Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Windows WMI Activity Trace

Supplemental Configuration Guide

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

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) 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. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

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.

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.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows WMI Activity Trace

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

Supported Versions:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Product Overview

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

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 **Custom Logs** and enter the channel name **Microsoft-Windows-WMI-Activity/Trace** to read WMI Activity/Trace Logs.

Mappings for Microsoft Windows WMI Activity Trace

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	Microsoft Windows WMI Activity Trace
Name	WMI-Activity Query executed on Win23 BIOS
Device Custom String 1	ClientMachineFQDN
Device Custom String 3	CorrelationId
Device Custom String 4	IsLocal
Device Custom String 5	Operation
Device Custom Number 1	OperationId
Device Custom Number 2	GroupOperationId
Source Host Name	ClientMachine
Source User Name	User
Source Process Id	ClientProcessId
File Create Time	ClientProcessCreationTime
File Path	NamespaceName

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!