Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Sysmon Logs

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

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
08/20/2020	Added support for Event ID 23 and Microsoft Sysmon version 11. Added and updated mappings for Event 3.
06/18/2020	Added support for Event 6, Event 8, Event 14, Event 19, Event 20, and Event 21. Added the 'Old File Hash - MITRE ID' mapping for Event 1, Event 2, Event 3, Event 5, Event 7, Event 9, Event 10, Event 11, Event 12, Event 13, Event 15, Event 17, Event 18, and Event 22. Added the 'Device Custom String 1 - EventType' mapping for Event 12, Event 13, Event 17, and Event 18.
05/21/2020	Updated the 'Device Host Name' field to 'Device Custom String 1' for Event 22.
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

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
- Microsoft Windows Server 2019

This connector supports Microsoft Sysmon Operational version 11 events.

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 **Custom Logs** field and enter **Microsoft-Windows-Sysmon/Operational**.

Mappings for Microsoft Sysmon Logs

General

ArcSight Field	Vendor Field
Destination Process Id	ProcessId
Device Product	'Sysmon'
Device Vendor	'Microsoft'
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Destination Process Name	Image
Destination Service Name	CommandLine
Device Action	'Process Create'
Device Custom String 1	IntegrityLevel
Device Custom String 6	LogonGuid
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
Message	Description
Name	'Process Created'
Old File Hash	MITRE ID
Old File Id	ParentProcessGuid
Old File Name	OriginalFileName

ArcSight Field	Vendor Field
Old File Path	CurrentDirectory
Source Nt Domain	__extractNTDomain(User)
Source Process Id	ParentProcessId
Source Process Name	ParentImage
Source Service Name	ParentCommandLine
Source User Id	LogonId
Source User Name	__extractNTUser(User)

Event 2

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File creation time changed'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File creation time changed'
Name	'File creation time changed'
Old File Create Time	PreviousCreationUtcTime
Old File Hash	MITRE ID

Event 3

ArcSight Field	Vendor Field
Destination Address	__oneOfAddress(DestinationIp) (for destination aware)
Device Custom IPv6 Address 2	__stringToIPv6Address(SourceIp) (for non-destination aware)
Device Custom IPv6 Address 3	__stringToIPv6Address(DestinationIp) (for non-destination aware)
Destination Host Name	DestinationHostname
Destination Port	__safeToInteger(DestinationPort)
Destination Process Name	Image

ArcSight Field	Vendor Field
Device Action	__concatenate("Initiated :",Initiated)
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Network connection detected'
Name	'Network connection detected'
Old File Hash	MITRE ID
Source Address	__oneOfAddress(SourceIp) (for destination aware)
Source Host Name	SourceHostname
Source Nt Domain	__extractNTDomain(User)
Source Port	__safeToInteger(SourcePort)
Source Port Name	SourcePortName
Source User Name	__extractNTUser(User)
Transport Protocol	Protocol

Event 4

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

Event 5

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid

ArcSight Field	Vendor Field
Message	'Process Terminated'
Name	'Process Terminated'
Old File Hash	MITRE ID

Event 6

ArcSight Field	Vendor Field
Device Action	'Driver Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	'Driver Loaded'
Name	'Driver Loaded'
Old File Hash	MITRE ID

Event 7

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Image Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	Description
Name	'Image Loaded'
Old File Hash	MITRE ID
Old File Name	OriginalFileName

Event 8

ArcSight Field	Vendor Field
Destination Process Name	TargetImage
Device Action	'CreateRemoteThread detected'
Device Process Id	SourceProcessId
Device Receipt Time	UtcTime
File Id	TargetProcessGuid
Message	'CreateRemoteThread detected'
Name	'CreateRemoteThread detected'
Old File Hash	MITRE ID
Old File Id	SourceProcessGuid
Source Process Name	SourceImage

Event 9

ArcSight Field	Vendor Field
Device Action	'RawAccessRead detected'
Device Custom String 5	Device
Device Receipt Time	UtcTime
Destination Process Name	Image
File Id	ProcessGuid
Message	'RawAccessRead detected'
Name	'RawAccessRead detected'
Old File Hash	MITRE ID

Event 10

ArcSight Field	Vendor Field
Additional Data.Source Thread Id	SourceThreadId
Destination Process Name	TargetImage
Device Action	'Process accessed'

ArcSight Field	Vendor Field
Device Custom String 1	GrantedAccess
Device Process Id	__safeToInteger(SourceProcessId)
Device Receipt Time	UtcTime
File Id	TargetProcessGUID
Message	'Process accessed'
Name	'Process accessed'
Old File Id	SourceProcessGUID
Old File Hash	MITRE ID
Old File Path	CallTrace
Source Process Name	SourceImage

Event 11

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

Event 12

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry object added or deleted'
Device Custom String 1	EventType
Device Receipt Time	UtcTime

ArcSight Field	Vendor Field
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry object added or deleted'
Name	'Registry object added or deleted'
Old File Hash	MITRE ID

Event 13

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry value set'
Device Custom String 1	EventType
Device Custom String 4	Details
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry value set'
Name	'Registry value set'
Old File Hash	MITRE ID

Event 14

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry key and value rename'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	NewName
Name	'Registry key and value rename'
Old File Hash	MITRE ID
Old File Path	TargetObject

Event 15

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File stream created'
Device Receipt Time	UtcTime
File Hash	Hash
File Id	ProcessGuid
File Create Time	CreationUtcTime
File Path	TargetFilename
Message	'File stream created'
Name	'File stream created'
Old File Hash	MITRE ID

Event 16

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

Event 17

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Created'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime

ArcSight Field	Vendor Field
File Id	ProcessGuid
Message	'Create Pipe'
Name	'Create Pipe'
Old File Hash	MITRE ID

Event 18

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Connected'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Pipe Connected'
Name	'Pipe Connected'
Old File Hash	MITRE ID

Event 19

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
Name	'WmiEventFilter activity detected'
Old File Hash	MITRE ID
Old File Path	EventNamespace
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 20

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
File Path	Destination
File Type	Type
Name	'WmiEventConsumer activity detected'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 21

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Filter
Device Custom String 5	Consumer
Device Receipt Time	UtcTime
Name	'WmiEventConsumerToFilter activity detected'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 22

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Dns query'

ArcSight Field	Vendor Field
Device Custom String 1	QueryName
Device Custom String 4	QueryResults
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Dns query'
Name	'Dns query'
Old File Hash	MITRE ID

Event 23

ArcSight Field	Vendor Field
Device Custom String 1	IsExecutable
Device Custom String 4	Archived
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Hash	Hashes
File Path	TargetFilename
Message	__concatenate("File has been deleted from ",__extractNTDomain(TargetFilename))
Name	'File Delete'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source Process Name	Image
Source User Name	__extractNTUser(User)

Event 255

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

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!