Micro Focus Security ArcSight Connectors

SmartConnector for Windows Event Log – Native: MS Local Administrator Password Solution

Supplemental Configuration Guide

Document Release Date: August 21, 2019
Software Release Date: August 21, 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
08/21/2019	First edition of this Configuration Guide

Contents

SmartConnector for Microsoft Windows Event Log – Native: Local Administrator Password Solution

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Local Administrator Password Solution 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 Local Administrator Password Solution

Product Overview

MS Local Administrator Password Solution 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

MS Local Administrator Password Solution

For complete information about Microsoft's Reporting and MS Local Administrator Password Solution, 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 MS Local Administrator Password Solution, 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 Local Administrator Password Solution

Event 5

ArcSight Field	Vendor Field
Name	__ifThenElse(%1,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")
Message	__ifThenElse(%1,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")
Reason	%1

Event 10

ArcSight Field	Vendor Field
Name	__stringConstant("Password expiration too long for computer")
Message	__stringConstant("Password expiration too long for computer")
Device Action	__stringConstant("Resetting password now")
Device Custom Number 1	__safeToLong(%1)
Device Custom String1 Label	Excessive Days
Device Custom String2 Label	Days to change password

Event 11

ArcSight Field	Vendor Field
Name	__stringConstant("It is not necessary to change password yet")
Message	__stringConstant("It is not necessary to change password yet")
Device Custom Number 2	__safeToLong(%1)

Event 12

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been changed")
Message	__stringConstant("Local Administrator password has been changed")

Event 13

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been reported to AD")
Message	__stringConstant("Local Administrator password has been reported to AD")

Event 14

ArcSight Field	Vendor Field
Name	__stringConstant("Finished Successfully")
Message	__stringConstant("Finished Successfully")

Event 15

ArcSight Field	Vendor Field
Name	__stringConstant("Beginning Processing")
Message	__stringConstant("Beginning Processing")

Event 16

ArcSight Field	Vendor Field
Name	__stringConstant("Admin account management not enabled")
Message	__stringConstant("Admin account management not enabled")
Device Action	__stringConstant("Exiting")

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!