Common Event Format Configuration Guide

CloudPassage

Halo 1.0

Date: Tuesday, August 06, 2013

CEF Connector Configuration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HP. HP does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified CEF:

The event format complies with the requirements of the HP ArcSight Common Event Format. The HP ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HP's ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

Halo Event Connector v. 1.0

July 12, 2013

Revision History

Date	Description
07/12/2013	First edition of this Configuration Guide.
08/06/2013	Version 1.0 Certified by HP Enterprise Security

CEF Connector Support Information when an issue is outside of the ArcSight team's ability

In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

Customer Support: support.cloudpassage.com

Phone - Customers who have upgraded to premium versions of CloudPassage may obtain email and/or telephone support by opening support tickets in the CloudPassage Portal.

Email - Customers who have upgraded to premium versions of CloudPassage may obtain email and/or telephone support by opening support tickets in the CloudPassage Portal.

Instructions - If you have questions regarding CloudPassage Halo functionalities or you need to report bugs, please visit the CloudPassage Community Support site.

Halo Event Connector Configuration Guide

This guide provides information for configuring the Halo Event Connector for syslog event collection. This Connector is supported on Windows Server 2008/2012, Linux and Mac OSX platforms. Device version 1.0 is supported.

Overview

The purpose of the Halo Event Connector is to retrieve event data from a CloudPassage Halo account and import it into an external tool—such as HP ArcSight—for indexing or processing. The Connector is a Python script that is designed to execute repeatedly, keeping the external tool up-to-date with Halo events as time passes and new events occur:

- The first time the Connector runs, it by default retrieves all logged events from a single Halo account. Then the Connector creates a file, writes the timestamp of the last-retrieved event in it, and saves it in the current directory. However:
  - You can specify up to five Halo accounts to extract events from simultaneously.
  - Instead of retrieving all events when the script runs the first time, you can retrieve only events after a certain point by using the **--starting=*datetime*** command-line option.
  - You can store the timestamp in a directory of your choice by specifying it in the **--configdir=*dirname*** command-line option.
- Every subsequent time it runs, the Connector retrieves only those events that were created after the timestamp stored in the file. At the end of the run, the script updates the file with the timestamp of the last-retrieved event during that run.

  Note: The **--starting=*datetime*** option applies only the first time that you run the script. Each subsequent execution starts from the timestamp of the last-retrieved event.
- During any script run, if no new events have occurred since the last run, no events are retrieved or imported into the external tool.

Configuration

This section describes the CloudPassage Halo Event Connector and explains how you can configure the connector to import Halo event data into HP's ArcSight SIEM tool.

Prerequisites

To get started, you must have the following privileges and software resources:

- An active CloudPassage Halo subscription. If you don't have one, Register for CloudPassage to receive your credentials and further instructions by email.
- Access to your CloudPassage API key. Best practice is to create a new read-only key specifically for use with this script.
- Python 2.6 or later. You can download Python from here.
- Access to HP's ArcSight SIEM tool. You can read more about HP ArcSight here.
- The Event Connector script (haloEvents.py) and its associated files.

***Note**:* The Event Connector makes calls to the CloudPassage Events API, which is available to all Halo subscribers at all levels (including Basic). Many other parts of the CloudPassage API are available only to Halo users with a NetSec or

Professional subscription; if you want to use those parts of the API, you can upgrade your subscription on the Manage Subscription page of the Halo Portal.

Setup your syslog server to forward Halo events to the ArcSight server

See which logger your system uses by running the following command:

*ls –d /etc/*syslog**

You will most likely see one of the following files listed:

- rsyslog.conf
- syslog-ng.conf
- syslog.conf

Edit the appropriate file with relevant information for your environment. For example, we use syslog-ng in our environment so we edited the syslog-ng.conf file and added the following lines to the end of the file:

```
destination d_arcsight {
  udp("hostname" port(1514));
};
log {
  source(s_src); destination(d_arcsight);
};
```

Setup and run the Halo Event Connector to stream events from Halo to HP's ArcSight

Command line arguments. In Python, you execute the Connector script with a command like this:

$ haloEvents.py *–cefsyslog –starting=2013-01-01*

This will stream Halo events in native ArcSight CEF format to your syslog daemon.

To view the set of supported command-line arguments, launch the script with the argument -? or -h to view the usage page.

Authentication to the Halo API. Halo requires the Connector to pass both the key ID and secret key values for a valid Halo API key in order to obtain the event data. You pass those values in a file named by default haloEvents.auth, located in the same directory as haloEvents.py and its associated script files. The format for the file is described in Section A.

Alternatively, you can pass those values in a different file by specifying the full path to the file in the **--auth=*filename*** option.

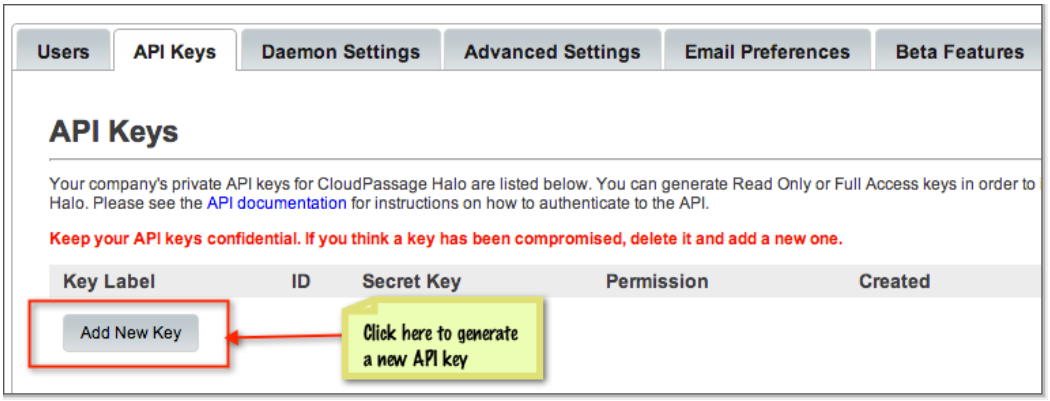
Output to a file. Whenever it writes event data to a disk file, the Connector appends the new data to the end of any existing data in the file.

Platform support. The Event Connector runs on Linux, Windows and Mac OSX operating systems.

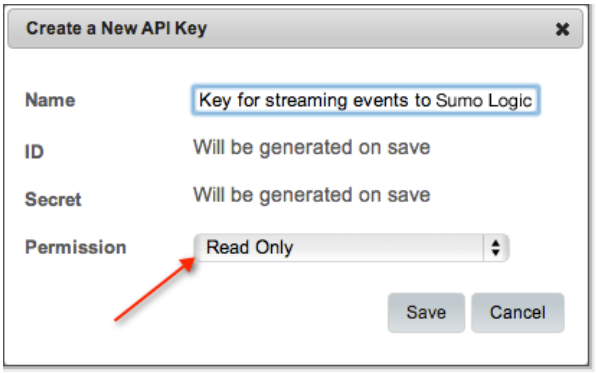
A. Retrieve and Save your CloudPassage API Key

The Connector retrieves events from your CloudPassage Halo account by making calls to the CloudPassage API. The API requires the script to authenticate itself during every session; therefore, you need to make your CloudPassage API Key available to the script.

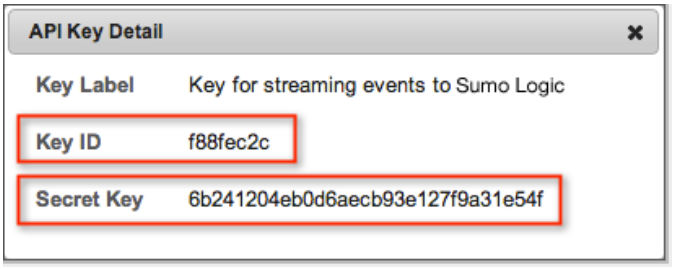
To retrieve your CloudPassage API key, log into the CloudPassage Portal and navigate to **Settings > Site Administration** and click the **API Keys** tab. (If you haven't generated an API key yet, do so by clicking **Add New Key**.)



If you do create an API key, we recommend that, as a best practice, you create a read-only key. A read-only key is all that you need to be able to retrieve Halo event data.



You will need to retrieve both the **Key ID** and the **Secret Key** values for the API key. Click **Show** for your key on the **API Keys** tab to display both values.



Copy the ID and the secret into a text file so that it contains just one line, with the key ID and the secret separated by a vertical bar ("|"):

your_key_id|your_secret_key

Note: If you want to stream events from multiple Halo accounts, add one additional line to this file for each account, containing the account's key ID and secret key formatted as above.

Save the file as haloEvents.auth (or any other name, if you will be using the **--auth** command option). You will need this authentication file to run the Connector.

We recommend that you execute the Connector script standalone first, to get familiar with the different input switches and output formats it supports. Then you can choose the options that best suit your needs in HP ArcSight.

1. Place all of the script-related files in the same directory. That is:
   - haloEvents.py
   - cpapi.py and cputils.py
   - remote_syslog.py (if you are running on Windows *and* you want to generate syslog output)
   - haloEvents.auth (unless you will use the --auth command option, in which case the authentication file can be anywhere.)
2. Set environment variables as necessary:

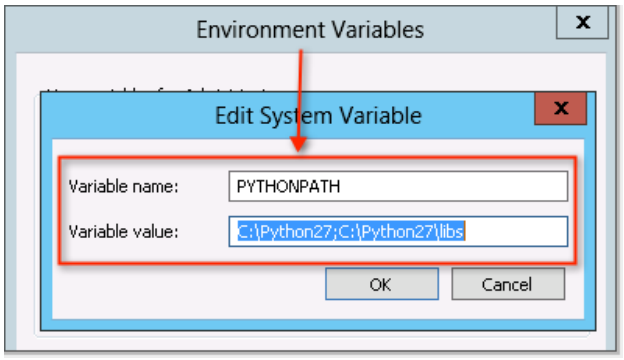
   On Linux:

   - Include the full path to the Python interpreter in the PATH environment variable.

   On Windows:

   - Set the variable PATH to include the location of haloEvents.py and the Python interpreter.

- Set the variable PYTHONPATH to include the location of the Python libraries and the Python interpreter.



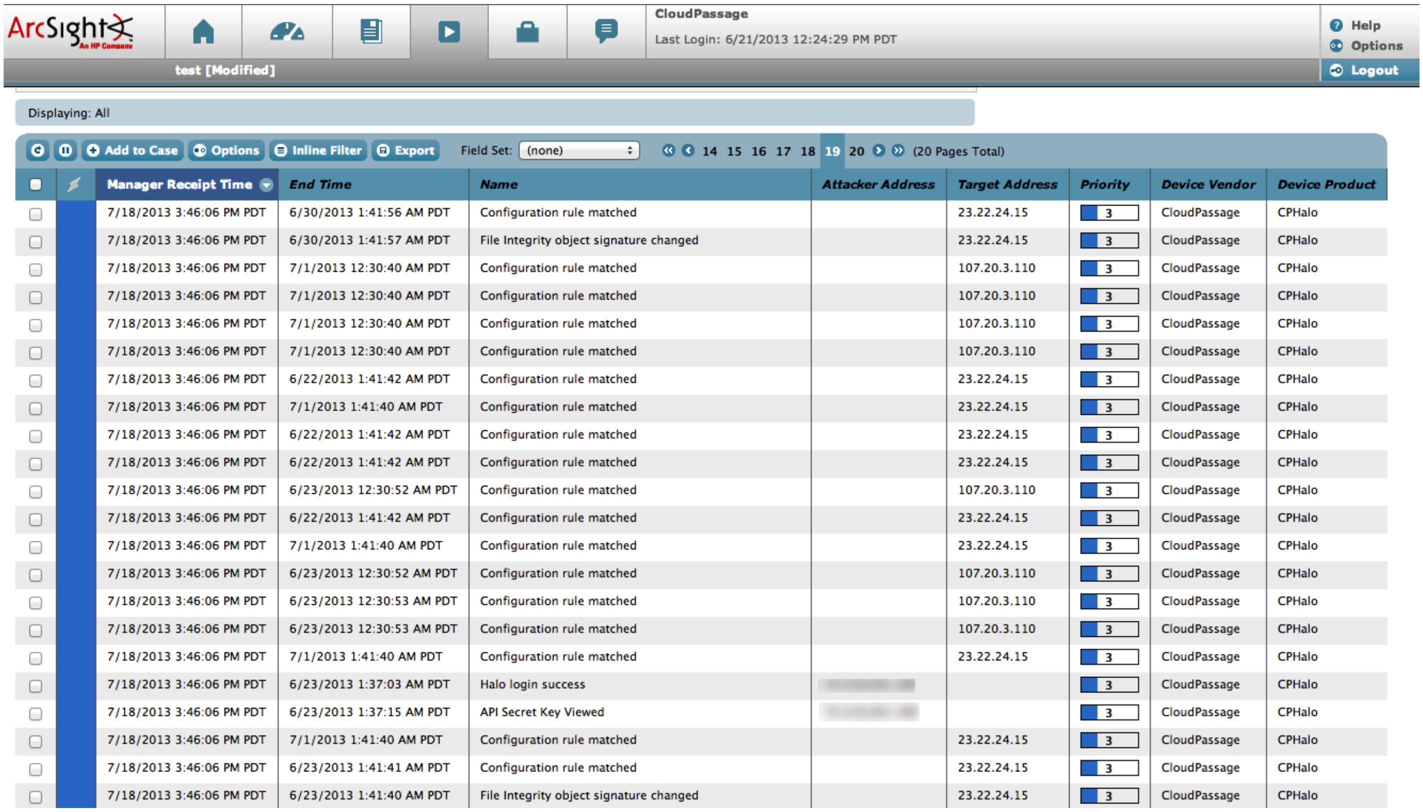
3. Launch the Connector from that directory, with a command like this:

   $ haloEvents.py --cef

   Since the arguments are for CEF, you should soon see CEF-formatted event values streaming to output. You may want to abort execution if your Halo account has accumulated a large number of events.

4. Run the script a few more times, experimenting with arguments to save output to a file, or to produce other output formats. (A syslog daemon must be running if you want to output syslog format. On Linux systems, the syslog daemon typically stores the data at /var/log/messages.)

Screen Shot



Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
7/18/2013 3:46:06 PM PDT	6/30/2013 1:41:56 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/30/2013 1:41:57 AM PDT	File Integrity object signature changed		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 12:30:40 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 12:30:40 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 12:30:40 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 12:30:40 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/22/2013 1:41:42 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 1:41:40 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/22/2013 1:41:42 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/22/2013 1:41:42 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 12:30:52 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/22/2013 1:41:42 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 1:41:40 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 12:30:52 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 12:30:53 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 12:30:53 AM PDT	Configuration rule matched		107.20.3.110	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 1:41:40 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 1:37:03 AM PDT	Halo login success	[illegible]		3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 1:37:15 AM PDT	API Secret Key Viewed	[illegible]		3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	7/1/2013 1:41:40 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 1:41:41 AM PDT	Configuration rule matched		23.22.24.15	3	CloudPassage	CPHalo
7/18/2013 3:46:06 PM PDT	6/23/2013 1:41:40 AM PDT	File Integrity object signature changed		23.22.24.15	3	CloudPassage	CPHalo

Events

A list of all events and associated event IDs are provided as an attachment

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.

Halo Event Connector Field Mappings

Vendor-Specific Event Definition	ArcSight Event Data Field
0	CEF Version
CloudPassage	Device Vendor
CPHalo	Device Product
1.0	Device Product Version
Event ID	Signature ID
Device IP	dvc
Direction	Device Direction
server_ip_address	dst
server_hostname	dhost
Message	msg
created_at	rt
actor_ip_address	src
actor_username	duser
object_name	fname
policy_name/rule_name	cs1
server_platform	cs2
server_id	cs3
server_group_name	cs4