Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Sysmon Logs

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

Trademark Notices

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
01/16/2020	Updated mappings for events 1 and 10.
09/19/2019	First edition of this Configuration Guide, for initial support of these events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Sysmon Logs 5
Product Overview 5
Microsoft Sysmon Logs Configuration 5
Connector Installation and Configuration 6
Mappings for Microsoft Sysmon Logs 6
General 6
Event 1 6
Event 2 7
Event 3 7
Event 4 8
Event 5 8
Event 7 9
Event 9 9
Event 10 10
Event 11 10
Event 12 11
Event 13 11
Event 15 11
Event 16 12
Event 17 12
Event 18 13
Event 22 13
Event 255 13

Send Documentation Feedback 14

SmartConnector for Microsoft Windows Event Log – Native: Microsoft Sysmon Logs

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Sysmon Logs 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 Sysmon Logs is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, users can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

Microsoft Sysmon Logs Configuration

For complete information about Microsoft's Reporting and Microsoft Sysmon Logs, 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 Sysmon Logs, 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 Sysmon Logs

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Sysmon'
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Name	'Process Created'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Message	Description
Old File Name	OriginalFileName
Destination Service Name	CommandLine
Old File Path	CurrentDirectory
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)
Device Custom String 6	LogonGuid
Source User Id	LogonId
Device Custom String 1	IntegrityLevel

ArcSight Field	Vendor Field
File Hash	Hashes
Old File Id	ParentProcessGuid
Source Process Id	ParentProcessId
Source Process Name	ParentImage
Source Service Name	ParentCommandLine
Device Action	'Process Create'
Destination Process Id	ProcessId
Source User Name	User
Destination User Name	User Id

Event 2

ArcSight Field	Vendor Field
Name	'File creation time changed'
File Id	ProcessGuid
Message	'File creation time changed'
Device Receipt Time	UtcTime
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
File Path	TargetFilename
File Create Time	CreationUtcTime
Old File Create Time	PreviousCreationUtcTime
Device Action	'File creation time changed'

Event 3

ArcSight Field	Vendor Field
Name	'Network connection detected'
Message	'Network connection detected'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)

ArcSight Field	Vendor Field
Destination Process Name	Image
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)
Transport Protocol	Protocol
Device Action	__concatenate("Initiated:",Initiated)
Source Address	__stringToIPv6Address(SourceIp)
Source Host Name	SourceHostname
Source Port	__safeToInteger(SourcePort)
Source Port Name	SourcePortName
Destination Address	__stringToIPv6Address(DestinationIp)
Destination Host Name	DestinationHostname
Destination Port	__safeToInteger(DestinationPort)

Event 4

ArcSight Field	Vendor Field
Name	'Sysmon service state changed'
Message	'Sysmon service state changed'
Device Receipt Time	UtcTime
Device Action	State
Additional Data.Schema Version	SchemaVersion

Event 5

ArcSight Field	Vendor Field
Name	'Process Terminated'
Message	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Device Action	'Process Terminated'

Event 7

ArcSight Field	Vendor Field
Name	'Image Loaded'
Message	Description
Device Receipt Time	UtcTime
Device Process Id	__safeToInteger(ProcessId)
File Id	ProcessGuid
Destination Process Name	Image
Device Custom String1	ImageLoaded
File Hash	Hashes
Old File Name	OriginalFileName
File Type	Signed
File Permission	SignatureStatus
Device Action	'Image Loaded'

Event 9

ArcSight Field	Vendor Field
Name	'RawAccessRead detected'
Message	'RawAccessRead detected'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Device Custom String 5	Device
Device Action	'RawAccessRead detected'

Event 10

ArcSight Field	Vendor Field
Name	'Process accessed'
Message	'Process accessed'
Device Receipt Time	UtcTime
Old File Id	SourceProcessGUID
Device Process Id	__safeToInteger(SourceProcessId)
Additional Data.Source Thread Id	SourceThreadId
Source Process Name	SourceImage
File Id	TargetProcessGUID
Destination Process Id	__safeToInteger(TargetProcessId)
Destination Process Name	TargetImage
Device Custom String1	GrantedAccess
Old File Path	CallTrace
Device Action	'Process accessed'

Event 11

ArcSight Field	Vendor Field
Name	'File created'
Message	'File created'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	ProcessId
Destination Process Name	Image
File Path	TargetFilename
File Create Time	CreationUtcTime
Device Action	'File Created'

Event 12

ArcSight Field	Vendor Field
Name	'Registry object added or deleted'
Message	'Registry object added or deleted'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	ProcessId
Destination Process Name	Image
File Path	TargetObject
Device Action	'Registry object added or deleted'

Event 13

ArcSight Field	Vendor Field
Name	'Registry value set'
Message	'Registry value set'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
File Path	TargetObject
Device Custom String 4	Details
Device Action	'Registry value set'

Event 15

ArcSight Field	Vendor Field
Name	'File stream created'
Message	'File stream created'
Device Receipt Time	UtcTime
File Id	ProcessGuid

ArcSight Field	Vendor Field
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
File Path	TargetFilename
File Create Time	CreationUtcTime
File Hash	Hash
Device Action	'File stream created'

Event 16

ArcSight Field	Vendor Field
Name	'Sysmon config state changed'
Message	'Sysmon config state changed'
Source Process Name	Configuration
File Hash	ConfigurationFileHash
Device Action	'Sysmon config state changed'
Device Receipt Time	UtcTime

Event 17

ArcSight Field	Vendor Field
Name	'Create Pipe'
Message	'Create Pipe'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Device Custom String 6	PipeName
Device Action	'Pipe Created'

Event 18

ArcSight Field	Vendor Field
Name	'Pipe Connected'
Message	'Pipe Connected'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Device Custom String 6	PipeName
Device Action	'Pipe Connected'

Event 22

ArcSight Field	Vendor Field
Name	'Dns query'
Message	'Dns query'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Device Process Id	__safeToInteger(ProcessId)
Destination Process Name	Image
Device Host Name	QueryName
Device Custom String 4	QueryResults
Device Action	'Dns query'

Event 255

ArcSight Field	Vendor Field
Name	'Error report'
Source Process Name	ID
Message	'Description
Device Receipt Time	UtcTime
Device Action	__stringConstant("Level : Error")

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!