



Hewlett Packard Enterprise

Common Event Format Configuration Guide

ABAP-Experts.com // NCMI GmbH

SecurityBridge

Date: Thursday, January 12, 2017



Table of Contents

| | |
|---|----|
| Common Event Format Configuration Guide | 1 |
| Table of Contents | 2 |
| SecurityBridge Configuration Guide | 3 |
| 1. Joint-Solution Overview..... | 3 |
| 2. Use Cases..... | 3 |
| Use case 1 - Parallel Logins of an account | 4 |
| Use Case 2 – Assignment of critical authorizations and authorization cover-ups..... | 4 |
| Use Case 3 – Execution of OS-Commands from within SAP..... | 4 |
| Use Case 4 – Critical remote function calls..... | 4 |
| Use Case 5 – Insecure RFC connections..... | 4 |
| Use Case 6 – Outdated GUI usage | 5 |
| Use Case 7 – Active whitelist changes | 5 |
| 3. SecurityBridge CEF Integration..... | 6 |
| A. Configuration of SecurityBridge to output CEF events | 6 |
| B. Events..... | 9 |
| C. Device Event Mapping to ArcSight Data Fields | 9 |
| 4. ArcSight Content for SecurityBridge..... | 10 |
| 5. Revision History..... | 10 |
| 6. Prerequisites | 10 |
| 7. Support..... | 11 |
| 8. Additional ArcSight Documentation..... | 11 |

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 HPE. HPE 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 HPE ArcSight Common Event Format. The HPE ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HPE'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.

SecurityBridge Configuration Guide

This guide provides information for configuring SecurityBridge for event collection. This Connector is supported on platforms running a SAP Netweaver ABAP stack, including those running within SAP's Enterprise Cloud.

1. Joint-Solution Overview

SecurityBridge from ABAP-Experts.com is a leading threat and vulnerability monitoring add-on for SAP environments. Information from more than 20 different data sources are correlated in order to create actionable security alerts.

Security relevant configuration changes are analyzed in real-time. Potential attack vectors are revealed and in conjunction with HPE ArcSight they can be removed before exploited by an attacker.

2. Use Cases

SecurityBridge provides pre-configured check patterns, and you can also configure alerts and use cases to environment specific requirements.

Out-of-the-box SecurityBridge is installed with predefined patterns covering both infrastructural and application vulnerabilities (at the time of releasing this configuration guide more than 60 event listening components covering +100 use cases) to validate recommendations originating from the German SAP User group (DSAG).

For an up-to-date overview of event listeners and use cases covered please contact ABAP-Experts directly. Below some randomly picked examples:

Use case 1 - Parallel Logins of an account

Although parallel logins by default are not allowed due to SAP license restrictions SecurityBridge monitors the use of an account being used from multiple terminals. In case the use of an account was identified originating from various terminals this may indicate identify theft. Next to an alert send to HPE ArcSight SecurityBridge can also send a real-time email alert to the user involved.

Use Case 2 – Assignment of critical authorizations and authorization cover-ups

Permission objects can be used to grant godrights to an account. Besides governmental compliance, certain objects shall be assigned only after explicit approval. Assignment without prior approval may indicate an attack or suspicious behavior. Also the assignment of critical authorizations to your own user-ID is handled separately. SecurityBridge comes preconfigured with a list of critical authorization profiles which can be extended by customers by environment specific roles and profiles.

Use Case 3 – Execution of OS-Commands from within SAP

e.g. standard program *RSBDCOS0* allows the execution of OS-commands from with the SAP GUI. Only basis resources having genuine reasons for executing OS-commands from within the SAP front end should be authorized to do so. Generally all other resources should have no access rights to execute any OS-command! Access to the OS running SAP is a major security breach.

Use Case 4 – Critical remote function calls

Using remote enabled functions SAP allows external systems (not necessarily SAP systems) to gain access to consume or update data within SAP. A SAP system may also call a remote function located on another SAP system. RFC functions are typically the backbone for (older) SAP integration scenarios though depending on the function consumed/called there is also a certain risk involved. Hackers may make use of remote enabled function modules to gain access to a system, to extract business critical data or to inject data into business or technical transactions.

SecurityBridge comes preconfigured with a list of function modules known for their exploit capabilities. Each use of such a function is reported in real-time.

Use Case 5 – Insecure RFC connections

RFC connections are commonly used to read, insert and update data within SAP instances. Attackers having access to the RFC connection setup may gain entire

SAP landscape access. Next to access control SecurityBridge also monitors whether a destination is secure or not. Destinations with fixed users, fixed passwords, will be highlighted. Also in case the user maintained within a destination has too much authorization the severity of an alert would be increased automatically.

Use Case 6 – Outdated GUI usage

A SAP GUI get installed locally in order to access an SAP backend. The use of outdated GUI versions may create a security risk as front-end exploits can be used. SecurityBridge is able to generate an alert whenever a user connects to the backend using an outdated GUI.

Use Case 7 – Active whitelist changes

A whitelist in SAP is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition.

Due to the potential sensitivity of whitelist data, it is interesting for a hacker to change the status to (in)active in order to access the data sources unnoticed.

3. SecurityBridge CEF Integration






A. Configuration of SecurityBridge to output CEF events

The initial installation of SecurityBridge is extensively documented as part of the SAP delivery package. This section therefore only summarizes how to enable CEF integration using flat files.

1. CEF output is handled centrally by the SecurityBridge controller

Your SAP landscape(s) may have many SAP instances which are to be guarded by SecurityBridge. Only one system needs to be nominated as controller, all other systems are defined as agents.

The screenshot displays the SecurityBridge configuration interface. At the top, there are buttons for 'Distribute configuration', 'Edit', 'Add', and 'Delete'. Below this is a table titled 'System information' with columns: Active, SAP System, Contr/Agent, Landscape, System type description, and Destination. The table contains five rows of system data. The first row, for system 'AED', is highlighted in yellow and has a green box around the 'Contr/Agent' icon. Below the table are buttons for 'Close', 'Save', and 'System check'. A section titled 'System Connection Details' is shown below the table, with fields for 'System name' (AED), 'Type of system' (C, with 'Security Controller' text to the right), 'Destination' (SecurityBridge@AED.100), and 'Active' (checked).

| Active | SAP System | Contr/Agent | Landscape | System type description | Destination |
|-------------------------------------|------------|---|------------|-------------------------|------------------------|
| <input checked="" type="checkbox"/> | AED |  | ABEX 7.3 | Production | SecurityBridge@AED.100 |
| <input checked="" type="checkbox"/> | AEQ |  | ABEX 7.3 | Acceptance | SecurityBridge@AEQ.100 |
| <input checked="" type="checkbox"/> | AE1 |  | ABEX 7.5 | Development | SecurityBridge@AE1.001 |
| <input type="checkbox"/> | AE2 |  | ABEX 7.5 | Acceptance | SecurityBridge@AE2.001 |
| <input type="checkbox"/> | RCK |  | ABEX AMAZO | Development | SecurityBridge@RCK.001 |

System Connection Details

System name: * AED

Type of system: * C Security Controller

Destination: * SecurityBridge@AED.100

Active:

2. Activate CEF to file

Within the connection settings you need to enable the checkboxes marked below. In this example a consolidated CEF file (covering all events across your entire SAP landscape) is generated every 3 minutes using a dedicated fileshare. Optionally you can also use an FTP server to port files.

Intrusion Detection Scanner (IDS)

| | |
|------------------------------|---|
| IDS Frequency in min: * | <input type="text" value="3"/> |
| Intrusion Scan User: | <input type="text" value="SECBRIDGE"/> |
| Password: | <input type="password" value="....."/> |
| Output via Controller | <input checked="" type="checkbox"/> |
| Output enabled | <input checked="" type="checkbox"/> |
| Write CEF to File | <input checked="" type="checkbox"/> |
| Base Path: * | <input type="text" value="/usr/sap/tmp/sefw"/> |
| Intermediate File Prefix: * | <input type="text" value="tmp"/> |
| Enable FTP Transfer | <input checked="" type="checkbox"/> |
| FTP Server name/IP: * | <input type="text" value="ftp.abap-experts.com"/> |
| FTP User: * | <input type="text" value="abap-expertscom@abap-experts.com"/> |
| FTP Directory: * | <input type="text" value="/tmp/cef/AED/"/> |
| FTP Password: * | <input type="password" value="....."/> |

Depending on your version of SecurityBridge also other outputs like webservice may be available.

B. Events

A list of event ID's is available as a separate PDF file 'SecurityBridge - Event Listeners 2016'. Please note this listing is continuously extended with newly identified vulnerabilities and released listeners. For an accurate overview please reach out to ABAP-Experts.com directly.

C. 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.

SecurityBridge Connector Field Mappings

| Vendor-Specific Event Definition | ArcSight Event Data Field |
|--|-----------------------------|
| SAP System ID | \$\$SAP\$SID |
| SAP Client | \$\$SAP\$CLIENT |
| Central database system | \$\$SAP\$DB |
| Operation system of the application server | \$\$SAP\$OS |
| SAP Release Status | \$\$SAP\$RELEASE |
| SAP Installation No. | \$\$SAP\$INSTALLATIONNUMBER |
| Computer name of the current SAP application server | \$\$SAP\$HOST |
| Destination/SAP Server Host | Dvchost / dhost |
| Terminal or source host | shost |
| Firstname, Lastname | Duser |
| SAP User-ID | evtusr |
| Timestamp of event occurrence | rt |
| Message string, generated by the SecurityBridge listener | msg |
| SAP System ID for which the event was identified | cs1label = 'SAPsid |

| Vendor-Specific Event Definition | ArcSight Event Data Field |
|--|--|
| SAP Client on which the event was identified | cs2label = 'SAPclient' |
| SAP Database on which the event was identified | cs3label = 'SAPdb' |
| Email address maintained on the controller (LDAP integration possible) | cs4label = 'Email address event originator' |
| Telephone and email of the main contact for the area of responsibility to which the event was assigned | cs5label = 'Main contact area of responsibility' |
| Telephone and email of the backup contact for the area of responsibility to which the event was assigned | Cs6label = 'Backup contact area of responsibility' |

4. ArcSight Content for SecurityBridge

5. Revision History

| Date | Description |
|------------|---|
| 05-01-2017 | First edition of this Configuration Guide. |
| 01-12-2017 | Version 730 Certified by HP Enterprise Security |

6. Prerequisites

| Product Name | Version Information | Operating System |
|-----------------------|---------------------|------------------|
| HPE Security ArcSight | | |

7. Support

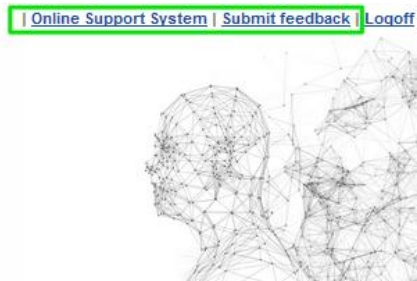
CEF Connector Support Information when an issue is outside of the ArcSight team's ability

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:

SecurityBridge Customer Support

Www OSS.ABAP-Experts.com

Instructions – SecurityBridge users may always use the integrated support options accessible through the configuration cockpit in the top right corner of your browser:



8. Additional ArcSight Documentation

For more information about the joint-solution, visit the HPE ArcSight Marketplace:
<https://marketplace.saas.hpe.com/arcSight/category/partner-integrations>

For more information about HPE Security ArcSight ESM:
<http://www8.hp.com/us/en/software-solutions/siem-security-information-event-management/index.html>