



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight Connectors**

SmartConnector for Windows Event Log –  
Unified: Microsoft Service Control Manager

Supplemental Configuration Guide

May 15, 2013

## Supplemental Configuration Guide

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

May 15, 2013

Copyright © 2010 – 2013 Hewlett Packard Enterprise Development LP

#### Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

#### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP 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.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

## Revision History

---

Date	Description
05/15/2013	Updated mappings for event 7045.
03/29/2013	First edition of this guide.

---

## Contents

Product Overview .....	5
Connector Installation and Configuration .....	5
Windows 2012/Windows 8 .....	5
General .....	5
Basic Service Control Manager Operations .....	5
7005 .....	5
7006 .....	6
7007 .....	6
7008 .....	6
7010 .....	6
7012 .....	6
7015 .....	6
7018 .....	6
7025 .....	6
7026 .....	6
7027 .....	7
7028 .....	7
7033 .....	7
Service Control Manager Basic Service Operations .....	7
7009 .....	7
7011 .....	7
7016 .....	7
7021 .....	7
7030 .....	8
7035 .....	8
7036 .....	8
7037 .....	8
7040 .....	8
Service Control Manager Service Start Operations .....	9
7000 .....	9
7001 .....	9
7002 .....	9
7003 .....	9
7017 .....	9
7019 .....	10
7020 .....	10

7022.....	10
7038.....	10
7039.....	10
7041.....	10
Service Control Manager Service Stop Operations.....	11
7023.....	11
7024.....	11
7031.....	11
7032.....	11
7034.....	12
7042.....	12
7043.....	12
7045.....	12

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

This guide provides information about the SmartConnector for Windows Event Log – Unified: Microsoft Service Control Manager and its event mappings to ArcSight data fields. Microsoft Windows 2012/Windows 8 events are supported.

The *ArcSight SmartConnector Mappings to Windows Security Events* 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 – Unified: 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 – Unified](#), selecting **Microsoft Windows Event Log – Unified** as the connector to be configured. During installation, select **true** for the **System Logs** field for system events to be collected.

### Windows 2012/Windows 8

#### General

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

### Basic Service Control Manager Operations

#### 7005

ArcSight Field	Vendor Field
Name	'The call failed with error'
Device Custom String 4	Reason or Error Code

**7006**

ArcSight Field	Vendor Field
Name	'The call failed with the following error'
Device Action	action
Device Custom String 4	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'

**7010**

ArcSight Field	Vendor Field
Name	'Timeout waiting for ReadFile'

**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 must not depend on a service'

**7018**

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

**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) failed to load'
Message	'The following boot-start or system-start driver(s) failed to load'
Device Process Name	process name

**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 Registry key denied access to SYSTEM account programs'
Message	'The Service Control Manager took ownership of the Registry key'

**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. The system is restarting.'
Device Custom String 4	Reason or Error Code

**Service Control Manager Basic Service Operations****7009**

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

**7011**

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

**7016**

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

**7021**

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

## 7030

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

## 7035

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

## 7036

ArcSight Field	Vendor Field
Name	'Service entered a state'
Message	'The service entered the state. The Windows Modules Installer service entered the running state. The Windows Modules Installer service entered the stopped state. The Win HTTP Web Proxy Auto-Discovery Service entered the running state. The Win HTTP Web Proxy Auto-Discovery Service entered the stopped state.'
Destination Service Name	service name
Device Action	action

## 7037

ArcSight Field	Vendor Field
Name	'The Service Control Manager encountered an error undoing a configuration change to the service'
Message	'The service is currently in an unpredictable state. If you do not correct this configuration, you may not be able to restart the 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	service name

## 7040

ArcSight Field	Vendor Field
Name	'The start type of the service was changed'
Message	'Start type of service was changed'
Destination Service Name	service name
Device Action	action



## Service Control Manager Service Start Operations

### 7000

ArcSight Field	Vendor Field
Name	'Service failed to start'
Message	'The service failed to start due to error'
Destination Service Name	service name
Device Custom String 4	Reason or Error Code
Reason	Reason or Error Code

### 7001

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

### 7002

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

### 7003

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

### 7017

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

**7019**

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

**7020**

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

**7022**

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

**7038**

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

**7039**

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

**7041**

ArcSight Field	Vendor Field
Name	'Service was unable to log on with the currently configured password.'
Destination Service Name	service name
Destination User Name	user name

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

## Service Control Manager Service Stop Operations

### 7023

ArcSight Field	Vendor Field
Name	'Service terminated.'
Message	'The service terminated with the following error'
Destination Service Name	service name
Reason	Reason or Error Code

### 7024

ArcSight Field	Vendor Field
Name	'The service terminated with service-specific error'
Destination Service Name	service name
Device Custom String 4	Reason or Error Code
Reason	Reason or Error Code
Message	'The service terminated with service-specific error'

### 7031

ArcSight Field	Vendor Field
Name	'A service terminated unexpectedly'
Destination Service Name	service name
Message	'The service terminated unexpectedly. It has down this x times. The following corrective action will be taken in x milliseconds.'
Device Action	action

### 7032

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

**7034**

ArcSight Field	Vendor Field
Name	'A service terminated unexpectedly'
Message	'It has done this x times'
Destination Service Name	service name
Device Custom Number 3	Count

**7042**

ArcSight Field	Vendor Field
Name	'A service was successfully sent a control'
Destination Service Name	service name
Device Custom String 4	Reason or Error Code
Message	'The service was successfully sent a control. The reason specified was'

**7043**

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

**7045**

ArcSight Field	Vendor Field
Name	'A service was installed in the system'
Destination Service Name	service name
File Path	file path
File Type	file type
Device Custom String 5	Service Start Type
Device Custom String 6	Service Account