
Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.2.0

SmartConnector for Microsoft Audit Collection System DB

Document Release Date: May 2021

Software Release Date: May 2021



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 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.

U.S. 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 U.S. 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 U.S. 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 U.S. 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 U.S. 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:

<https://www.microfocus.com/support-and-services/documentation>

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

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

SmartConnector for Microsoft Audit Collection System DB	5
Product Overview	5
Supported Versions	6
Configuration	6
Installing and Configuring Microsoft Audit Collection Services	6
Deploying Audit Collection Services	6
Downloading the JDBC Driver	7
Add a JDBC Driver to the Connector Appliance/ArcSight Management Center	8
Configure the JDBC Driver and Windows Authentication	9
Installing the SmartConnector	10
Prerequisites	10
Installing Core Software	11
Installing JDBC Driver	11
For the Connector Appliance or ArcSight Management Center	12
Configuring the JDBC Driver and Windows Authentication	13
Configuring the Connector	13
Run the SmartConnector	14
Device Event Mapping to ArcSight Fields	16
Microsoft ACS with Operations Manager 2007-2012 Mappings	16
Microsoft Auditing Collection System Mappings	17
Troubleshooting	19
Send Documentation Feedback	21

SmartConnector for Microsoft Audit Collection System DB

This guide provides information to install the SmartConnector for Microsoft Audit Collection System DB and configuring the device for event collection.

Product Overview

The Microsoft Audit Collection System (ACS) offers a solution to the problem of security log management. With ACS, audit events are securely sent to a central repository in real time and are stored in an SQL database.

In Operations Manager, you can use Audit Collection Services (ACS) to collect records generated by an audit policy and store them in a centralized database. By default, when an audit policy is implemented on a Microsoft Windows computer, that computer automatically saves all events generated by the audit policy to its local Security log. This is so for Windows workstations as well as servers.



With ACS, only a user who has specifically been given the right to access the ACS database can run queries and create reports on the collected data.

In Operations Manager 2007, the deployment of ACS involves the following:

ACS Forwarders

The service that runs on ACS forwarders is included in the Operations Manager agent. By default, this service is installed but not enabled when the Operations Manager agent is installed. You can enable this service for multiple agent computers at once using the Enable Audit Collection task. After you enable this service, all security events are sent to the ACS collector in addition to the local Security log.

ACS Collector

The ACS collector receives and processes events from ACS forwarders and then sends this data to the ACS database. This processing includes disassembling the data so that it can be spread across several tables within the ACS database, minimizing data redundancy, and applying filters so that unnecessary events are not added to the ACS database.

ACS Database

The ACS database is the central repository for events that are generated by an audit policy within an ACS deployment. The ACS database can be located on the same computer

as the ACS collector, but for best performance, each should be installed on a dedicated server.

The server that hosts the ACS database must have Microsoft SQL Server 2005 or Microsoft SQL Server 2008. You can choose an existing or new installation of SQL Server. The Enterprise edition is recommended by Microsoft because of the stress of daily ACS database maintenance.

Supported Versions

Microsoft ACS with Operations Manager 2007, 2007 R2, 2012, and 2012 R2 are supported.



This connector does not retrieve the fields 'String07 - String22' fields in the dtEvent tables in the interest of high performance SQL Query. These fields often are not populated by the ACS collector and do not contain any significant pieces of information when they are populated. However, String01 through String06 are mapped to the Device Custom String fields. See the Event Mappings section for more detail. All the remaining important fields in the dtEvent tables are retrieved into the ArcSight fields.



In high throughput environments, if the connector is shut down for extended periods of time, a large number of events can collect which can clog the connector on restart. This condition can be avoided by setting preservestate to false. See the Troubleshooting section for instructions on setting preservestate.

Configuration

Installing and Configuring Microsoft Audit Collection Services

For complete information about installation and configuration requirements for Microsoft ACS, see <http://technet.microsoft.com/en-us/library/bb381258.aspx>

Deploying Audit Collection Services

To deploy ACS:

- 1 Plan an audit policy for your organization.

- 2 Plan your ACS server deployment, including deciding which server will act as the ACS database and which Operations Manager 2007 Management Server will act as the ACS collector.
- 3 Plan which Operations Manager agents will be ACS forwarders. All computers from which you want to collect security events must be ACS forwarders.
- 4 Install and configure prerequisites for ACS components.
- 5 (Optional). Separate administrator and auditor roles by doing the following:
 - A Create a local group just for users who access and run reports on the data in the ACS database. (See [Creating user and group accounts.](#))
 - B Grant the newly created local group access to the SQL database by creating a new SQL Login for the group and assigning that login the db_datareader permission. (See [Creating a SQL Login.](#))
 - C Add the user accounts of users who will act as auditors to the local group.
- 6 Deploy the ACS Database and ACS Collector or Collectors. See "How to Install an ACS Collector and Database" at <http://technet.microsoft.com/en-us/library/bb381258.aspx> for complete information.
- 7 Run the **Enable Audit Collection** task to start the ACS Forwarder service on the ACS forwarders. For more information, see <http://technet.microsoft.com/en-us/library/bb381258.aspx>.
- 8 Implement your audit policy within your organization.

Downloading the JDBC Driver

During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you download to a SmartConnector folder. For information about and to download the MS SQL Server JDBC Driver, see:

<http://msdn.microsoft.com/en-us/sqlserver/aa937724>



Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

When you download the JDBC driver, the version of the jar file depends on the version of the JRE the connector uses:

- Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Prior versions, which run JRE 1.6, require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

Install the driver.

For software connectors, copy the jar file appropriate for your SQL Server version from the installation folder for the SQL Server JDBC driver to a temporary location; you will copy this file to \$ARCSIGHT_HOME/current/user/agent/lib, (where \$ARCSIGHT_HOME refers to the SmartConnector installation folder, such as c:\ArcSight\SmartConnectors) after the core SmartConnector software has been installed at step 3 of Install the SmartConnector. Copy only the jar file associated with the version of the driver to be installed to this location.

Add a JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as described in this section.

- 1 From the Connector Appliance/ArcSight Management Center, select **Setup -> Repositories**.
- 2 Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
- 3 Click **Upload to Repository**.
- 4 From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
- 5 Retain the default selection and click **Next**.
- 6 Click **Upload** and locate and select the .jar file you downloaded in step 3 of SmartConnector Installation.
- 7 Click **Submit** to add the specified file to the repository and click **Next** to continue.
- 8 After adding all files you require, click **Next**.
- 9 In the **Name** field, enter a descriptive name for the zip file (JDBCdriver, for example). Click **Next**.

- 10 Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
- 11 To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
- 12 Select the container or containers into which the driver is to be uploaded; click **Next**.
- 13 Click **Done** to complete the process.
- 14 Add the connector through the Connector Appliance/ArcSight Management Center interface; see the *Connector Appliance/ArcSight Management Center Online Help* for detailed information. Descriptions of parameters to be entered during connector configuration are provided in the "Install the SmartConnector" section of this guide.

Configure the JDBC Driver and Windows Authentication

This section provides guidance on how to use a JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only. As previously described, download the SQL JDBC drivers from Microsoft and install the driver before beginning this procedure.



The JDBC driver does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

Microsoft Type 4 JDBC drivers (versions 4.0 or later) support integrated authentication. Windows Authentication works only when using one of these drivers. You also will need to add `;integratedSecurity=true` to the JDBC URL entry for the connection to your database.

- 1 Copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory. For example, the JDBC driver download path for SQL JDBC driver version 4.0 for 32-bit environment would be `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll` and, for 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`.



When upgrading a connector, the `$ARCSIGHT_HOME\jre\bin` directory is overwritten; therefore, you will need to copy the authentication file to this folder again after update.

- 2 Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.

- 3 When entering the connector parameters, in the **JDBC Database URL** field, append `;integratedSecurity=true` to the end of the URL string.

The following is an example; note that the name or instance of the database configured at installation/audit time should be used.

```
jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true
```

- 4 Complete the remaining connector wizard configuration steps.
- 5 After completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should login to the database. The Connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends you do not install database connectors on the database server or any mission critical servers as this might cause performance issues.

Prerequisites

- Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly. For more information, see [ArcSight Documentation](#) page.
- If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at [Configuring the SmartConnector](#).
- Make sure that you have the following:
 - Local access to the machine where the SmartConnector is to be installed
 - Administrator passwords
- Download the MS SQL Server JDBC Driver. For more information, see: <http://msdn.microsoft.com/en-us/sqlserver/aa937724>



Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file might be different for some JDBC driver versions.

Refer to the following table to download the JDBC driver and the jar files depending on the JRE version that the connector uses:

JAR File Version	JRE Version	JAR File Name
7.2.1 and later	1.8	sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
7.1.2 and later	1.7	sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
Earlier versions	1.6	sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

Installing Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.
- 3 Follow the wizard to complete the installation of the core connector software, then exit the wizard.

Installing JDBC Driver

For Software Connectors

1. Copy the jar file that is appropriate for your SQL Server version from the installation folder for the SQL Server JDBC driver to `$ARCSIGHT_HOME/current/user/agent/lib`, (where `$ARCSIGHT_HOME` refers to the SmartConnector installation folder, for example: `c:\ArcSight\SmartConnectors`).
2. Copy the only jar file that is associated with the version of the driver to be installed to this location.

For the Connector Appliance or ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as described in the following section:

- 1 From the Connector Appliance/ArcSight Management Center, select **Setup > Repositories**.
- 2 Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
- 3 Click **Upload to Repository**.
- 4 From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
- 5 Retain the default selection and click **Next**.
- 6 Click **Upload** and locate and select the .jar file you downloaded in step 3 of SmartConnector Installation.
- 7 Click **Submit** to add the specified file to the repository and click **Next** to continue.
- 8 After adding all files you require, click **Next**.
- 9 In the **Name** field, enter a descriptive name for the zip file (JDBCdriver, for example). Click **Next**.
- 10 Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
- 11 To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
- 12 Select one or more containers into which you want to upload the driver, then click **Next**.
- 13 Click **Done** to complete the process.
- 14 Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.



Refer to the Installing and Configuring the SmartConnector section to know more about the descriptions of parameters to be entered during connector configuration.

Configuring the JDBC Driver and Windows Authentication

This section provides guidance on how to use a JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only.



The JDBC driver does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

Microsoft Type 4 JDBC drivers (versions 4.0 or later) support integrated authentication. Windows Authentication works only when using one of these drivers.

Copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory. For example, the JDBC driver download path for SQL JDBC driver version 4.0 for 32-bit environment would be `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll` and, for 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`.



When upgrading a connector, the `$ARCSIGHT_HOME\jre\bin` directory is overwritten; therefore, you will need to copy the authentication file to this folder again after update.

Configuring the Connector

1. Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.
2. Specify the relevant [Global Parameters](#), when prompted.
3. From the **Type** drop-down list, select **Microsoft Audit Collection System DB** as the type of connector, then click **Next**.
4. Select as the type of connector, then click **Next**.
5. Enter the following parameters to configure the SmartConnector, then click **Next**.

6.

Parameter	Description
JDBC Driver	Select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
JDBC URL	<p>Enter: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>;1433;DatabaseName=<MS SQL Server Database Name>', substituting actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.</p> <p>To configure JDBC Driver and Windows Authentication, add ;integratedSecurity=true to the JDBC URL entry for the connection to your database.</p> <p>For example, jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</p> <p>Note that the name or instance of the database configured at installation or audit time must be used.</p>
Database User	Enter the login name of the database user with database audit privilege.
Database Password	Enter the password for the database user.

7. Select a [destination and configure parameters](#).
8. Specify a name for the connector.
9. Select whether you want to [run the connector as a service or in the standalone mode](#).
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying parameters, see [SmartConnector User Guide](#).



When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the

platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter Ctrl+C in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft ACS with Operations Manager 2007-2012 Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit_failure; High = Error; Medium = Warning, Unknown; Low = Audit_success, Information
Destination Host Name	One of (EventMachine, DB_HOST)
Destination NT Domain	One of (PrimaryDomain, TargetDomain)
Destination Process Name	One of (PrimarySid, TargetSid)
Destination User ID	PrimaryLogonId
Destination User Name	One of (PrimaryUser, TargetUser)
Device Custom Date 1	CollectionTime
Device Custom Number 2	Id
Device Custom String 1	StringValue01
Device Custom String 2	StringValue02
Device Custom String 3	StringValue03
Device Custom String 4	StringValue04
Device Custom String 5	StringValue05
Device Custom String 6	StringValue06
Device Event Category	Source
Device Event Class ID	Both (Source, EventId)
Device External ID	_DB_CURRENT_TABLE_ID
Device Host Name	AgentMachine
Device NT Domain	HeaderDomain
Device Process Name	HeaderSid
Device Product	'Microsoft Auditing Collection System'
Device Receipt Time	CreationTime

ArcSight ESM Field	Device-Specific Field
Device Severity	Type (0=Unknown, 1=Error, 2=Warning, 4=Information, 8=Audit_succsss, 16=Audit_failure)
Device Vendor	'Microsoft'
Device Version	SCOM 2007/2012
External ID	SequenceNo
Name	One of (Category, 'ACS Event')
Source NT Domain	One of (ClientDomain, PrimaryDomain)
Source Process Name	ClientSid
Source User ID	ClientLogonId
Source User Name	One of (ClientUser, HeaderUser,PrimaryUser)

Microsoft Auditing Collection System Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit_failure; High = Error; Medium = Warning, Unknown; Low = Audit_success, Information)
Destination Host Name	AuditMachine
Destination NT Domain	One of (PrimaryDomain, TargetDomain)
Destination Process Name	One of (TargetSid, PrimaryUser)
Destination User ID	PrimaryLogonId
Destination User Name	One of (PrimaryUser, TargetUser)
Device Custom Date 1	CollectionTime
Device Custom Number 2	Id
Device Event Category	Source
Device Event Class ID	Both (Source, EventId)
Device Host Name	AgentMachine
Device NT Domain	HeaderDomain
Device Process Name	HeaderSid
Device Product	'Microsoft Auditing Collection System'
Device Receipt Time	CreationTime

ArcSight ESM Field	Device-Specific Field
Device Severity	Type (0=Unknown, 1=Error, 2=Warning, 4=Information, 8=Audit_success, 16=Audit_failure)
Device Vendor	'Microsoft'
Device Version	ACS
External ID	SequenceNo
Name	One of (Category, 'ACS Internal Event')
Source NT Domain	ClientDomain
Source Process Name	ClientSid
Source User ID	ClientLogonId
Source User Name	One of (ClientUser, HeaderUser)

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection.'"

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The `preservestate` parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting `preservestate` to disabled (false) in the `agent.properties` file allows the connector to skip the old events and start from real time. The `agent.properties` file is located in the `$ARCSIGHT_HOME\current\user\agent` folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require `sqljdbc42.jar`. Versions 7.1.2 and later use JRE 1.7 and require `sqljdbc41.jar`. Prior versions of the connector that run JRE 1.6 require `sqljdbc4.jar`.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 SmartConnector for Microsoft Audit Collection System DB (Micro Focus Security ArcSight Connectors 8.2.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!