



Micro Focus Security ArcSight Connectors

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

Supplemental Configuration Guide

Document Release Date: January 16, 2020

Software Release Date: January 16, 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.

US 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 US 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 US 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 US 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 US 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: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
01/16/2020	First edition of this guide

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows Event Log	6
Product Overview	6
Connector Installation and Configuration	6
jajajaSpecific Windows Security Event Mappings	7
General	7
104	7
1100	7
1101	7
1102	8
1104	8
1105	8
Send Documentation Feedback	9

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

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows Event Log 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

The ***SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings*** document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Windows Event Log.

Product Overview

The Windows event log is a detailed record of system, security and application notifications stored by the Windows operating system that is used by administrators to diagnose system problems and predict future issues.

These event logs are used to record important hardware and software actions that the administrator can use to troubleshoot issues with the operating system. The Windows operating system tracks specific events in its log files, such as application installations, security management, system setup operations on initial startup, and problems or errors.

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 **System Logs, Security Logs** field for system events to be collected.

jajajaSpecific Windows Security Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The log file was cleared'
Message	concatenate('The 'Channel',' log file was cleared')
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName
File Type	Channel
File Path	BackupPath

1100

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The event logging service has shut down.'

1101

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Audit events have been dropped by the transport. The real time backup file was corrupt due to improper shutdown.'
Device Custom Number 3	Reason

1102

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The audit log was cleared.'
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination User ID	SubjectLogonId

1104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The security log is now full'
Message	concatenate('The ',Channel,' log file was cleared')
SourceNtDomain	SubjectDomainName
SourceUserName	SubjectUserName
FileType	Channel
FilePath	BackupPath

1105

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Event log automatic backup.'
File Type	Channel
File Name	BackupPath

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)

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!