Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Windows ESENT Logs

Supplemental Configuration Guide

Document Release Date: June 18, 2020
Software Release Date: June 18, 2020

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

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:

ArcSight Product Documentation on the Micro Focus Security Community

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
06/18/2020	First edition of this Configuration Guide to provide support for Microsoft Windows ESENT events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows ESENT Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows ESENT Logs and its event mappings to ArcSight data fields.

Supported Versions:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)

Product Overview

Microsoft Windows ESENT is an embeddable and transactional database engine which is used for data storage. You can use ESENT for applications that need reliable, high-performance, and low-overhead storage of structured or semi-structured data. The ESENT engine can help with data needs ranging from something as simple as a hash table that is too large to store in memory to something more complex such as an application with tables, columns, and indexes.

SmartConnector for Microsoft Windows Event Log – Native (WINC) provides support for ESENT application of Windows.

Connector Installation and Configuration

Follow the installation and configuration procedures in the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*, selecting **Microsoft Windows Event Log – Native** as the connector to be configured. During installation, select **true** for the **Application Logs** field to collect the ESENT application events.

Mappings for Microsoft Windows ESENT Logs

General

ArcSight Field	Vendor Field
Device Vendor	‘Microsoft’
Device Product	'ESENT'
Device Version	'Unknown'

Event ID 325

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine created a new database"
Source Process Id	%2
Source Service Name	%1

Event ID 326

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine attached a database"
Source Process Id	%2
Source Service Name	%1

Event ID 327

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine detached a database"
Source Process Id	%2
Source Service Name	%1

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 Supplemental Configuration Guide (Connectors 7.15.0)

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 arcsight_doc@microfocus.com.

We appreciate your feedback!