



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft System Center
Operations Manager DB

Configuration Guide

October 17, 2017

Configuration Guide

SmartConnector for Microsoft System Center Operations Manager DB

October 17, 2017

Copyright © 2003 – 2017 Hewlett Packard Enterprise Development LP

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

<https://community.saas.hpe.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>.

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
07/15/2017	Updated JDBC download information.
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 System Center Operations Manager 2012 R2 on SQL Server 2012 and Windows Server 2012 R2. Updated parameter screen image.
09/30/2013	Updated "Create an ODBC Data Source" section and added troubleshooting information regarding connection failure.
11/15/2012	Added support for Systems Center Operations Manager 2012 on SQL Server 2008 and Windows Server 2008 R2 SP1.
06/30/2012	Split connector configuration guide for SQL Server 2000 support into a separate guide and marked support as Legacy. Support for SQL Server 2008 added to this connector.
05/15/2012	Added new installation procedure.
02/15/2012	Added driver download information for Connector Appliance.

Contents

Product Overview.....	4
Configuration.....	4
Download and Install a JDBC Driver.....	4
Configure the JDBC Driver and Windows Authentication.....	5
Install the SmartConnector.....	6
Prepare to Install Connector.....	6
Install Core Software.....	6
Download SQL Server JDBC Driver.....	7
Set Global Parameters (optional).....	7
Select Connector and Add Parameter Information.....	8
Select a Destination.....	9
Complete Installation and Configuration.....	10
Run the SmartConnector.....	10
Device Event Mapping to ArcSight Fields.....	10
Operations Manager 2012 Event Mappings.....	11
Operations Manager 2007 Event Mappings.....	11
Additional Mappings for Microsoft Forefront Client Security Events.....	12
Operations Manager 2005 Event Mappings.....	12
Troubleshooting.....	13

SmartConnector for Microsoft System Center Operations Manager DB

This guide provides information for installing the SmartConnector for Microsoft System Center Operations Manager DB and configuring the device for event collection. SQL Server versions 2005, 2007, 2008, and 2012 are supported with this connector. The following Operations Manager versions are supported:

Microsoft Operations Manager 2005
Microsoft System Center Operations Manager 2007
Microsoft System Center Operations Manager 2007 R2 on Windows Server 2003 R2
Microsoft Forefront Client Security v1.1 SP1 with MOM 2005
Microsoft System Center Operations Manager 2012 on Windows Server 2008 with SQL Server 2008
Microsoft System Center Operations Manager 2012 R2 on Windows Server 2012 R2 with SQL Server 2012

Product Overview

Microsoft Systems Center Operations Manager is designed to simplify monitoring and management of large, heterogeneous IT infrastructures.

Microsoft Forefront Client Security provides unified, easily managed malware protection for business desktops, laptops, and server operating systems. Forefront Client Security with Microsoft Operations Manager 2005 is supported.



The preferred Operations Manager setup method is to use SQL Server Authentication. The ODBC source you create on the machine where you install the SmartConnector must match the configuration of the SCOM setup authentication type; otherwise, the SmartConnector cannot successfully authenticate.

Configuration

This section provides instructions for configuring the Microsoft Systems Center Operations Manager Database to send events to the ArcSight SmartConnector.

If you are using the Audit Collection Services (ACS) agent with Operations Manager, use the SmartConnector for Microsoft Audit Collection System DB.

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.

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.

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

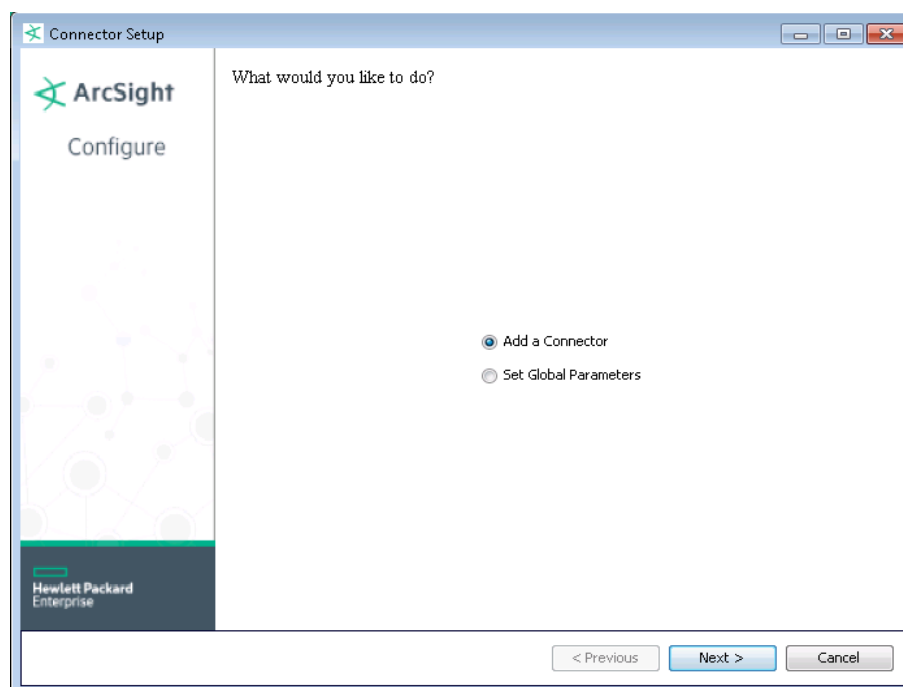
Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HPE SSO and Protect 724 sites.

- 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. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.
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	When 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. The initial setting is IPv4.

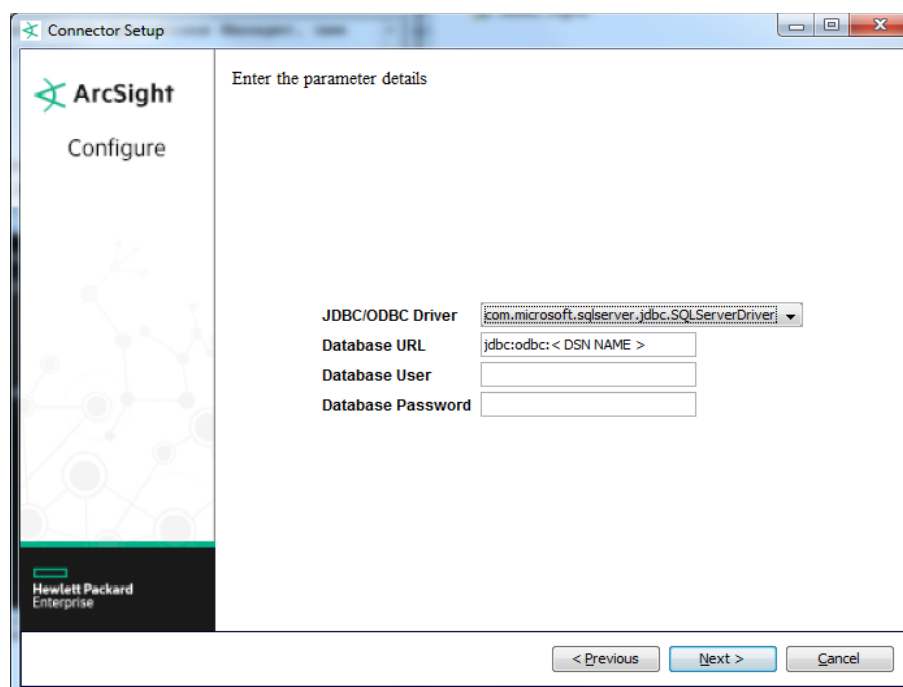
The following parameters should be configured only if you are using HPE SecureData solutions to provide encryption. See the *HPE SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the HPE SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The HPE SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for HPE SecureData.
Format Preserving Secret	Enter the secret configured for HPE SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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 Systems Center Operations Manager DB** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
JDBC/ODBC Driver	Select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
Database 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 user name of the MS SQL Server DB user with appropriate database privilege.
Database Password	Microsoft SCOM database URL password

The SmartConnector settings must match the settings you entered in the data source configuration for the machine upon which you are installing the SmartConnector.

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 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.

Due to limitations in event format in Operations Manager 2007, events cannot be further parsed by the Windows Event Log SmartConnector as is done with SCOM 2005.

Support for Microsoft Forefront Client Security events has been added; the mappings shown in the Forefront Client Security event mappings table are in addition to support for the same event mappings as for SCOM events.

Operations Manager 2012 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 3; Medium = 2; Low = 1
Destination Host Name	LoggingComputer
Destination NT Domain	extracted from EventUser
Destination User Name	extracted from EventUser
Device Custom Date 2	TimeAdded
Device Custom Number 2	Number (Windows Event Number)
Device Custom String 1	RuleName
Device Custom String 2	PublisherName (Event Source)
Device Custom String 3	RuleCategory
Device Custom String 5	ObjectFullName
Device Event Category	Channel
Device Event Class ID	Both (Channel, Number)
Device Host Name	LoggingComputer
Device Product	'Operations Manager'
Device Receipt Time	TimeGenerated
Device Severity	RulePriority
Device Vendor	'Microsoft'
External ID	EventId
Message	EventParameters
Name	RuleName

Operations Manager 2007 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 3; Medium = 2; Low = 1
Destination Host Name	LoggingComputer
Destination User ID	Destination User Name
Device Custom Date 2	TimeAdded
Device Custom Number 2	Number (Windows Event Number)
Device Custom String 1	RuleName
Device Custom String 2	PublisherName
Device Custom String 3	RuleCategory
Device Event Category	Channel
Device Event Class ID	Channel plus Number
Device Host Name	LoggingComputer
Device Product	'Microsoft Operations Manager 2007'
Device Receipt Time	TimeGenerated

ArcSight ESM Field	Device-Specific Field
Device Severity	RulePriority
Device Vendor	'Microsoft'
External ID	EventId
Message	EventParameters
Name	RuleName

Additional Mappings for Microsoft Forefront Client Security Events

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Issue Name
Device Custom String 3	Risk
Device Product	'Microsoft Forefront'
Device Severity	Severity
Name	extracted from Message field

Operations Manager 2005 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit Failure; High = Error; Medium = Warning; Low = Success, Information, Audit Success
Destination Host Name	ComputerName
Destination User ID	UserName
Device Custom Date 2	TimeStored
Device Custom Number 3	isAlerted
Device Custom String 1	EventId
Device Custom String 4	idEvent
Device Custom String 5	oneof (SourceName,"Unknown")
Device Custom String 6	SourceCategory
Device Event Category	ProviderName
Device Event Class ID	SourceName plus EventId
Device Host Name	ComputerName
Device Product	Microsoft Operations Manager 2005
Device Receipt Time	TimeGenerated
Device Severity	EventType
Device Vendor	Microsoft
File Name	MsgFileName
File Type	"Message File"
Message	Message
Name	Event name from Message field
Source Host Name	(Optional) SourceComputerName

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.