



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager Supplemental Configuration Guide**

Document Release Date: April 16, 2018

Software Release Date: April 16, 2018

## Legal Notices

Micro Focus  
The Lawn  
22-30 Old Bath Road  
Newbury, Berkshire RG14 1QN  
UK

<https://www.microfocus.com>

## Copyright Notice

© Copyright 2010-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services 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.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the US Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the US Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This US Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## 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: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

## Revision History

Date	Description
11/30/2016	Added Windows Server 2016 support.
02/15/2016	Added support for Windows 10 system events.
02/16/2015	First edition of this guide.

# Contents

SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager .....	7
Product Overview .....	7
Connector Installation and Configuration .....	7
Mappings for Windows 2016, 2012, 8, and 10 .....	8
General .....	8
7000 .....	8
7001 .....	8
7002 .....	9
7003 .....	9
7005 .....	9
7006 .....	9
7007 .....	9
7008 .....	10
7009 .....	10
7010 .....	10
7011 .....	10
7012 .....	10
7015 .....	10
7016 .....	11
7017 .....	11
7018 .....	11
7019 .....	11
7020 .....	11
7021 .....	11
7022 .....	12
7023 .....	12
7024 .....	12
7025 .....	12
7026 .....	12
7027 .....	13
7028 .....	13
7030 .....	13
7031 .....	13
7032 .....	14
7033 .....	14
7034 .....	14
7035 .....	14

7036 .....	15
7037 .....	15
7038 .....	15
7039 .....	16
7040 .....	16
7041 .....	16
7042 .....	16
7043 .....	17
7045 .....	17
Send Documentation Feedback .....	18

# SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager

This guide provides information about the SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager and its event mappings to ArcSight data fields.

Supported versions:

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The ***SmartConnector for Microsoft Windows Event Log – Native 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 the SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager.

## Product Overview

Service Control Manager (SCM) is a special system process under Windows NT family of operating systems that starts, stops, and interacts with Windows service processes. It is located in %SystemRoot%\System32\services.exe executable. Service processes interact with SCM through a well-defined API, and the same API interface is used internally by the interactive Windows service management tools such as the MMC snap-in Services.msc and the command-line Service Control utility sc.exe.

## 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 2016, 2012, 8, and 10

### General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

### 7000

ArcSight Field	Vendor Field
Name	'Service failed to start'
Message	'The 'param1' service failed to start due to error: 'param2''
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)
Reason	param2

### 7001

ArcSight Field	Vendor Field
Name	'A service depends on other service which failed to start'
Message	'The 'param1' service depends on the 'param2' service which failed to start because of error: 'param3''
Destination Service Name	param1
Source Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3



## 7002

ArcSight Field	Vendor Field
Name	'The 'param1' service depends on the 'param2' group and no member of this group started'
Destination Service Name	param1

## 7003

ArcSight Field	Vendor Field
Name	'A service depends on a nonexistent service'
Message	'The 'param1' service depends on a nonexistent service 'param2''
Destination Service Name	param1
Source Service Name	param2

## 7005

ArcSight Field	Vendor Field
Name	'The 'param1' call failed with error 'param2'
Device Custom String 4	Param2 (Reason or Error Code)

## 7006

ArcSight Field	Vendor Field
Name	'The 'param1' call failed for 'param2' with the following error 'param3''
Device Action	param2 (action)
Device Custom String 4	Param3 (Reason or Error Code)

## 7007

ArcSight Field	Vendor Field
Name	'The system reverted to its last known good configuration'
Message	'The system is restarting'

## 7008

ArcSight Field	Vendor Field
Name	'No backslash is in the account name'

## 7009

ArcSight Field	Vendor Field
Name	'Timeout waiting for the service to connect'
Message	'Timeout 'param1' waiting for the 'param2' service to connect'
Destination Service Name	param2

## 7010

ArcSight Field	Vendor Field
Name	'Timeout waiting for ReadFile'

## 7011

ArcSight Field	Vendor Field
Name	'Timeout waiting for a transaction response from the 'param2' service'
Destination Service Name	param2

## 7012

ArcSight Field	Vendor Field
Name	'Message returned in transaction has incorrect size'

## 7015

ArcSight Field	Vendor Field
Name	'Boot-start or system-start driver 'param1' must not depend on a service'

7016

ArcSight Field	Vendor Field
Name	'The 'param1' service has reported an invalid current state'
Destination Service Name	param1

7017

ArcSight Field	Vendor Field
Name	'Detected circular dependencies demand starting 'param1''
Destination Service Name	param1

7018

ArcSight Field	Vendor Field
Name	'Detected circular dependencies auto-starting services'

7019

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a service in a group which starts later.'
Destination Service Name	param1

7020

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a group which starts later'
Destination Service Name	param1

7021

ArcSight Field	Vendor Field
Name	'About to revert to the last known good configuration because the 'param1' service failed to start'
Destination Service Name	param1

## 7022

ArcSight Field	Vendor Field
Name	'The 'param1' service hung on starting'
Destination Service Name	param1

## 7023

ArcSight Field	Vendor Field
Name	'A service terminated with error.'
Message	The 'param1' service terminated with the following error 'param2'
Destination Service Name	param1
Reason	param2
Device Custom String 4	param2 (Reason or Error Code)

## 7024

ArcSight Field	Vendor Field
Name	'The 'param1' service terminated with the following service-specific error'
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)

## 7025

ArcSight Field	Vendor Field
Name	'At least one service or driver failed during system startup'
Message	'Use Event Viewer to examine the event log for details'

## 7026

ArcSight Field	Vendor Field
Name	'The boot-start or system-start driver(s) did not load'
Message	'The following boot-start or system-start driver(s) did not load: 'param1''
Device Process Name	param1

## 7027

ArcSight Field	Vendor Field
Name	'Windows could not be started as configured'
Message	'A previous working configuration was used instead'

## 7028

ArcSight Field	Vendor Field
Name	'The 'param1' Registry key denied access to SYSTEM account programs'
Message	'The Service Control Manager took ownership of the Registry key'
File Name	param1

## 7030

ArcSight Field	Vendor Field
Name	'The 'param1' service is marked as an interactive service'
Destination Service Name	param1
Message	'The system is configured to not allow interactive services. This service may not function properly.'

## 7031

ArcSight Field	Vendor Field
Name	Both ('The 'param1,' service terminated unexpectedly')
Destination Service Name	param1 (service name)
Message	Both ('The 'param1,' service terminated unexpectedly. It has done this 'param2,' time(s). The following corrective action will be taken in 'param3,' milliseconds: 'param5')
Device Action	param5 (action)

## 7032

ArcSight Field	Vendor Field
Name	'The Service Control Manager tried to take a corrective action 'param1' after the unexpected termination of the 'param2' service'
Device Action	param1
Message	'This action failed with error'
Destination Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)

## 7033

ArcSight Field	Vendor Field
Name	'The Service Control Manager did not initialize successfully'
Message	'The security configuration server (scserv.dll) failed to initialize with error 'param1'. The system is restarting.'
Device Custom String 4	param1 (Reason or Error Code)

## 7034

ArcSight Field	Vendor Field
Name	'A service terminated unexpectedly'
Message	'It has done this 'param2' times'
Destination Service Name	param1
Device Custom Number 3	param2 (Count)

## 7035

ArcSight Field	Vendor Field
Name	'The 'param1' service was successfully sent a 'param2' control'
Destination Service Name	param2

## 7036

ArcSight Field	Vendor Field
Name	'Service entered the 'param2" state'
Message	The 'param1' service entered the 'param2' state.'
Destination Service Name	param1
Device Action	param2

## 7037

ArcSight Field	Vendor Field
Name	'The Service Control Manager encountered an error undoing a configuration change to the 'param1' service'
Message	'The service's 'param2' is currently in an unpredictable state. If you do not correct this configuration, you may not be able to restart the 'param1' service or may encounter other errors. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1

## 7038

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to the following error: 'param3'. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

## 7039

ArcSight Field	Vendor Field
Name	'A service process other than the one launched by the Service Control Manager connected when starting the 'param1' service'
Destination Service Name	param1
Message	'The Service Control Manager launched process 'param2' and process 'param3' connected instead. Note that if this service is configured to start under a debugger, this behavior is expected.'

## 7040

ArcSight Field	Vendor Field
Name	'Start type of 'param1' service was changed from 'param2' to 'param3''
Message	'Start type of 'param1' service was changed from 'param2' to 'param3''
Destination Service Name	param1
Device Action	param3

## 7041

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password.'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	'Logon failure: the user has not been granted the requested logon type at this computer'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to error. This service account does not have the necessary user right 'Log on as a service''
Reason	'Logon failure: the user has not been granted the requested logon type at this computer'

## 7042

ArcSight Field	Vendor Field
Name	'A service was successfully sent a control'
Destination Service Name	param1 (service name)



ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Message	'The 'param1' service was successfully sent a 'param2' control. The reason specified was 'param3' ['param4'] Comment: 'param5'
Reason	Both('param3','param4')

## 7043

ArcSight Field	Vendor Field
Name	'The 'param1' service did not shutdown properly after receiving a preshutdown control'
Destination Service Name	param1

## 7045

ArcSight Field	Vendor Field
Name	'A service was installed in the system'
Destination Service Name	ServiceName
File Path	ImagePath
Device Custom String 5	StartType
Device Custom String 6	AccountName

# 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](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!