



Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Antimalware

Supplemental Configuration Guide

Document Release Date: August 20, 2020

Software Release Date: August 20, 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: 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/ctp/productdocs

Revision History

Date	Description
08/20/2020	<p>Added the following new events:</p> <ul style="list-style-type: none"> • Event 1005 • Event 5000 • Event 5001 • Event 5004 <p>Removed "Product Name - productName" value from all the events.</p>
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 1005	7
Event 1011	7
Event 1013	8
Event 1116	8
Event 1117	10
Event 1150	11
Event 2000	11
Event 2001	12
Event 2002	12
Event 2010	13
Event 2011	13
Event 3002	14
Event 5000	14
Event 5001	14
Event 5004	14
Event 5007	15
Event 5010	15
Event 5012	15
 Send Documentation Feedback	 16

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
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
File Path	Scan resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom Number 1	Scan Time Hours
Device Custom Number 2	Scan Time Minutes
Device Custom Number 3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1005

ArcSight Field	Vendor Field
Device Custom String 1 Label	Scan ID
Device Custom String 1	Scan ID
Device Custom String 5	Error Code
Device Custom String 5 Label	Error Code
Device Event Category	Scan Type
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Reason	Error Code

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User

ArcSight Field	Vendor Field
Sid	SID
Device Custom String 1	Threat Name
Device Custom Number 1	Threat ID
Device Custom Number 2	Severity ID
Device Custom Number 3	Category ID
FWLink	FWLink
File Path	Path
Device Severity	Severity Name
Device Custom String 4	Category Name
Device Custom String2	Signature Version
(Concatenating both the fields)	Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Detection ID
Device Custom Date 1	Detection Time
Device Custom Number 1	Threat ID
Device Custom String 1	Threat Name
Device Custom Number 2	Severity ID
Device Custom String 3	Severity Name
Device Custom Number 3	Category ID

ArcSight Field	Vendor Field
Device Custom String 4	Category Name
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2)	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2)	Engine Version

Event 1117

ArcSight Field	Vendor Field
Product Version	Device Version
Detection ID	Device Custom String 5
Detection Time	Device Custom Date 1
Threat ID	Device Custom Number 1
Threat Name	Device Custom String 1
Severity ID	Device Custom Number 2
Severity Name	Device Custom String 3
Category ID	Device Custom Number 3
Category Name	Device Custom String 4
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action Name	Action Name
Error Code	Error Code

ArcSight Field	Vendor Field
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1150

ArcSight Field	Vendor Field
Device Version	Product Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 2000

ArcSight Field	Vendor Field
Device Venison	Product Version
File Id	Current Signature Version
Old File Id	Previous Signature Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type

ArcSight Field	Vendor Field
Update Type Index	Update Type Index
Device Custom String 6	Update Type
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Current Engine Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Previous Engine Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom String 5	Error Code
Reason	Error Description
File Path	FWLink

Event 2002

ArcSight Field	Vendor Field
Product Verison	Device Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Previous Engine Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Current Engine Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Feature Index	Feature Index
Feature Name	Feature Index Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type

ArcSight Field	Vendor Field
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Error Code
Reason	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
File Id	Feature ID
Device Custom Number 1	Configuration
Device Custom Number 1 Label	Configuration

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	New Value

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

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.

We appreciate your feedback!