Micro Focus Security
ArcSight Connectors

SmartConnector for Windows Event Log – Native: Microsoft Windows Windows Update Client

Supplemental Configuration Guide

Document Release Date: June 19, 2019
Software Release Date: June 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

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
06/19/2019	First edition of this Configuration Guide, for initial support of tthese events.

Contents

SmartConnector for Microsoft Windows Event Log – Native: Windows-Windows Update Client

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Windows-Windows Update Client 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

Windows-Windows Update Client 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

Windows-Windows Update Client Configuration

For complete information about Microsoft's Reporting and Windows-Windows Update Client, 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 Windows-Windows Update Clien tLog, 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-WindowsUpdateClient

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft-Windows-WindowsUpdateClient'

Event 16

ArcSight Field	Vendor Field
Name	'Unable to Connect: Windows is unable to connect to the automatic updates service'

Event 17

ArcSight Field	Vendor Field
Name	'Installation Ready: The following updates are downloaded and ready for installation'

Event 18

ArcSight Field	Vendor Field
Name	'Installation Ready : The updates are downloaded and scheduled for installation'
Device Custom String 4 Label	stringConstant("Scheduled Install Date")
Device Custom String 4	schedinstalldate
Device Custom String 5 Label	stringConstant("Scheduled Install Time")

ArcSight Field	Vendor Field
Device Custom String 5	schedinstalltime
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 19

ArcSight Field	Vendor Field
Name	'Installation Successful: Window successfully installed the updates'
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 20

ArcSight Field	Vendor Field
Name	Installation Failure: Windows failed to install the Updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 21

ArcSight Field	Vendor Field
Name	Restart Required : The computer must be restarted
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 22

ArcSight Field	Vendor Field
Name	Restart Required : The computer will be restarted

Event 27

ArcSight Field	Vendor Field
Name	Automatic Updates is now paused

Event 28

ArcSight Field	Vendor Field
Name	Automatic Update is now resumed

Event 43

ArcSight Field	Vendor Field
Name	Installation Started: Windows has started installing the updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 44

ArcSight Field	Vendor Field
Name	Downloading Started: Windows Update started downloading an update
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")

ArcSight Field	Vendor Field
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

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!