



# **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

### 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

© Copyright 2010-2019 Micro Focus or one of its affiliates.

### 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

<b>Phone</b>	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>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs</a>

## 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 .....	4
Product Overview .....	4
Microsoft Antimalware .....	4
Connector Installation and Configuration .....	5
Mappings for Windows Event Log Native: Microsoft Antimalware .....	5
Event 1000 .....	5
Event 1001 .....	6
Event 1002 .....	6
Event 1011 .....	7
Event 1013 .....	7
Event 1116 .....	8
Event 1117 .....	9
Event 1150 .....	10
Event 2000 .....	11
Event 2001 .....	11
Event 2002 .....	12
Event 2010 .....	12
Event 2011 .....	13
Event 3002 .....	13
Event 5007 .....	13
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 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 Remote Access.

## Product Overview

Microsoft Antimalware is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

## Microsoft Antimalware

For complete information about Microsoft's Reporting and Microsoft Antimalware, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>



When configuring the Microsoft Antimalware, specify **system** as the event log type for Microsoft Remote Access.

## 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
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
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
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



ArcSight Field	Vendor Field
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
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

ArcSight Field	Vendor Field
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 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
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

ArcSight Field	Vendor Field
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](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!