



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Windows Event Log – Native: Microsoft Windows Defender Antivirus**

### **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 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

<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

<b>Date</b>	<b>Description</b>
01/16/2020	First edition of this Configuration Guide.

# Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows Defender	
AntiVirus .....	5
Product Overview .....	5
Microsoft Windows Defender AntiVirus .....	5
Connector Installation and Configuration .....	6
Mappings for Microsoft Windows Defender AntiVirus .....	6
Event 1000 .....	6
Event 1001 .....	6
Event 1002 .....	7
Event 1009 .....	7
Event 1011 .....	8
Event 1013 .....	9
Event 1015 .....	9
Event 1116 .....	10
Event 1117 .....	12
Event 1150 .....	13
Event 1151 .....	13
Event 2000 .....	14
Event 2001 .....	15
Event 2002 .....	15
Event 2010 .....	16
Event 2011 .....	17
Event 2030 .....	17
Event 3002 .....	18
Event 5000 .....	18
Event 5001 .....	18
Event 5004 .....	18
Event 5007 .....	18
Event 5010 .....	19
Event 5012 .....	19
Send Documentation Feedback .....	20

## SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows Defender AntiVirus

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

For complete information about Microsoft's Reporting and Microsoft Windows Defender AntiVirus, 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 Windows Defender AntiVirus, 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 Microsoft Windows Defender AntiVirus

### Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
File Path	Scan Resources

### Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index

ArcSight Field	Vendor Field
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Hours"
Device Custom Number1	Scan Time Hours
Device Custom Number2 Label	"Minutes"
Device Custom Number2	Scan Time Minutes
Device Custom Number3 Label	"Seconds"
Device Custom Number3	Scan Time Seconds

## Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

## Event 1009

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

ArcSight Field	Vendor Field
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

## Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID



ArcSight Field	Vendor Field
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

## Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1 Label	"Action Time"
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

## Event 1015

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"

ArcSight Field	Vendor Field
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
FWLink	FWLink
Source Process Name	Process Name
File Path	Path Found
Request Context	Detection Origin
Old File Type	Detection Type
Source Service Name	Detection Source

## Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

ArcSight Field	Vendor Field
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
Origin ID	Origin ID
Request Context	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
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

## Event 1117

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
Origin ID	Origin ID

ArcSight Field	Vendor Field
Request Context	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
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

## Event 1150

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

## Event 1151

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String1 Label	"RTP State/ OA State/ IOAV State/ BM State"
Device Custom String 1	RTP State/ OA State/ IOAV State/ BM State
Device Custom Number1	safeToLong(updateRevisionNumber)
Device Custom Number1 Label	"Last AV Signature Age"

ArcSight Field	Vendor Field
Device Custom Number1	AV signature age
Device Custom Number2 Label	"Last AS Signature Age"
Device Custom Number2	AS signature age
Device Custom Number3 Label	"Last quick scan age"
Device Custom Number3	Last quick scan age
Device Floating Point1 Label	"Last full scan age"
Device Floating Point1	Last full scan age
File Create Time	AV signature creation time
Old File Create Time	AS signature creation time
Start Time	Last quick scan start time
End Time	Last quick scan end time
Device Custom String4 Label	"Last Quick Scan Source"
Device Custom String4	Last quick scan source
Device Custom Date1 Label	"Last full scan start time"
Device Custom Date1	Last full scan start time
Device Custom Date2 Label	"Last full scan end time"
Device Custom Date2	Last full scan end time
Device Custom String6 Label	"Last full scan source"
Device Custom String6	Last full scan source
Product status	Product status

## Event 2000

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index

ArcSight Field	Vendor Field
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version

## Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
File Path	Source Path

## Event 2002

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

ArcSight Field	Vendor Field
Source User ID	SID
Device Custom String2 Label	"Current/ Previous Engine Version"
Device Custom String2	Current Engine Version, Previous Engine Version
Feature Index	Feature Index
Device Event Category	Feature Name

## Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
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
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

## Event 2030

ArcSight Field	Vendor Field
Device Version	Product Version

## Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
File ID	Feature ID
File Hash	Feature Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	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
Device Custom Number	"Configuration"
Device Custom Number1 Label	Configuration
File ID	Feature ID

## Event 5007

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

ArcSight Field	Vendor Field
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 )**

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!