opentext™

ArcSight SmartConnectors

Software Version: 8.4.3

ArcSight CEF for Cloud Implementation Standard

Document Release Date: October 2023
Software Release Date: October 2023

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

ArcSight Common Event Format for Cloud Implementation Standard

The Common Event Format (CEF) Standard, developed by ArcSight, lets vendors and their customers quickly integrate their product information into ESM. CEF is an open log management standard that simplifies log management, letting third parties 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, which can be analyzed later by an enterprise management system.

To know more about the CEF protocol, to see a list of CEF mappings as well as supported date formats, and to understand how to implement the standard, see ArcSight Common Event Format Implementation Standard. It details the header and predefined extensions used within the standard as well as how to create user defined extensions.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- Technical Requirements Guide for SmartConnector, which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- Installation and User Guide for SmartConnectors, which provides detailed information about installing SmartConnectors.
- Configuration Guides for ArcSight SmartConnectors, which provides information about configuring SmartConnectors to collect events from different sources.
- Configuration Guide for SmartConnector Load Balancer, which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors 8.4.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, contact Open Text Support for Micro Focus products.

Overview

The ArcSight CEF for Cloud Implementation Standard specifies the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

ArcSight SmartConnector technology addresses the core challenge of log collection by providing an effective and highly scalable infrastructure to simplify and optimize the aggregation and normalization of logs across thousands of devices and hundreds of locations.

Historically, ArcSight connectors were designed to run within an enterprise IT environment using a syslog-based standard, with all devices contained on the customer premises. Increasingly, enterprises around the world are adopting cloud-based services that have different characteristics and requirements than on premise devices and applications.

The ArcSight Cloud CEF Implementation Standard addresses these challenges by specifying the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

Challenges in Cloud Event Collection

Enabling log event collection between a cloud service provider and a customer running ArcSight security products differs significantly from traditional log collection processes. These differences include:

• **Network architecture:** The architecture of cloud technologies differs from the network architecture on which traditional ArcSight devices operate.

• **Event generation:** Security events generated by devices in the cloud differ from events generated by traditional security devices in content, format, and transport mechanism.

• **Security:** Log collection for cloud-based services involves securely importing events from outside to inside the customer's environment.

• **Scalability:** Each cloud application changes rapidly and the volume continues to grow, making it challenging to keep current with traditional log collection processes.

To address these differences, ArcSight has developed standards for:

• Event retrieval from cloud vendors that can be re-used across many different types of cloud service providers.

• Use of standard HTTPS for security and support of strong authentication and access control.

• The overall transport format for a retrieved batch of events using JSON.

• Common format for event content called ArcSight CEF.

Supported Industry Standards

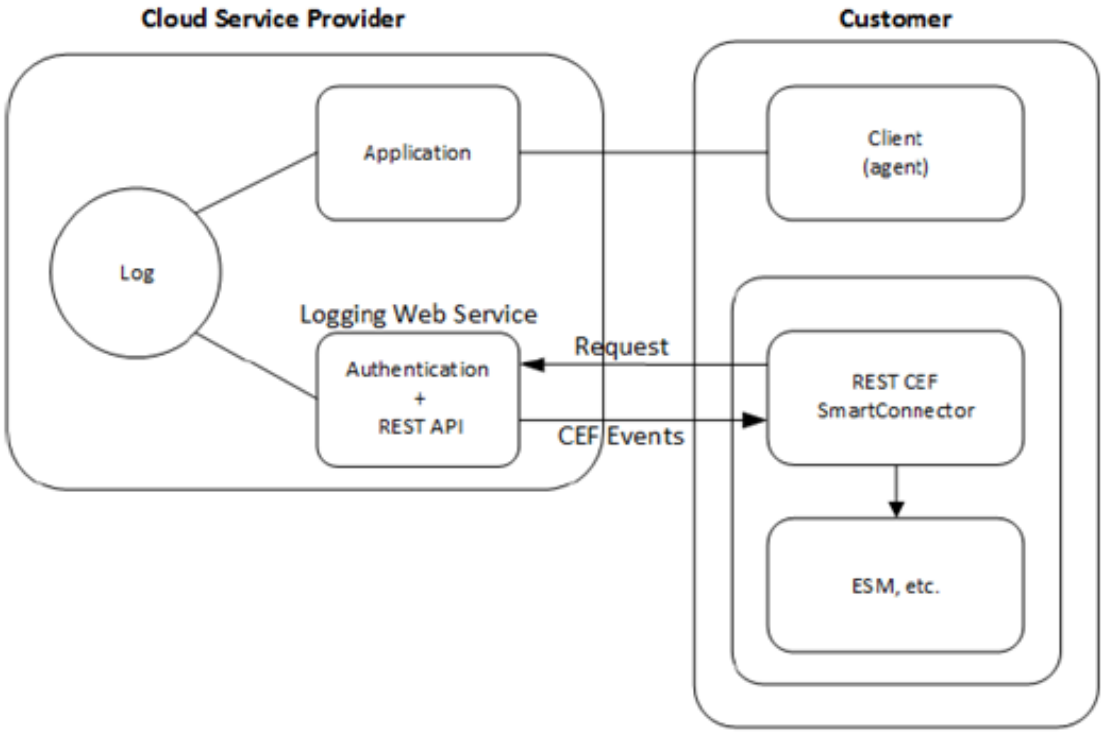
The Cloud CEF Implementation Standard supports the following industry standards:

- REST Web Service APIs
- OAuth 2.0 or Basic authentication
- JSON event transport format
- ArcSight Common Event Format

The ArcSight Cloud CEF Implementation Standard provides the development toolkit to integrate with the cloud service providers using these standards.

ArcSight CEF for the Cloud

The SmartConnector for ArcSight Common Event Format for REST is the device that customers of ArcSight and the cloud-based service provider will use to retrieve events. This is based on the following model:



Cloud service provider customers (“Client” in the diagram) interact with applications typically using a web browser or other user interface. The cloud-based application creates log entries as a by-product of these interactions. The particular log entries are application dependent.

The cloud service provider must provide a logging web service component. The logging web service retrieves the log entries and includes a REST API, support for authentication, and ArcSight Cloud CEF as the event format.

As an open log management standard, Cloud CEF improves the interoperability of security-related information by reducing various message syntaxes to one matching the ArcSight schema. This API must use ArcSight Cloud CEF as the event format.

There are three main elements to the Cloud CEF solution:

1. The REST CEF SmartConnector retrieves events through a REST API exposed by the cloud service provider.
2. Events are retrieved in ArcSight CEF format and transported over HTTPS (which may require an access token).
3. Retrieved events are sent to ArcSight products such as ArcSight Enterprise Security Manager (ESM).

SmartConnector for ArcSight Common Event Format REST

The SmartConnector for ArcSight Common Event Format REST lets customers configure an authentication method and the REST API URLs for event retrieval. The connector is typically located on customer premises, although it can be run on the service provider platform, where it attempts to retrieve the latest events as reported by the cloud service provider REST APIs.

The Cloud CEF Implementation Standard mandates that the cloud service provider adhere to the following conditions for authentication and event retrieval, by implementing an authentication mechanism and event retrieval APIs:

Authentication

Authentication is generally required to gain access to the cloud server containing the event data. Each cloud service provider defines the authentication method used for its servers. The REST CEF SmartConnector provides flexible authentication support. Initially the two authentication methods supported are OAuth 2.0 and Basic authentication. The REST CEF SmartConnector user chooses the authentication method at connector installation time based on the capabilities of the cloud service provider.

OAuth 2.0 Authentication: The OAuth 2.0 standard is defined by IETF RFC 649. With OAuth 2.0, a third party application (in this case, the REST CEF SmartConnector) can be allowed access to server resources without disclosing the credentials of the resource owner.

To achieve this, the cloud service provider implementation of OAuth 2.0 must support:

- Callback URLs for the local host, so that the connector can access the authentication code and complete the OAuth authentication.
- HTTPS for local host URLs

  For example, https://localhost:8080/oauth2callback is an example of a supported callback URL, known as a redirect_uri in the OAuth 2.0 specification.
- Provisions for maintaining a valid refresh token without human intervention. If refresh tokens are used, there must be a mechanism for automatically extending the refresh token expiration date.

  For example, if the refresh token is initially valid for 14 days and is used to acquire a new access token, the expiration date is extended for 14 more days.

Basic Authentication: In Basic authentication, the client provides an identifier (a username) and a shared secret (a password). Basic authentication is defined by RFC 2617. This authentication method uses TLS protocol, in which both the identifier and shared secret are encrypted. A client certificate might also be required by the vendor to verify the client's identity.

Event Retrieval APIs

The REST CEF SmartConnector retrieves events using REST API calls over secure transport (HTTPS). It expects CEF events in JSON format.

The API endpoint URL is comprised of several elements:

- The base URL
- The CEF events endpoint
- One or more event query arguments

Each of these elements are described in the following sections.

Base URL

The API endpoint base URL is specific to the cloud service provider, and includes the host name and path designation.

The base URL can be static or dynamic, although static URLs are recommended. If Dynamic URLs are used, the vendor must provide the means to get the dynamic portion of the URLs.

- Static URLs, such as https://api.abc.com/1.0/auditEvents, are the same for any user.
- Dynamic URLs, such as https://<SomeUserSpecificValue>.api.abc.com/1.0/auditEvents, include a value (<SomeUserSpecificValue> in this example) derived from the authenticated user using OAuth.

CEF Events Endpoint

The CEF events component of the path denotes a service that conforms to the REST CEF SmartConnector standard.

For example, a base URL of https://www.acmeapis.com/admin/reports contains the hostname www.acmeapis.com, and the path specification /admin/reports.

When combined with the cef-events endpoint, the event retrieval URL becomes:

https://www.acmeapis.com/admin/reports/cef-events

Event Query Arguments

The following query parameters are defined:

• startTime=<timestamp>

where <timestamp> follows the form yyyy-MM-dd'T'HH:mm:ss.SSSZ.

Example: 2012-05-15T00:01:02.345-08:00

The timestamp components after yyyy-MM-dd'T'HH:mm:ss are optional. The time zone designator is Z or +hh:mm or -hh:mm. If the startTime is not specified, events are retrieved beginning with the earliest available event.

• maxResults=<number>

where <number> is an integer. This specifies that nomore than <number> events should be returned in the response. If maxResults is not specified, the number of events produced is determined by the cloud service provider.

• eventType=<event type list>

The <event type list> is a comma-separated list of the event types to retrieve. The individual event type names are specific to the cloud service provider. If eventType is not specified, events of all types are retrieved.

The REST CEF SmartConnector periodically requests new events from the server. The polling period has a default value of 30 seconds, which is user-configurable. If a request to the server for events produces some events, the connector immediately makes another request using the continuation capability. This process continues until a request for events produces no events, after which the connector reverts to the configured polling period.

Retrieved Response Format

The server returns the response in an HTML document. The content type is application/JSON, as defined by RFC 4627. Contained within the document is a collection of CEF-formatted event data. The document content is formatted as follows:

```
{
"format" : "cef",
"version" : "1.0",
"timestamp" : <timestamp in standard format>,"count" : <number>,
"events" :[
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]",
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]",
.
"CEF:Version|Device Vendor|Device Product|Device
Version|SignatureID|Name|Severity|[Extension]"
],
"links" : [
{
"rel": "next",
"href": URL
}
]
```

Continuation

When the connector starts up, it makes a first request to the server using the Events URL provided in the setup configuration to get the first set of events, and uses the URL contained in the “links” array of the response for each subsequent request.

Whenever the server has more events than can be contained in a single response, the connector immediately makes additional requests to retrieve more events using the URL from links array contained in the response. If there are no events in the response, the connector waits for the configured polling period to retrieve more events using the URL from the links array contained in the response.

CEF Mappings

The ArcSight Common Event Format is defined in ArcSight Common Event Format Implementation Standard. Cloud service providers must use this document to map native event fields to the appropriate CEF key value.

Summary

If a cloud service provider supports OAuth 2.0 or Basic authentication, and exposes REST APIs for event retrieval in ArcSight CEF (over JSON) format, ArcSight and cloud service providers customers can monitor their applications on the service provider's cloud platform.

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 ArcSight CEF for Cloud Implementation Standard (SmartConnectors 8.4.3)

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!