



Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Antimalware

Supplemental Configuration Guide

Document Release Date: September 19, 2019

Software Release Date: September 19, 2019

Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2010-2019 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 CFR. 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 CFR. 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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
09/19/2019	First edition of this Configuration Guide, for initial support of these events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Antimalware	5
Product Overview	5
Connector Installation and Configuration	5
Mappings for Windows Event Log Native: Microsoft Antimalware	6
Event 1000	6
Event 1001	6
Event 1002	7
Event 1011	7
Event 1013	8
Event 1116	8
Event 1117	9
Event 1150	11
Event 2000	11
Event 2001	12
Event 2002	12
Event 2010	12
Event 2011	13
Event 3002	14
Event 5007	14
Event 5010	14
Event 5012	14
 Send Documentation Feedback	 15

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Antimalware

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

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 Antimalware.

Product Overview

Microsoft Antimalware is a network service in Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

Microsoft Antimalware is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system.

The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

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** field for system events to be collected.

Mappings for Windows Event Log Native: Microsoft Antimalware

Event 1000

ArcSight Field	Vendor Field
Product Name	productName
Product Version	productVersion
Scan ID	deviceCustomString1
Scan Type Index	scanTypeIndex
Scan Type	deviceEventCategory
Scan Parameter Index	scanParameterIndex
Scan Parameters	deviceAction
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Scan resources	filePath

Event 1001

ArcSight Field	Vendor Field
Product Name	productName
Product Version	productVersion
Scan ID	deviceCustomString1
Scan Type Index	scanTypeIndex
Scan Type	deviceEventCategory
Scan Parameter Index	scanParameterIndex
Scan Parameters	deviceAction

ArcSight Field	Vendor Field
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Scan Time Hours	deviceCustomNumber1
Scan Time Minutes	deviceCustomNumber2
Scan Time Seconds	deviceCustomNumber3

Event 1002

ArcSight Field	Vendor Field
Product Name	productName
Product Version	productVersion
Scan ID	deviceCustomString1
Scan Type Index	scanTypeIndex
Scan Type	deviceEventCategory
Scan Parameter Index	scanParameterIndex
Scan Parameters	deviceAction
Domain	sourceNtDomain
User	sourceUserName
SID	sid

Event 1011

ArcSight Field	Vendor Field
Product Name	productName
Product Version	productVersion
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Threat Name	deviceCustomString1
Threat ID	deviceCustomNumber1
Severity ID	deviceCustomNumber2

ArcSight Field	Vendor Field
Category ID	deviceCustomNumber3
FWLink	FWLink
Path	filePath
Severity Name	deviceSeverity
Category Name	deviceCustomString4
Signature Version	deviceCustomString2
Engine Version	(Concatenating both the fields)

Event 1013

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion
Timestamp	deviceCustomDate1
Domain	sourceNtDomain
User	sourceUserName
SID	sid

Event 1116

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion
Detection ID	deviceCustomString5
Detection Time	deviceCustomDate1
Threat ID	deviceCustomNumber1
Threat Name	deviceCustomString1
Severity ID	deviceCustomNumber2
Severity Name	deviceCustomString3
Category ID	deviceCustomNumber3
Category Name	deviceCustomString4
FWLink	FWLink

ArcSight Field	Vendor Field
Status Code	statusCode
Status Description	statusDescription
State	state
Source ID	sourceID
Source Name	sourceName
Process Name	sourceProcessName
Detection User	sourceUserName
Path	filePath
Origin ID	originID
Origin Name	originName
Execution ID	executionID
Execution Name	executionName
Type ID	typeID
Type Name	oldFileType
Pre Execution Status	preExecutionStatus
Action ID	actionID
Action Name	devicAction
Error Code	errorCode
Error Description	reason
Post Clean Status	postCleanStatus
Additional Action ID	additionalActionID
Additional Action String	additionalActionString
Remediation User	remediationUser
Signature Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2
Engine Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2

Event 1117

ArcSight Field	Vendor Field
Product Name	productName
Product Version	productVersion

ArcSight Field	Vendor Field
Detection ID	deviceCustomString5
Detection Time	deviceCustomDate1
Threat ID	deviceCustomNumber1
Threat Name	deviceCustomString1
Severity ID	deviceCustomNumber2
Severity Name	deviceCustomString3
Category ID	deviceCustomNumber3
Category Name	deviceCustomString4
FWLink	FWLink
Status Code	statusCode
Status Description	statusDescription
State	state
Source ID	sourceID
Source Name	sourceName
Process Name	sourceProcessName
Detection User	sourceUserName
Path	filePath
Origin ID	originID
Origin Name	originName
Execution ID	executionID
Execution Name	executionName
Type ID	typeID
Type Name	oldFileType
Pre Execution Status	preExecutionStatus
Action ID	actionID
Action Name	devicAction
Error Code	errorCode
Error Description	reason
Post Clean Status	postCleanStatus
Additional Action ID	additionalActionID

ArcSight Field	Vendor Field
Additional Action String	additionalActionString
Remediation User	remediationUser
Signature Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2
Engine Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2

Event 1150

ArcSight Field	Vendor Field
Product Name	productName
Product Verison	deviceVersion
Signature Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2
Engine Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2

Event 2000

ArcSight Field	Vendor Field
Product Name	productName
Product Verison	deviceVersion
Current Signature Version	fileId
Previous Signature Version	oldFileId
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Signature Type Index	signatureTypeIndex
Signature Type	deviceEventCategory
Update Type Index	updateTypeIndex
Update Type	deviceCustomString6
Current Engine Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2
Previous Engine Version	(Concatenating both Engine Version and Signature Version in deviceCustomString2

Event 2001

ArcSight Field	Vendor Field
Product Name	productName
Product Verison	deviceVersion
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Error Code	deviceCustomString5
Error Description	reason
FWLink	filePath

Event 2002

ArcSight Field	Vendor Field
Product Name	productName
Product Verison	deviceVersion
Previous Engine Version	(Concatenating both Previous Engine Version and Current Version in deviceCustomString2
Current Engine Version	(Concatenating both Previous Engine Version and Current Version in deviceCustomString2
Domain	sourceNtDomain
User	sourceUserName
SID	sid
Feature Index	featureIndex
Feature Index Name	featureName

Event 2010

ArcSight Field	Vendor Field
Product Name	productName
Product Verison	deviceVersion
Current Signature Version	fileId

ArcSight Field	Vendor Field
Signature Type Index	signatureTypeIndex
Signature Type	deviceEventCategory
Current Engine Version	deviceCustomString2
Dynamic Signature Type Index	dynamicSignatureTypeIndex
Dynamic Signature Type	dynamicSignatureType
Persistence Path	filePath
Dynamic Signature Version	dynamicSignatureVersion
Persistence Limit Type Index	persistenceLimitTypeIndex
Persistence Limit Type	persistenceLimitType
Persistence Limit Value	persistenceLimitValue

Event 2011

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion
Current Signature Version	fileId
Signature Type Index	signatureTypeIndex
Signature Type	deviceEventCategory
Current Engine Version	deviceCustomString2
Dynamic Signature Type Index	dynamicSignatureTypeIndex
Dynamic Signature Type	dynamicSignatureType
Persistence Path	filePath
Dynamic Signature Version	dynamicSignatureVersion
Persistence Limit Type Index	persistenceLimitTypeIndex
Persistence Limit Type	persistenceLimitType
Persistence Limit Value	persistenceLimitValue
Removal Reason Index	removalReasonIndex
Removal Reason Value	reason

Event 3002

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion
Error Code	deviceCustomString5
Error Description	reason

Event 5007

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion
Old Value	oldFileName
New Value	fileName

Event 5010

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion

Event 5012

ArcSight Field	Vendor Field
Product Name	productName
Product Version	deviceVersion

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!