to in an IP network in IPv4 format. For example: "192.168.10.1".
SecureSphere Placeholder	${Event.sourceInfo.sourceIp}
SecureSphere Definition	The source IP address.
SecureSphere Event Type	Security events.

CEF Key	spt
CEF Definition	The valid port numbers are between 0 and 65535.
SecureSphere Placeholder	${Event.sourceInfo.sourcePort}
SecureSphere Definition	The source port.
SecureSphere Event Type	Security events.

CEF Key	Proto
CEF Definition	Identifies the Layer-4 protocol used. The possible values are protocol names, i.e. TCP or UDP.
SecureSphere Placeholder	${Event.sourceInfo.ipProtocol}
SecureSphere Definition	The protocol used.
SecureSphere Event Type	Security events.

CEF Key	Rt
CEF Definition	The time when the activity of the event referred to started. The format is MMM dd yyyy HH:mm:ss.
SecureSphere Placeholder	$dateTool.format('date.arcsight',${Alert.createTime})
SecureSphere Definition	The alert time.
SecureSphere Event Type	Security events.

CEF Key	Cat
CEF Definition	Represents the category assigned to the originating device. Usually devices use their own categorization schema to classify events.
SecureSphere Placeholder	Alert
SecureSphere Definition	The type of the event.
SecureSphere Event Type	Security events.

CEF Key	cs1
CEF Definition	Custom field is used to map fields that do not fit into any other field available in the CEF dictionary.
SecureSphere Placeholder	${Rule.parent.displayName}
SecureSphere Definition	The violated policy's name.
SecureSphere Event Type	Security events.

CEF Key	cs2
CEF Definition	Custom field is used to map fields that do not fit into any other field available in the CEF dictionary.
SecureSphere Placeholder	${Alert.serverGroupName}
SecureSphere Definition	The server group name.
SecureSphere Event Type	Security events.

CEF Key	cs3
CEF Definition	Custom field is used to map fields that do not fit into any other field available in the CEF dictionary.
SecureSphere Placeholder	For Firewall events: ${Alert.description} For other security events: ${Alert.serviceName}
SecureSphere Definition	${Alert.description} is the alert description ${Alert.applicationName} is the service name.
SecureSphere Event Type	Security events.

CEF Key	cs4
CEF Definition	Custom field is used to map fields that do not fit into any other field available in the CEF dictionary.
SecureSphere Placeholder	For non firewall security events: ${Alert.applicationName}
SecureSphere Definition	${Alert.applicationName} is the application name.
SecureSphere Event Type	Security events.

CEF Key	cs5
CEF Definition	Custom field is used to map fields that do not fit into any other field available in the CEF dictionary.
SecureSphere Placeholder	For non firewall security events: ${Alert.description}
SecureSphere Definition	${Alert.description} is the alert description
SecureSphere Event Type	Security events.

CEF Key	cs1Label
CEF Definition	All custom fields have a corresponding label field for the description of the field.
SecureSphere Placeholder	Policy.
SecureSphere Definition	Policy label.
SecureSphere Event Type	Security events.

CEF Key	cs2Label
CEF Definition	All custom fields have a corresponding label field for the description of the field.
SecureSphere Placeholder	ServerGroup.
SecureSphere Definition	ServerGroup Label.
SecureSphere Event Type	Security events.

CEF Key	cs3Label
CEF Definition	All custom fields have a corresponding label field for the description of the field.
SecureSphere Placeholder	For non Firewall alerts Service. For Firewall Alerts: Description
SecureSphere Definition	Application is Service Label. Description is Description Label
SecureSphere Event Type	Security events.

CEF Key	cs4Label
CEF Definition	All custom fields have a corresponding label field for the description of the field.
SecureSphere Placeholder	For non Firewall alerts Application.
SecureSphere Definition	Application is Service Label.
SecureSphere Event Type	Security events.

CEF Key	cs5Label
CEF Definition	All custom fields have a corresponding label field for the description of the field.
SecureSphere Placeholder	For non Firewall alerts Description
SecureSphere Definition	Description is Description Label
SecureSphere Event Type	Security events.

CEF Key	Suser
CEF Definition	Identifies the source user by name. This field represents the user associated with the event's source.
SecureSphere Placeholder	${Event.username}
SecureSphere Definition	The system user who caused the event. It can be specific user who logged into the system or a system user.
SecureSphere Event Type	System events.

CEF Key	cat
CEF Definition	Represents the category assigned to the originating device. Usually devices use their own categorization schema to classify events.
SecureSphere Placeholder	System Event.
SecureSphere Definition	The type of the event.
SecureSphere Event Type	System events.

CEF Key	rt
CEF Definition	The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss.
SecureSphere Placeholder	$dateTool.formatToArcsight(${Event.createTime})
SecureSphere Definition	The system event time.
SecureSphere Event Type	System events.

Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

Imperva SecureSphere Connector Field Mappings

Vendor-Specific Event Definition	ArcSight Event Data Field

Vendor-Specific Event Definition	ArcSight Event Data Field