



Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log - Native: Microsoft-Windows-AppLocker Supplemental Configuration Guide

Document Release Date: August 20, 2020

Software Release Date: August 20, 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

© Copyright 2010-2020 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

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
08/20/2020	First edition of this configuration guide, for initial support of these events.

Contents

- SmartConnector for Microsoft Windows Event Log - Native: Microsoft-Windows-AppLocker 4
- Product Overview 4
- Microsoft-Windows-AppLocker Configuration 4
- Connector Installation and Configuration 5
- Mappings for Microsoft-Windows-AppLocker 5
 - Event 1015 5
 - Event 1016 5
 - Event 1017 5
 - Event 3006 6
 - Event 3008 6
 - Event 3009 6
 - Event 3010 7
 - Event 3011 7
 - Event 3012 7
 - Event 3013 8
 - Event 8001 8
 - Event 8002 8
 - Event 8003 9
 - Event 8004 9
 - Event 8005 10
 - Event 8006 10
 - Event 8007 11

- Send Documentation Feedback 12

SmartConnector for Microsoft Windows Event Log - Native: Microsoft-Windows-AppLocker

This guide provides information about the SmartConnector for Microsoft Windows Event Log - Native: Microsoft-Windows-AppLocker and its event mappings to ArcSight data fields.

Supported Versions:

- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

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-AppLocker is a network service in Windows 10, Windows Server 2012, Windows Server 2012 R2, 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
- DNS Client

Microsoft-Windows-AppLocker Configuration

For complete information about Microsoft's Reporting and Microsoft-Windows-AppLocker, 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-AppLocker, 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-AppLocker

Event 1015

ArcSight Field	Vendor Field
Name	"Name resolution timed out after the DNS server did not respond"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event 1016

ArcSight Field	Vendor Field
Name	"A name not found error was returned"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event 1017

ArcSight Field	Vendor Field
Name	"The DNS server's response to a query"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event 3006

ArcSight Field	Vendor Field
Name	"DNS query is called"
Device Custom String 1	QueryName
Device Custom String 5	ServerList
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	InterfacelIndex

Event 3008

ArcSight Field	Vendor Field
Name	"DNS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	QueryStatus

Event 3009

ArcSight Field	Vendor Field
Name	"Network query initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress
Device Dns Domain	DNSServerAddress

Event 3010

ArcSight Field	Vendor Field
Name	"DNS Query sent to DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress

Event 3011

ArcSight Field	Vendor Field
Name	"Received response from DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress
Event Outcome	ResponseStatus

Event 3012

ArcSight Field	Vendor Field
Name	"NETBIOS query is initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress

Event 3013

ArcSight Field	Vendor Field
Name	"NETBIOS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Event Outcome	Status

Event 8001

ArcSight Field	Vendor Field
Name	"The AppLocker policy was applied successfully to this computer."

Event 8002

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

Event 8003

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

Event 8004

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

Event 8005

ArcSight Field	Vendor Field
Name	FilePath, " was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

Event 8006

ArcSight Field	Vendor Field
Name	FilePath, " was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

Event 8007

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6:	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath

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!