

ENTERPRISE SECURITY



Common Event Format Configuration Guide

Lieberman Software

Enterprise Random Password Manager

Date: Wednesday, May 09, 2012



LIEBERMANSOFTWARE..



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.

CEF Certified:

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

Enterprise Random Password Manager (ERPM)

January 2012

Revision History

Date	Description
01/24/12	First edition of this Configuration Guide.
05/07/12	Updated with ERPM 4.83.4
05/09/12	Certified by HP ArcSight

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:

Lieberman Software Corporation Customer Support

Phone - 1-310-550-8575

Email - support@liebsoft.com

Instructions – Call or email support. Identify your name, company, product, version and a description of the problem as well as the steps required to reproduce the problem. Screenshots are helpful as are program logs.



ERPM Configuration Guide

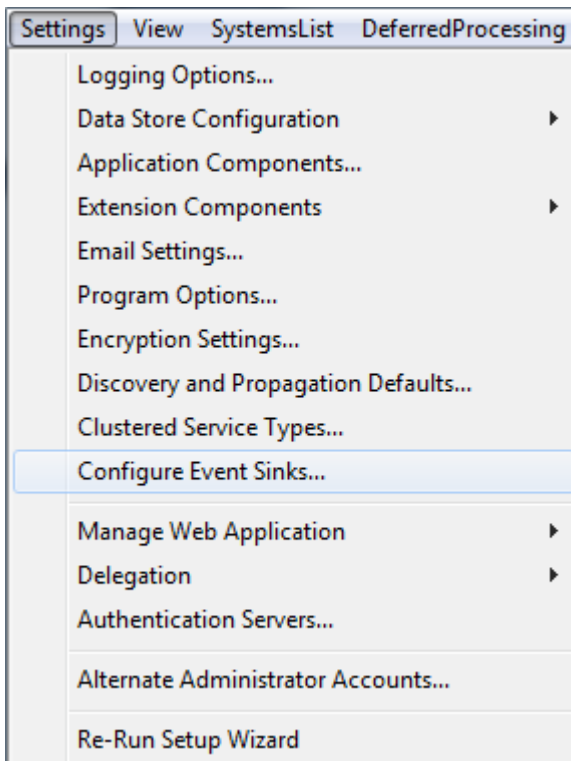
This guide provides information for configuring ERPM for syslog event collection. This Connector is supported on Windows platforms. Device versions up to 4.83.4 are supported.

Overview

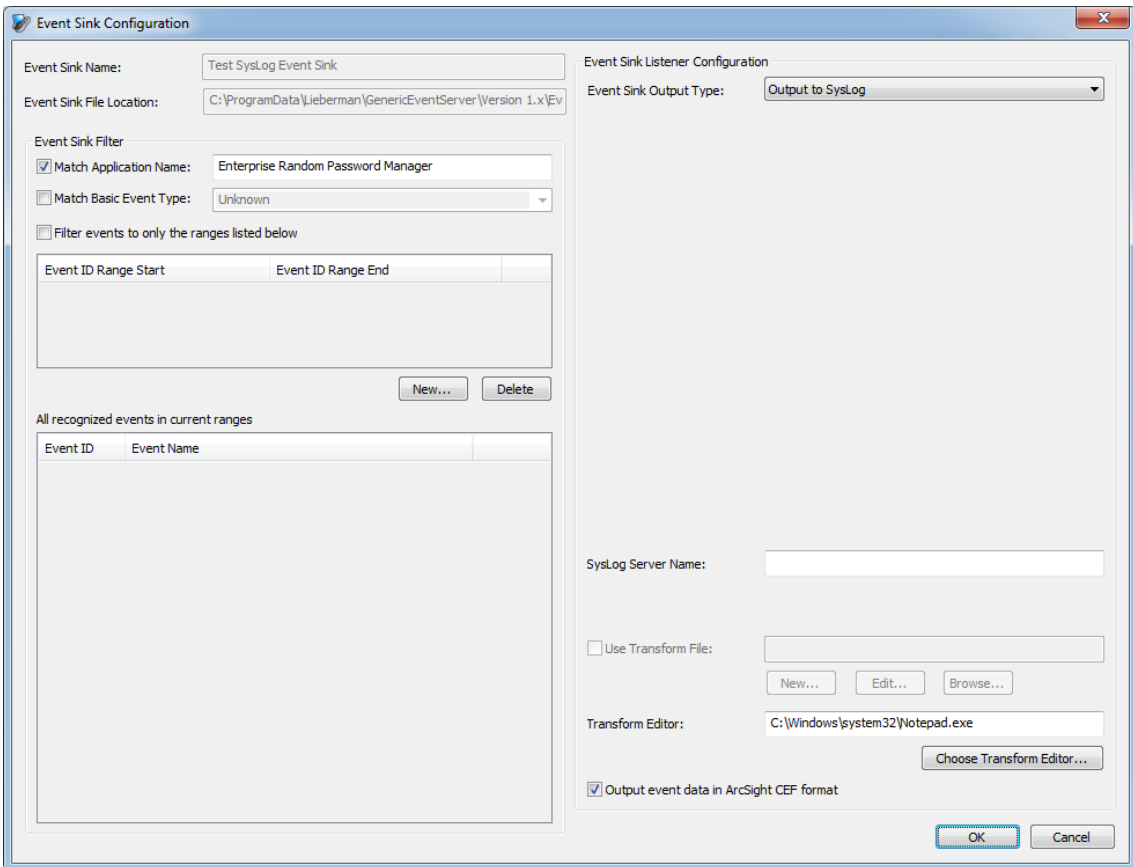
ERPM is an account management utility for securing and managing privileged, primarily service, accounts. ERPM contains an event generation and forwarding model, which supports a flexible event forwarding configuration with various filters and connectors available.

Configuration

Forwarding events to an ArcSight instance is accomplished via the Event Sinks configuration interface, which is accessible in the console application from the Settings ->Configure Event Sinks... menu selection:



This will open the event sinks list for the application, and adding a new (or editing an existing) event sink will bring up the event sink configuration dialog:



This dialog allows the administrator to configure event forwarding. To configure forwarding to ArcSight, first configure the desired event filter parameters (left side of the dialog). You can forward all events by leaving the event filter unselected, or select particular events or ranges to send to ArcSight. Then, for the output type, select "Output to SysLog" (which is the input type for ArcSight). Fill in the server name to be the name or IP address for the ArcSight receiver server, and select the "Output event data in ArcSight CEF format" check box. When you click OK, the new sink will be saved, and will be automatically updated in the event forwarder.

Screen Shot

The screenshot shows the ArcSight Console interface. The main window displays a list of events for the channel 'Liebsoft (84%)'. The events are sorted by 'Manager Receipt Time' and include columns for End Time, Name, Device Vendor, Device Product, Device Severity, Device Action, Device Event Category, and Device Event Class.

Manager Receipt Time	End Time	Name	Device Vendor	Device Product	Device Severity	Device Action	Device Event Category	Device Event Class
25 Apr 2012 14:29:43 PDT	25 Apr 2012 14:28:47 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_CONSI
25 Apr 2012 14:29:13 PDT	25 Apr 2012 14:28:14 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_CONSI
25 Apr 2012 12:33:58 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_SCHEE
25 Apr 2012 12:33:58 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_SCHEE
25 Apr 2012 12:33:58 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_SCHEE
25 Apr 2012 12:33:58 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Success	Liebsoft	Enterprise Random Password Manager	4			EVENT_ID_SCHEE
25 Apr 2012 12:33:58 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_SCHEE
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_PASSV
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_F
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Status Update	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_R
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Status Update	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Status Update	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Start	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_S
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Generic Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_T
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Start	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_S
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Generic Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_D
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Start	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_S
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_A
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Success	Liebsoft	Enterprise Random Password Manager	4			EVENT_ID_JOB_A
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_CONSI
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Start	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Failure	Liebsoft	Enterprise Random Password Manager	5			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Job Processing Complete, Success	Liebsoft	Enterprise Random Password Manager	4			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_H
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_H
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_JOB_C
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_PASSV
25 Apr 2012 12:33:51 PDT	25 Apr 2012 12:32:44 PDT	Operation Notification, General	Liebsoft	Enterprise Random Password Manager	3			EVENT_ID_PASSV

Events

The list of all events generated by ERPM is contained in the ERPM documentation, and may change with new product releases.



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.

ERPM Connector Field Mappings

Vendor-Specific Event Definition	ArcSight Event Data Field
"Liebsoft"	Device Vendor
Application Name (eg: Enterprise Random Password Manager)	Device Product
Application Version (eg: 4.83.4)	Device Version
Event ID	Device Event Class ID
Fixed value, based on general event type	Severity
Operation result message, if applicable	Message
General Event Type Examples are: - Success - Failure - Operation Status Update - Trace	cs1
Job ID (if applicable)	cs2
IP Address for web request (if applicable)	cs3
Login Name for web user - Only applicable for events generated while processing web interface operations	cs4
Manager Name / Role for web user - Only applicable for events generated while processing web interface operations	cs5
Group Name	cs6
Host Domain generating event, or target domain for operation (see note)	sntdom/dntdom
Host System generating event, or target system for operation (see note)	shost/dhost
Account under which operation is performed, or target account for operation (see note)	suser/duser

Notes and Other Information

Use of sntdom/dntdom, shost/dhost and suser/duser

The system name for the system generating the event and the credentials processing the operation at the time of the event generation are included in every event generated by our application. Per ArcSight configuration instructions, for similarity with existing conventions, these are included in the dhost/duser fields respectively, for events for which there is not otherwise an enumerated and differentiated (in our event data) target system or account. However, for events which contain a target system, the generating system is sent as shost, and the target system is sent as dhost. Similarly, for events which are generated which have an enumerated target account, the processing-under account is moved to suser, and the target account is sent as duser. If the suser/duser is a domain account, the domain information is saved in sntdom/dntdom field.

