



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Windows Event Log - Native: Microsoft Windows ESENT Logs Supplemental Configuration Guide**

Document Release Date: September 17, 2020

Software Release Date: September 17, 2020

## Legal Notices

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

<https://www.microfocus.com>

## Copyright Notice

© Copyright 2010-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## 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: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

### Revision History

Date	Description
09/17/2020	Added support to the following event ids: 102, 103, 105, 224, 225, 300, 301, 302, 330, 335, 455 and 641.
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 .....	5
Product Overview .....	5
Connector Installation and Configuration .....	5
Mappings for Microsoft Windows ESENT Logs .....	6
General .....	6
Event Id 102 .....	6
Event Id 103 .....	6
Event Id 105 .....	6
Event Id 224 .....	7
Event Id 225 .....	7
Event Id 300 .....	7
Event Id 301 .....	7
Event Id 302 .....	8
Event Id 325 .....	8
Event Id 326 .....	8
Event Id 327 .....	8
Event Id 330 .....	9
Event Id 335 .....	9
Event Id 455 .....	9
Event Id 641 .....	10
Send Documentation Feedback .....	11

# 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 10
- 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 102

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is starting a new instance

### Event Id 103

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine stopped the instance

### Event Id 105

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine started a new instance

## Event Id 224

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4 to %5
Name	Deleting log files

## Event Id 225

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	No log files can be truncated

## Event Id 300

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is initiating recovery steps

## Event Id 301

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
File Type	%6

ArcSight Field	Vendor Field
Device Custom String 1	%7
Device Custom String 1 Label	Number of times log record seen
Name	The database engine has finished replaying log file

## Event Id 302

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine has successfully completed recovery steps

## 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
Source Process Name	%3

## Event Id 327

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine detached a database"



ArcSight Field	Vendor Field
Source Process Id	%2
Source Service Name	%1

## Event Id 330

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%7
Device Custom String 4 Label	Default engine version
Name	The database format version is being held back

## Event Id 335

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%5
Reason	%7
Name	Replay of a create for database at log position was deferred

## Event Id 455

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%5
Device Custom String 4 Label	Error
Name	Error occurred while opening log file

## Event Id 641

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Device Custom String 4	%5
Device Custom String 4 Label	Log format version
Device Custom String 5	%6
Device Custom String 5 Label	Current log format version
Name	The log format feature version could not be used

# 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 8.0.0)**

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 [Documentation-Feedback@microfocus.com](mailto:Documentation-Feedback@microfocus.com).

We appreciate your feedback!