



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Windows Event Log – Native: Microsoft SQL Server Audit**

### **Supplemental Configuration Guide**

Document Release Date: August 30, 2018

Software Release Date: August 30, 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
07/15/2017	Added support for Microsoft SQL Server 2016 event collection.
06/30/2016	Added mappings for security event 18454.
02/15/2016	Added mappings for security events 17811, 49916, and 49917.
11/17/2015	Added support for Microsoft SQL Server 2014 event collection. Updated SQL Server Audit configuration information and mappings.
05/15/2015	Added support for Microsoft SQL Server 2012 SP1 event collection.
02/16/2015	First edition of this Configuration Guide, for initial support of MS SQL Server Audit application events with the Microsoft Windows Event Log -- Native connector.

# Contents

SmartConnector for Windows Event Log – Native: Microsoft SQL Server Audit .....	8
Product Overview .....	8
SQL Server Audit Configuration .....	8
Customize Event Source Mapping .....	9
Connector Installation and Configuration .....	9
Collect Events from the Event Log .....	9
Microsoft SQL Server Audit Application Event Log Mappings .....	10
General .....	10
Event 615 .....	10
Event 849 .....	10
Event 852 .....	10
Event 919 .....	10
Event 958 .....	11
Event 1486 .....	11
Event 1814 .....	11
Event 1945 .....	11
Event 2007 .....	12
Event 2812 .....	12
Event 3406 .....	12
Event 3407 .....	13
Event 3408 .....	13
Event 3421 .....	13
Event 3454 .....	13
Event 5084 .....	14
Event 5579 .....	14
Event 5701 .....	14
Event 5703 .....	14
Event 6253 .....	15
Event 6527 .....	15
Event 8128 .....	15
Event 9013 .....	15
Event 9666 .....	16
Event 9688 .....	16
Event 9689 .....	16
Event 10981 .....	16
Event 12288 .....	16
Event 12291 .....	17

Event 15268 .....	17
Event 15457 .....	17
Event 15477 .....	17
Event 17069 .....	17
Event 17101 .....	18
Event 17103 .....	18
Event 17104 .....	18
Event 17107 .....	18
Event 17108 .....	18
Event 17110 .....	19
Event 17111 .....	19
Event 17115 .....	19
Event 17125 .....	19
Event 17126 .....	20
Event 17136 .....	20
Event 17137 .....	20
Event 17147 .....	20
Event 17148 .....	20
Event 17152 .....	21
Event 17162 .....	21
Event 17164 .....	21
Event 17176 .....	22
Event 17177 .....	22
Event 17199 .....	22
Event 17201 .....	22
Event 17550 .....	23
Event 17551 .....	23
Event 17561 .....	23
Event 17656 .....	23
Event 17658 .....	24
Event 17663 .....	24
Event 17811 .....	24
Event 18453 .....	24
Event 18454 .....	25
Event 18456 .....	25
Event 18488 .....	25
Event 18496 .....	25
Event 19030 .....	26
Event 19031 .....	26
Event 19032 .....	26
Event 26018 .....	26

Event 26022 .....	26
Event 26037 .....	27
Event 26048 .....	27
Event 26067 .....	27
Event 26076 .....	28
Event 30090 .....	28
Event 33090 .....	28
Event 33204 .....	28
Event 33205 .....	28
Event 33217 .....	30
Event 33218 .....	30
Event 49903 .....	30
Event 49904 .....	30
Event 49910 .....	30
Event 49916 .....	31
Event 49917 .....	31
 Send Documentation Feedback .....	 32

# SmartConnector for Windows Event Log – Native: Microsoft SQL Server Audit

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

Event collection is supported as follows:

Microsoft Windows Server Version	Microsoft SQL Server Version
2008, 2008 R2	2008, 2012
2012	2012 SP1, 2014, 2016

*SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* 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 SQL Server Audit.

## Product Overview

With SQL Server 2008, Microsoft introduced an SQL Server Audit feature that provides a true auditing solution for enterprise customers. While SQL Trace can be used to satisfy many auditing needs, SQL Server Audit offers a number of advantages that can help DBAs more easily achieve their goals, such as meeting regulatory compliance requirements.

The SQL Server Audit feature is intended to replace SQL Trace as the preferred auditing solution. SQL Server Audit is meant to provide full auditing capabilities and only auditing capabilities, unlike SQL Trace, which is also used for performance debugging.

## SQL Server Audit Configuration

For complete information about auditing in SQL Server, see Microsoft's SQL Server documentation at [https://msdn.microsoft.com/en-us/library/cc280525\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/cc280525(v=sql.120).aspx). This link takes you to the SQL Server 2014 version. You can select another version from the **Other Versions** drop down menu, but the basic steps are the same for sending audit events to an application log. From the left pane at this link, click **Create a Server Audit** and **Server Audit Specification** for detailed instructions.

Using SQL Server Management Studio, create a server audit as follows:

1. In Object Explorer, expand the **Security** folder.
2. Right-click the **Audits** folder and select **New Audit** to open a **Create Audit** window.



3. Enter a name for your audit (for example, **LoginFailed**). For **Audit destination**, select **Application Log** from the list.
4. Click **OK** to accept the default settings and save the new audit specification.
5. The new audit will appear in the **Audits** folder. To enable the audit, select the audit you created, right-click, and select **Enable Audit**.

## Customize Event Source Mapping

See the *Configuration Guide for the SmartConnector for Microsoft Windows Event Log – Native* for complete information about customizing event source mapping.

## 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.

## Collect Events from the Event Log

To set up the connector to collect application events:

1. From \$ARCSIGHT\_HOME\current\bin, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select **Navigate to the Modify table parameters** window.
5. To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **SQL Server Audit** in the **Custom Log Names** field.
6. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
7. Select **Exit** and click **Next** to exit the configuration wizard.
8. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*.

## Microsoft SQL Server Audit Application Event Log Mappings

### General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Destination User Name	""

### Event 615

ArcSight Field	Vendor Field
Name	'Could not find database'
Message	'Could not find database ID '%1', name '%2,'

### Event 849

ArcSight Field	Vendor Field
Name	'Using locked pages for buffer pool'
Message	'Using locked pages for buffer pool'

### Event 852

ArcSight Field	Vendor Field
Name	'Using conventional memory in the memory manager'
Message	'Using conventional memory in the memory manager'

### Event 919

ArcSight Field	Vendor Field
Name	'User is changing database script level'
Message	'User '%1,' is changing database script level entry '%2,' to a value of '%3'

ArcSight Field	Vendor Field
Source User Name	%1
Device Custom Number 1	%2 (Level entry)
Device Custom Number 2	%3 (Changed value)

## Event 958

ArcSight Field	Vendor Field
Name	'The resource database build version'
Message	'The resource database build version is '%1
Device Custom String 4	%1 (Database build version)

## Event 1486

ArcSight Field	Vendor Field
Name	'Database Mirroring Transport is disabled in the endpoint configuration'
Message	'Database Mirroring Transport is disabled in the endpoint configuration'

## Event 1814

ArcSight Field	Vendor Field
Name	'Could not create tempdb'
Message	'Could not create tempdb. You may not have enough disk space available.'

## Event 1945

ArcSight Field	Vendor Field
Name	'Warning! The maximum key length'
Message	One of (Warning! The maximum key length for a "%1," index is "%2," bytes. The index "%3," has maximum length of "%4," bytes. For some combination of large values, the insert/update operation will fail.), (Warning! The maximum key length is "%1," bytes. The index "%2," has maximum length of "%3," bytes. For some combination of large values, the insert/update operation will fail.)
Device Custom String 1	Both (One of (%2, %1), 'bytes') (Maximum key length)

ArcSight Field	Vendor Field
Device Custom String 2	One of (%3,%2) (Index)
Device Custom String 3	Both (One of (%4, %3), 'bytes') (Maximum index)
Device Custom String 4	%1 (Index Type)

## Event 2007

ArcSight Field	Vendor Field
Name	'The module depends on the missing object'
Message	'The module '%1,' depends on the missing object '%2,'. The module will still be created; however, it cannot run successfully until the object exists.'
Device Custom String 1	%1 (Module)
Device Custom String 2	%2 (Missing object)

## Event 2812

ArcSight Field	Vendor Field
Name	'Could not find stored procedure'
Message	'Could not find stored procedure '%1
Device Custom String 2	%1 (Stored procedure)

## Event 3406

ArcSight Field	Vendor Field
Name	'Transactions rolled forward in database'
Message	%1' transactions rolled forward in database '%2, '(';%3,'
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

## Event 3407

ArcSight Field	Vendor Field
Name	'Transactions rolled back in database'
Message	%1,' transactions rolled back in database '%2,' (%3;)'
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

## Event 3408

ArcSight Field	Vendor Field
Name	'Recovery is complete'
Message	'Recovery is complete. This is an informational message only. No user action is required.'

## Event 3421

ArcSight Field	Vendor Field
Name	'Recovery completed for database'
Message	'Recovery completed for database '%1,' (database ID '%2;') in '%3; second(s) (analysis '%4; ms, redo '%5; ms, undo '%6; ms.)'
Device Custom String 1	%1 (Database name)
Device Custom String 2	%4 ms (Analysis time)
Device Custom String 3	%5 ms (Redo time)
Device Custom String 4	%6 ms (Undo time)
Device Custom String 5	%3 s (Completed recovery time)
Device Custom String 6	%2 (Database ID)

## Event 3454

ArcSight Field	Vendor Field
Name	'Recovery is writing a checkpoint in database.'
Message	'Recovery is writing a checkpoint in database '%1,' (%2;)'

ArcSight Field	Vendor Field
Device Custom String 1	%1 (Database name)
Device Custom Number 1	%2 (Database ID)

## Event 5084

ArcSight Field	Vendor Field
Name	'Setting database option'
Message	'Setting database option '%1,' to '%2,' for database '%3,''
Device Custom String 1	%3 (Database name)
Device Custom String 2	%1 (Old option)
Device Custom String 3	%2 (New option)

## Event 5579

ArcSight Field	Vendor Field
Name	'File system access'
Message	'#FILESTREAM: effective level = '%1,', configured level = '%2,', file system access share name = '%3,''

## Event 5701

ArcSight Field	Vendor Field
Name	'Changed database context'
Message	'Changed database context to '%1'
Device Custom String 1	%1 (Database name)
Device Action	'Changed'

## Event 5703

ArcSight Field	Vendor Field
Name	'Changed language setting'
Message	'Changed language setting to '%1'
Device Custom String 1	%1 (Language setting)
Device Action	'Changed'

## Event 6253

ArcSight Field	Vendor Field
Name	'Common language runtime (CLR) functionality initialized using CLR'
Message	'Common language runtime (CLR) functionality initialized using CLR version '%1,' from '%2'
File Path	%2
Device Custom String 4	%1 (File version)

## Event 6527

ArcSight Field	Vendor Field
Name	'.NET Framework runtime has been stopped'
Message	'.NET Framework runtime has been stopped'

## Event 8128

ArcSight Field	Vendor Field
Name	'Execute extended stored procedure.'
Message	'Using '%1,' version '%2,' to execute extended stored procedure '%3.'. This is an informational message only; no user action is required.'
File Name	%1
Device Custom String 3	%2 (File version)
Device Custom String 4	%3 (Extended stored procedure)

## Event 9013

ArcSight Field	Vendor Field
Name	'Tail of the log for database is being rewritten'
Message	'Tail of the log for database '%1,' is being rewritten to match the new sector size of '%2,' bytes. '%3,' bytes at offset '%4,' in file '%5,' will be written'

## Event 9666

ArcSight Field	Vendor Field
Name	'Service endpoint is in disabled or stopped state'
Message	'The ',%1,' endpoint is in disabled or stopped state'
Destination Service Name	%1

## Event 9688

ArcSight Field	Vendor Field
Name	'Service Broker manager has started'
Message	'Service Broker manager has started'

## Event 9689

ArcSight Field	Vendor Field
Name	'Service Broker manager has shut down'
Message	'Service Broker manager has shut down'

## Event 10981

ArcSight Field	Vendor Field
Name	'Resource governor reconfiguration succeeded'
Message	'Resource governor reconfiguration succeeded'

## Event 12288

ArcSight Field	Vendor Field
Name	'Package started'
File Name	%1



## Event 12291

ArcSight Field	Vendor Field
Name	'Package failed'
File Name	%1

## Event 15268

ArcSight Field	Vendor Field
Name	'Authentication mode'
Message	'Authentication mode is '%1
Device Custom String 3	%1 (Authentication mode)

## Event 15457

ArcSight Field	Vendor Field
Name	'Configuration option changed'
Message	'Configuration option '%1,' changed from '%2,' to '%3,'. Run the RECONFIGURE statement to install'
Device Custom String 3	%1 (Configuration option)
Device Custom Number 1	%2 (Old value)
Device Custom Number 2	%3 (New value)

## Event 15477

ArcSight Field	Vendor Field
Name	'Caution: Changing any part of an object name could break scripts and stored procedures'
Message	'Caution: Changing any part of an object name could break scripts and stored procedures'

## Event 17069

ArcSight Field	Vendor Field
Name	'Microsoft SQL Server 2012 (SP1)'
Message	%1

## Event 17101

ArcSight Field	Vendor Field
Name	'Microsoft Corporation'
Message	'Microsoft Corporation'

## Event 17103

ArcSight Field	Vendor Field
Name	'All rights reserved'
Message	'All rights reserved'

## Event 17104

ArcSight Field	Vendor Field
Name	'Server process ID'
Message	'Server process ID is ',%1
Destination Process ID	%1

## Event 17107

ArcSight Field	Vendor Field
Name	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'
Message	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'

## Event 17108

ArcSight Field	Vendor Field
Name	'Password policy update was successful'
Message	'Password policy update was successful'
Device Action	'Update'

## Event 17110

ArcSight Field	Vendor Field
Name	'Registry startup parameters'
Message	'Registry startup parameters' ;%1
Device Custom String 1	%1 (Parameters)

## Event 17111

ArcSight Field	Vendor Field
Name	'Logging SQL Server messages'
Message	'Logging SQL Server messages in file' ;%1
File Name	%1

## Event 17115

ArcSight Field	Vendor Field
Name	'Command Line Startup'
Message	'Command Line Startup Parameters: ' ;%1
Device Action	'Startup'
Device Custom String 1	%1 (Parameters)

## Event 17125

ArcSight Field	Vendor Field
Name	'Using dynamic lock allocation'
Message	'Using dynamic lock allocation. Initial allocation of ' ;%1,' Lock blocks and ' ;%2,' Lock Owner blocks per node'
Device Custom Number 1	%1 (Lock blocks)
Device Custom Number 2	%2 (Lock owner blocks)

## Event 17126

ArcSight Field	Vendor Field
Name	'SQL Server is now ready for client connections'
Message	'SQL Server is now ready for client connections'

## Event 17136

ArcSight Field	Vendor Field
Name	'Clearing tempdb database'
Message	'Clearing tempdb database'

## Event 17137

ArcSight Field	Vendor Field
Name	'Starting up database'
Message	'Starting up database ',%1
Device Custom String 1	%1 (Database name)

## Event 17147

ArcSight Field	Vendor Field
Name	'SQL Server is terminating because of a system shutdown'
Message	'SQL Server is terminating because of a system shutdown. This is an informational message only. No user action is required.'

## Event 17148

ArcSight Field	Vendor Field
Name	'SQL Server is terminating'
Message	'SQL Server is terminating in response to a 'stop' request from Service Control Manager'

## Event 17152

ArcSight Field	Vendor Field
Name	'Node configuration'
Message	'Node configuration: node '%1,' CPU mask: '%2,' '%3,' Active CPU mask: '%4,' '%5,'. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.'
Device Custom String 2	%1 (Node)
Device Custom String 3	%2 (CPU mask)
Device Custom String 4	%4 (Active CPU mask)
Device Custom String 5	%3 (Flag CPU mask)
Device Custom String 6	%5 (Flag Active CPU mask)

## Event 17162

ArcSight Field	Vendor Field
Name	'SQL Server is starting'
Message	'SQL Server is starting at normal priority base (=7)'

## Event 17164

ArcSight Field	Vendor Field
Name	'SQL Server detected sockets'
Message	'SQL Server detected '%1,' sockets with '%2,' cores per socket and '%3,' logical processors per socket, '%4,' total logical processors; using '%5,' logical processors based on SQL Server licensing. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected sockets)
Device Custom Number 2	%2 (Cores per socket)
Device Custom Number 3	%3 (Processors per socket)
Device Custom String 3	%4 (Total processors)
Device Custom String 4	%5 (Using processors)

## Event 17176

ArcSight Field	Vendor Field
Name	'This instance of SQL Server last reported using a process ID'
Message	'This instance of SQL Server last reported using a process ID of '%1,' at '%2,' (local) '%3,' (UTC). This is an informational message only; no user action is required.'
Destination Process ID	%1
Device Custom Date 1	%2, 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (local))
Device Custom Date 2	%3 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (UTC))

## Event 17177

ArcSight Field	Vendor Field
Name	'This instance of SQL Server has been using a process ID'
Message	'This instance of SQL Server has been using a process ID of '%1,' since '%2,' (local) '%3,' (UTC). '

## Event 17199

ArcSight Field	Vendor Field
Name	'Restart SQL Server using the trace flag'
Message	'Dedicated administrator connection support was not started because it is disabled on this edition of SQL Server. If you want to use a dedicated administrator connection, restart SQL Server using the trace flag '%1.'. This is an informational message only. No user action is required.'
Device Custom Number 1	%1 (Trace flag)

## Event 17201

ArcSight Field	Vendor Field
Name	'Dedicated admin connection support was established'
Message	'Dedicated admin connection support was established for listening locally on port '%1'
Destination Port	%1

## Event 17550

ArcSight Field	Vendor Field
Name	'DBCC TRACEON, server process'
Message	'DBCC TRACEON '%1,' server process ID (SPID) '%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' %1
Destination Process ID	%2

## Event 17551

ArcSight Field	Vendor Field
Name	'DBCC TRACEOFF, server process'
Message	'DBCC TRACEOFF '%1,' server process ID (SPID) '%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' %1
Destination Process ID	%2

## Event 17561

ArcSight Field	Vendor Field
Name	'index restored'
Message	'index restored for '%2,' '%3'
Device Custom String 1	%2 (Report server database)
Device Custom String 3	%3 (Object name)

## Event 17656

ArcSight Field	Vendor Field
Name	'Warning'
Message	'Warning*****'

## Event 17658

ArcSight Field	Vendor Field
Name	'SQL Server started in single-user mode'
Message	'SQL Server started in single-user mode. This is an informational message only. No user action is required.'

## Event 17663

ArcSight Field	Vendor Field
Name	'Server name'
Message	'Server name is ',%1
Destination Host Name	%1

## Event 17811

ArcSight Field	Vendor Field
Name	'The maximum number of dedicated administrator connections for this instance'
Message	'The maximum number of dedicated administrator connections for this instance is ',%1,''
Device Custom Number 1	%1 (Maximum administrator connections)

## Event 18453

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using Windows authentication'
Destination User Name	%1
Destination NT Domain	%1
Device Custom String 1	%2 (Windows authentication)



## Event 18454

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using SQL Server authentication'
Source User Name	%1
Source Address	%2
Device Custom IPv6 Address 2	%2 (Source IPv6 Address)

## Event 18456

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user '%1.' '%2' '%3
Device Custom String 3	%2 (Login failed)
Source User Name	%1
Source Address	%3

## Event 18488

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user '%1.' Reason: The password of the account must be changed. '%2
Source User Name	%1
Source Address	%2

## Event 18496

ArcSight Field	Vendor Field
Name	'System Manufacturer and System Model Information'
Message	'System Manufacturer: '%1,' System Model: '%2,'
Device Custom String 1	%1 (System Manufacturer)
Device Custom String 2	%2 (System Model)

## Event 19030

ArcSight Field	Vendor Field
Name	'SQL Trace was started'
Message	'SQL Trace ID '%1,' was started by login '%2,''
Device Custom String 1	%1 (Trace ID)
Source User Name	%2

## Event 19031

ArcSight Field	Vendor Field
Name	'SQL Trace stopped'
Message	'SQL Trace stopped. Trace ID = '%1,'. Login Name = '%2'
Source User Name	%2

## Event 19032

ArcSight Field	Vendor Field
Name	'SQL Trace was stopped due to server shutdown'
Message	'SQL Trace was stopped due to server shutdown. Trace ID = '%1,'. This is an informational message only; no user action is required.'
Device Custom Number 1	%1 (Trace ID)

## Event 26018

ArcSight Field	Vendor Field
Name	'A self-generated certificate was successfully loaded for encryption'
Message	'A self-generated certificate was successfully loaded for encryption'

## Event 26022

ArcSight Field	Vendor Field
Name	'Server is listening'
Message	'Server is listening on [%1,' < '%2,' > '%3,']'

ArcSight Field	Vendor Field
Device Custom String 4	%1 (Listening Address)
Application Protocol	%2
Destination Port	%3

## Event 26037

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Server Principal Name'
Message	'Error: ', '%1,', state: ', '%2,', Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos'

## Event 26048

ArcSight Field	Vendor Field
Name	'Server local connection provider is ready to accept connection'
Message	'Server local connection provider is ready to accept connection on [, '%1,']'
File Path	%1

## Event 26067

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Service Principal Name (SPN)'
Message	'The SQL Server Network Interface library could not register the Service Principal Name (SPN) ', '%1,', for the SQL Server service. Windows return code: ', '%2,', state: ', '%3,', Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This is an informational message. Further action is only required if Kerberos authentication is required by authentication policies and if the SPN has not been manually registered.'
Source Service Name	%1
Reason	%2
Device Custom String 1	%3 (State)

## Event 26076

ArcSight Field	Vendor Field
Name	'SQL Server is attempting to register a Service Principal Name (SPN)'
Message	'SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.'

## Event 30090

ArcSight Field	Vendor Field
Name	'New instance of full-text filter daemon host process has been successfully started.'
Message	'A new instance of the full-text filter daemon host process has been successfully started.'

## Event 33090

ArcSight Field	Vendor Field
Name	'Attempting to load library into memory'
Message	'Attempting to load library '%1,' into memory. This is an informational message only. No user action is required'
File Name	%1

## Event 33204

ArcSight Field	Vendor Field
Name	'SQL Server Audit could not write to the security log'
Message	'SQL Server Audit could not write to the security log'

## Event 33205

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Event Class ID	All of (class_type, 'I', action_id)
Device Action	action_id
Event Outcome	succeeded

ArcSight Field	Vendor Field
File ID	object_id
File Type	class_type
File Name	object_name
File Size	sequence_number
File Hash	audit_schema_version
Old File ID	transaction_id
Message	statement
Source User ID	server_principal_id
Source User Name	server_principal_name
Source NT Domain	server_principal_name
Destination User ID	One of (server_principal_id, target_server_principal_id)
Destination NT Domain	One of (target_server_principal_name, server_principal_name)
Destination Host Name	server_instance_name
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	statement
Device Custom String 3	database_name
Device Custom String 4	Device Custom String 4 = database_principal_name
Device Custom String 5	One of (target_database_principal_name, database_principal_name)
Device Custom String 6	schema_name
Old File Name	All of (Additional Information : , additional_information)
Source Address	One of (additional_information, device address (In case the address is local machine))
Source Host Name	device host name (In case the address is local machine)
Destination User Name	One Of (target_server_principal_name, server_principal_name)
Device Custom IPv6 Address 2	additional_information

## Event 33217

ArcSight Field	Vendor Field
Name	'SQL Server Audit is starting the audits'
Message	'SQL Server Audit is starting the audits. This is an informational message. No user action is required.'

## Event 33218

ArcSight Field	Vendor Field
Name	'SQL Server Audit has started the audits'
Message	'SQL Server Audit has started the audits. This is an informational message. No user action is required.'

## Event 49903

ArcSight Field	Vendor Field
Name	'Detected RAM'
Message	'Detected '%1,' of RAM. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected RAM)

## Event 49904

ArcSight Field	Vendor Field
Name	'Service account'
Message	'The service account is '%1,'. This is an informational message; no user action is required.'
Source Service Name	%1

## Event 49910

ArcSight Field	Vendor Field
Name	'Software Usage Metrics is disabled'
Message	'Software Usage Metrics is disabled'

## Event 49916

ArcSight Field	Vendor Field
Name	'UTC adjustment'
Message	'UTC adjustment.'
Device Custom String 1	All of 1%, ; 2% (UTC Adjustment)

## Event 49917

ArcSight Field	Vendor Field
Name	'Default collation'
Message	All of 'Default collation';%1,' (%2,';%3,')'
Device Custom String 1	%2 (Language)
Device Custom String 4	%1 (SQL collation)
Device Custom Number 2	%3 (Language 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 )**

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!