Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft Audit Collection System DB

Configuration Guide

January 17, 2017

Configuration Guide

SmartConnector for Microsoft Audit Collection System DB

January 17, 2017

Warranty

Restricted Rights Legend

Revision History

Date	Description
01/17/2017	Updated mappings for Source User Name and Source NT Domain in the "Microsoft ACS with Operations Manager 2007-2012" table.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Removed ODBC support due to Java 8 implementation.
02/14/2014	Added support for Operations Manager 2012 R2.
09/30/2013	Updated "Create an ODBC Data Source" section and added troubleshooting information regarding connection failure.
12/21/2012	Added support for Microsoft System Center Operations Manager 2012 and updated mappings.
05/15/2012	Added new installation procedure.
02/15/2012	Added driver download information for Connector Appliance.

SmartConnector for Microsoft Audit Collection System DB

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

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.

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

Configuration

Deploy 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 prerequesites 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.

Download and Install a 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.

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.

Install 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 could cause performance issues.

Prepare to Install Connector

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

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. 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 "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

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

Install 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 HPE SSO and Protect 724 sites.

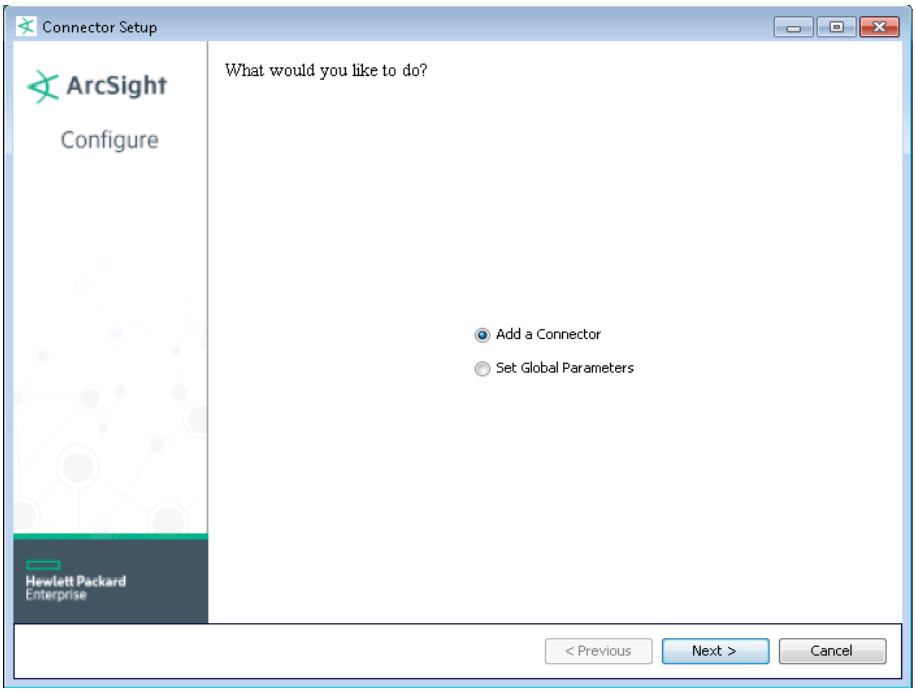
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction
Choose Install Folder
Choose Shortcut Folder
Pre-Installation Summary
Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:



Download SQL Server JDBC Driver

To download a Microsoft SQL Server JDBC driver, click **Cancel** to leave the configuration wizard at this point and copy the jar file you downloaded earlier (see "Download and Install a JDBC Driver") to `$ARCSIGHT_HOME/current/user/agent/lib`.

From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

Set Global Parameters (optional)

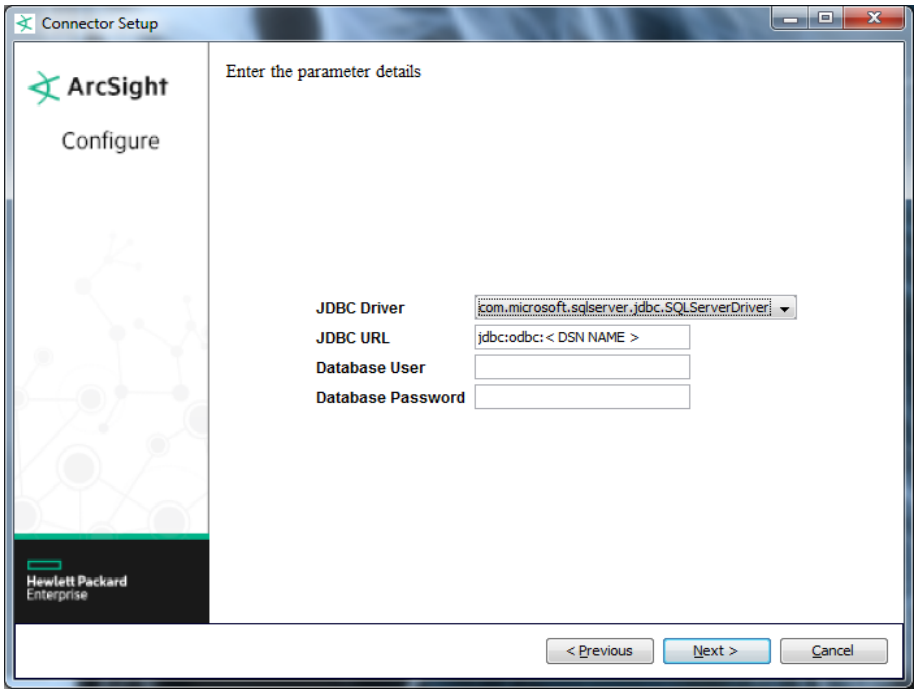
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'.
Remote management listener port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	If both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is IPv4.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **Microsoft Audit Collection System DB** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
JDBC Driver	Select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
JDBC URL	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>.
Database User	Enter the login name of the database user with database audit privilege.
Database Password	Enter the password for the database user.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.

4 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.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.

Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

For instructions about upgrading the connector or modifying parameters, see the *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
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')

ArcSight ESM Field	Device-Specific Field
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)
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 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.