
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Microsoft Audit Collection System DB SmartConnector

Document Release Date: February 2022

Software Release Date: February 2022



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2022 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

Contents

- Configuration Guide for SmartConnector for Microsoft Audit Collection System DB ... 5
- Product Overview 6
 - Supported Versions 7
- Configuration 8
 - Installing and Configuring Microsoft Audit Collection Services 8
 - Deploying Audit Collection Services 8
 - Downloading the JDBC Driver 9
- Installing the SmartConnector 10
 - Preparing to Install the SmartConnector 10
 - Installing and Configuring the SmartConnector 10
 - Adding JDBC Driver to the Connector Appliance/ArcSight Management Center 13
- Device Event Mapping to ArcSight Fields 14
 - Microsoft ACS with Operations Manager 2007-2012 Mappings 14
 - Microsoft Auditing Collection System Mappings 15
- Troubleshooting 17
- Send Documentation Feedback 19

Configuration Guide for 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.

This guide provides a high level overview of ArcSight SmartConnectors.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

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. Identify the server that will act as the ACS database and the Operations Manager 2007 Management Server that will act as the ACS collector.
3. Identify the Operations Manager agents that 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) Do the following to separate administrator and auditor roles:
 - a. [Create a local group](#) for users who access and run reports on the data in the ACS database.
 - 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.
 - c. Add 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

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.



Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar to mssql-jdbc-9.4.0.jre8.jar.
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

For more information and to download the MS SQL Server JDBC Driver, see [aa937724](#)

Installing the SmartConnector

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

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

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy the jar file associated with the version of the driver that you downloaded earlier to `$ARCSIGHT_HOME/current/user/agent/lib`
5. (Optional) To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory.

An example of The JDBC driver download path for SQL JDBC driver is:

- For version 4.0 for 32-bit environment is `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll`
- For 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`



Note: If you are upgrading the SmartConnector, you must copy the authentication file to `$ARCSIGHT_HOME\jre\bin` again after update, as the upgrade process overwrites the `$ARCSIGHT_HOME\jre\bin` directory.

6. To add JDBC Driver to ArcMC or Connector Appliance, see Adding JDBC Driver to the Connector Appliance/ArcSight Management Center.
 7. Copy certificate and JDBC files to SmartConnector folders as follows:
 - Copy the `jssecacerts` certificate that you installed during the device configuration to the SmartConnector installation folder `$ARCSIGHT_HOME/current/jre/lib/security`.
-
- Note:** You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.
- Copy the `vjdbc.jar` and `commons-logging-1.1.jar` files to the SmartConnector installation folder `$ARCSIGHT_HOME/current/user/agent/lib`. These files are located in the `lib` directory that was created when you downloaded the JDBC driver and unzipped the package.
 8. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup.bat` file to start the SmartConnector Configuration Wizard.
 9. Specify the relevant Global Parameters, when prompted.
 10. From the **Type** drop-down list, select **Microsoft Audit Collection System DB** as the type of connector, then click **Next**.
 11. Enter the following parameters to configure the SmartConnector, then click **Next**.

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

12. Select a destination and configure parameters.
13. Specify a name for the connector.
14. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.
15. Select whether you want to run the connector as a service or in the standalone mode.
16. Complete the installation.
17. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).



Note: 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.

Adding 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 required containers, as follows:

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.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (for example, JDBCdriver). 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*.

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
Device Severity	Type (0=Unknown, 1=Error, 2=Warning, 4=Information, 8=Audit_success, 16=Audit_failure)

Configuration Guide for Microsoft Audit Collection System DB SmartConnector

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
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`.

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 Configuration Guide for Microsoft Audit Collection System DB SmartConnector (SmartConnectors 8.3.0)

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!