Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Microsoft SQL Server Multiple Instance Audit DB

Configuration Guide

November 30, 2016

Configuration Guide

SmartConnector for Microsoft SQL Server Multiple Instance Audit DB

November 30, 2016

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://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Removed ODBC support due to Java 8 implementation.
11/14/2014	Updated versions supported and ODBC data source configuration information.
06/30/2014	Added support for SQL Server 2014.
11/15/2013	Updated JDBC driver and Windows authentication information; updated parameter descriptions.
09/30/2013	Added troubleshooting information regarding connection failure.
08/15/2013	Added new mappings, a procedure for mounting a drive in Linux, hyperlinks to MS-SQL Server Column IDs and Event IDs, and the missing step in the MS-SQL Server installation.
06/28/2013	Updated procedure for changing the name of processed files and in troubleshooting not ready for processing file problem.
09/28/2012	Added support for SQL Server 2012.
06/30/2012	Updated 2005/2008 mappings for Device Host Name; added Event Outcome mapping; updated parameter entry screen.

Contents

SmartConnector for Microsoft SQL Server Multiple Instance Audit DB

This guide provides information for installing the SmartConnector for Microsoft SQL Server Multiple Instance Audit DB and configuring the device for audit log event collection via the SQL Trace mechanism. The following SQL Server versions are supported.

Microsoft SQL Server 2000 SP3, SP4, SP5 (C2 Auditing and General Trace Auditing)
Microsoft SQL Server 2005
Microsoft SQL Server 2008, R2, SP3
Microsoft SQL Server 2012
Microsoft SQL Server 2014

Event collection via SQL Server Audit mechanism for SQL Server 2008 is supported with the SmartConnector for Microsoft Windows Event Log – Unified.

Product Overview

Microsoft SQL Server provides auditing as a way to trace and record activity that has happened on each instance of SQL Server (for example, successful and failed logins). SQL Server also provides an interface (SQL Query Analyzer) for managing audit records.

There are two possible authentication methods that can be used with the SmartConnector for Microsoft SQL Server Audit DB – *Microsoft Windows Authentication* and *Mixed Mode Authentication* (which uses both SQL Server and Windows authentication). Although Microsoft recommends Windows Authentication, this document describes installing and configuring the SmartConnector using both methods of authentication.

Configuration Steps

Before installing the SmartConnector, perform the following configuration steps:

- Download a SQL Server JDBC driver (not necessary when using an ODBC data source).
- Mount a drive on Linux platforms.
- For SQL Server 2008, ensure TCP/IP connection is enabled.
- Create a Local SQL Server User.
- Share permissions for the database log folder.
- Create a Domain SQL Server User. This step is required for all authentication modes and operating system environments. System administrator privilege is required for SQL Server database access and for granting folder permissions.
- Enable Auditing.

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.

Mount a Drive on Linux Platforms

When installing the SmartConnector on Linux platforms, follow these steps to allow connector access to the trace files on the SQL Server machine.

To mount the drive:

1. Open a terminal window.
2. Execute the following commands:

   ```
   id <user>
   sudo mkdir <mount point>
   ```

   where you substitute:

   `<user>` with the username of the user running the connector
   `<mount point>` with the actual mount point on the Linux machine (for example, `/mnt/mssql`)

3. Execute the following command:

   ```
   sudo mount //<ipaddressOfSQLServer>/<sqltrace> <mount point> -o
   nosuid,uid=<uid>,gid=<guid>,username=<SQLServerusername>,password=<SQLSer
   verpassword>,rw
   ```

   where you substitute:

   `<sqltrace>` with the name of the shared drive containing the trace files
   `<uid>` and `<guid>` with information from execution of the commands in step 2
   `<SQLServerusername>` and `<SQLServerpassword>` with the actual Windows share user and password required to access the SQL Server.

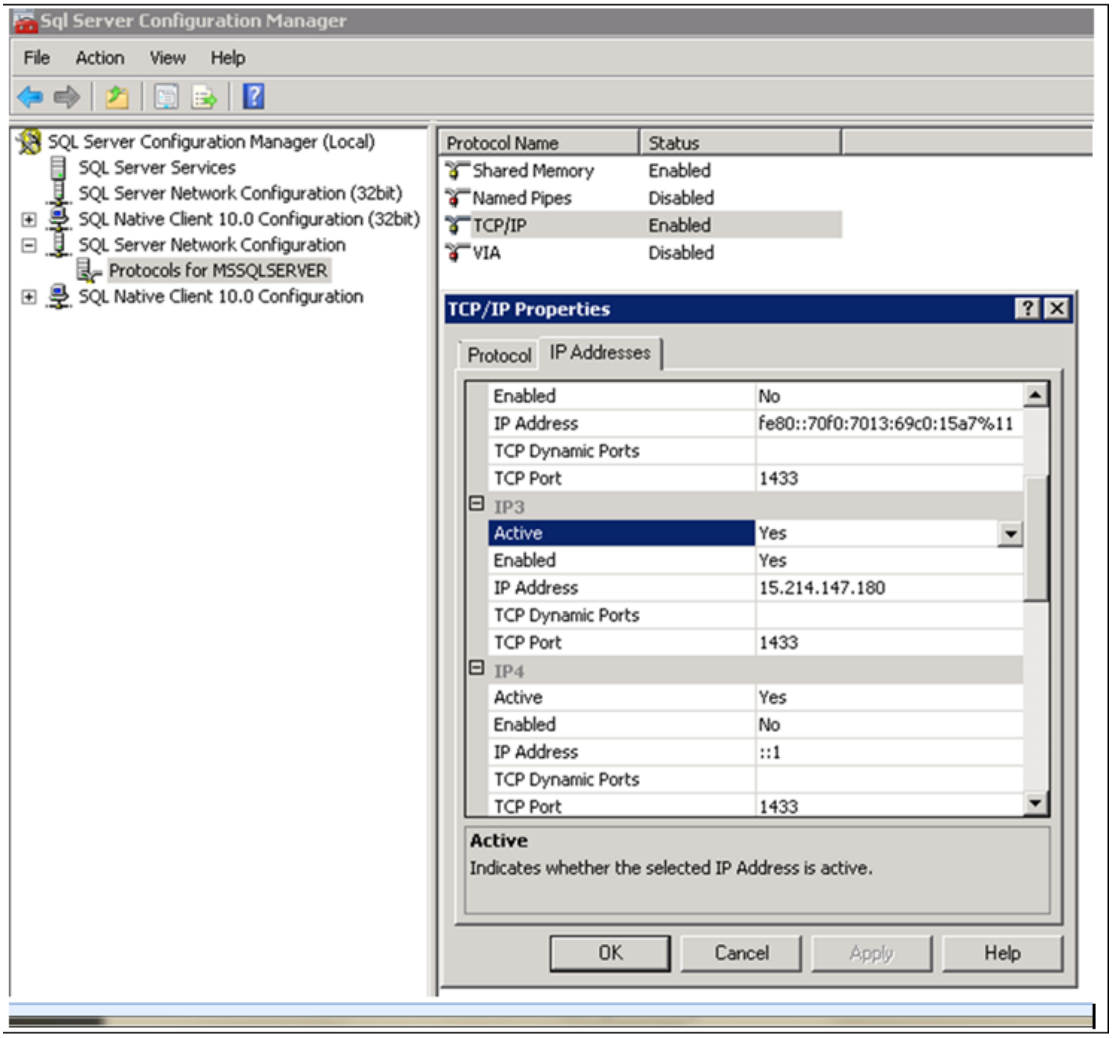
4. To verify the shared folder was successfully mounted, execute the following command:

   ```
   ls <mount point>
   ```

Ensure TCP/IP Connection is Enabled with SQL Server 2008

Connection to the SQL Server may be refused if the TCP/IP connection is not enabled. Use the following steps.

1. Open **Start -> All Programs -> Microsoft SQL Server 2008 R2 -> Configuration Tools -> SQL Server Configuration Manager**.
2. In the left pane, expand **SQL Server Network Configuration** and select **Protocols for [your server]**.
3. Double-click **TCP/IP** and ensure that the IP address you are using to connect to your SQL Server is active and enabled.



Create a Local SQL Server User

Instructions are provided for creating a local SQL Server user on SQL Server 2005 and later versions (2005, 2008, 2012, 2014). This step is required when using SQL Server Authentication.

To collect events using a non-administrative SQL Server 2005, 2008, 2012, or 2014 database account:

1. Right-click **Security > Logins** and select **New Login...** to create a new database user account named `sqlaudit`.
2. On the **General** tab, select **SQL Server authentication** and provide a password for `sqlaudit`.
3. Set the default database of this user to `master` (from the **User Mapping** tab, check the box in the **Map** column for the ***master database***).
4. Grant this user (`sqlaudit`) **Connect**, **Execute**, and **Select** permissions.
5. Enable the proxy account to the same user (`sqlaudit`). (`SQL Server -> Properties -> Security ->enable proxy account`)

6 Go to SQL Server -> Properties -> Permissions and grant the user permission to **Alter trace**.

Share Permissions for the Database Log Folder

A valid SQL Logon ID (either SQL user account or a Domain/Windows user account) must be used and granted specific database permissions.

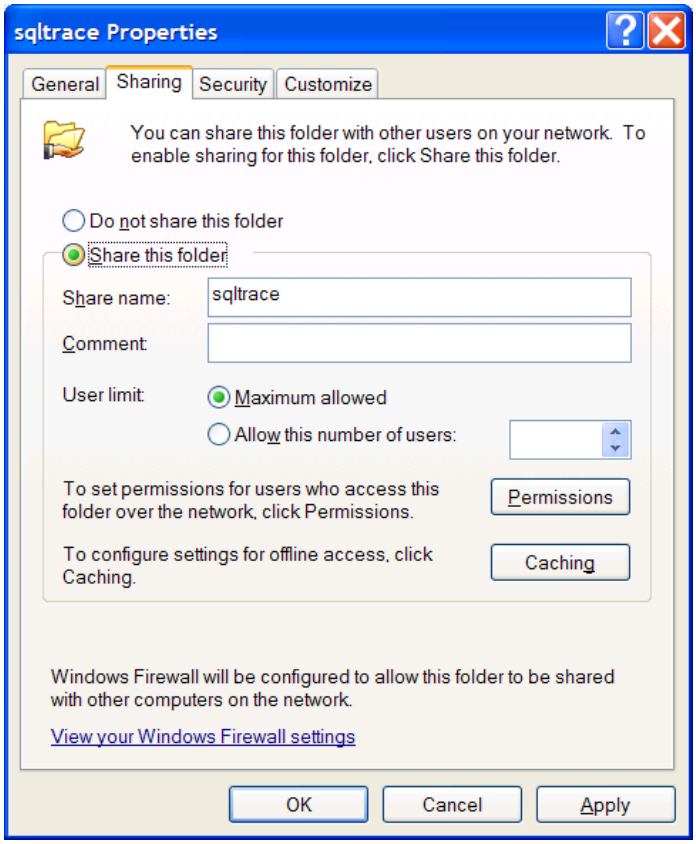
By default the Windows Service account is a local system account that will not have permission to access an SQL Server setup for Windows Authentication. So, for Windows Authentication to work, the SQL Audit Connector Service must run as a valid Windows account that has been granted permissions in the SQL Server.

To share permissions for the database log folder:

1 Log in to the SQL Server database machine.

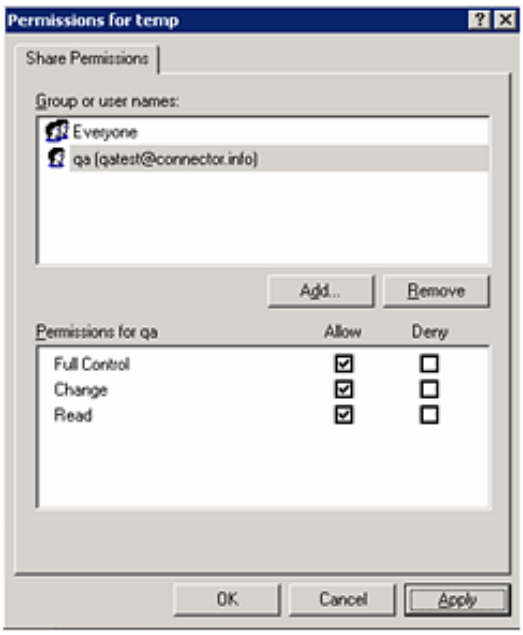
2 Right-click on the name of the log file folder (`sqltrace` in these examples); select **Properties**.

3 From the **Sharing** tab, select **Share this folder** and enter the name of the folder in the **Share name** field.



4 For **User limit**, keep the default value of **Maximum allowed** selected, or select **Allow this number of users** and select a value. Click **Apply**.

5 Click the **Permissions** button.



6 Click **Add** to add the user you created in "Create a Domain User from the Domain Controller."

7 Check **Allow** for **Full Control**, **Change**, and **Read** for this user; click **Apply**.

8 Click **OK** to exit the **Permissions** window.

9 Click the **Security** tab and select the Domain Controller user you created.

10 Give **Allow** permission for **Full Control** to this user.

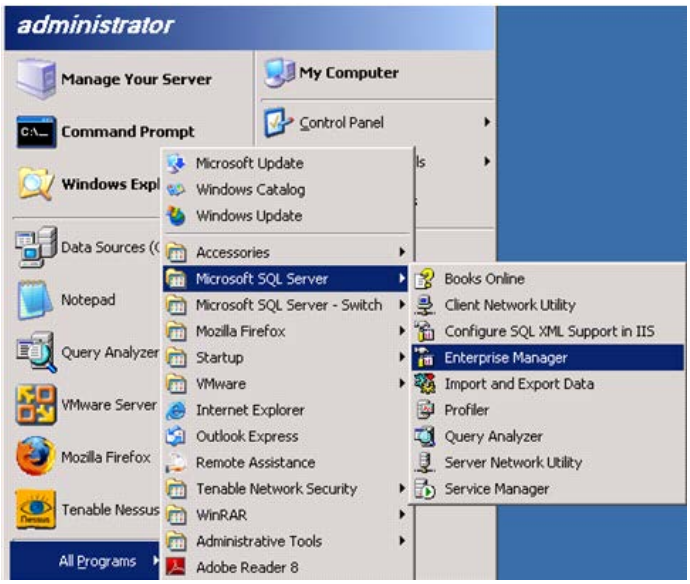
11 Click **Apply** and then **OK** to exit the **Properties** window.

Create a Domain User from the Domain Controller

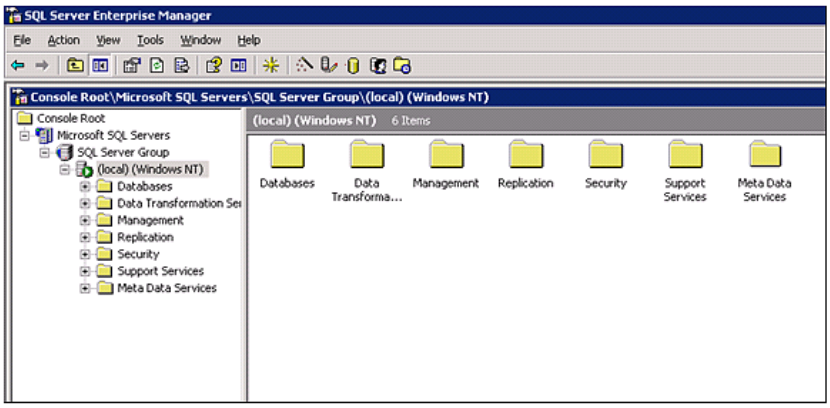
A valid SQL Logon ID (either SQL user account or a Domain/Windows user account) must be used and granted specific database permissions (see "Share Permissions for the Database Log Folder").

The following procedure depicts creating a user in a Windows environment with Windows authentication.

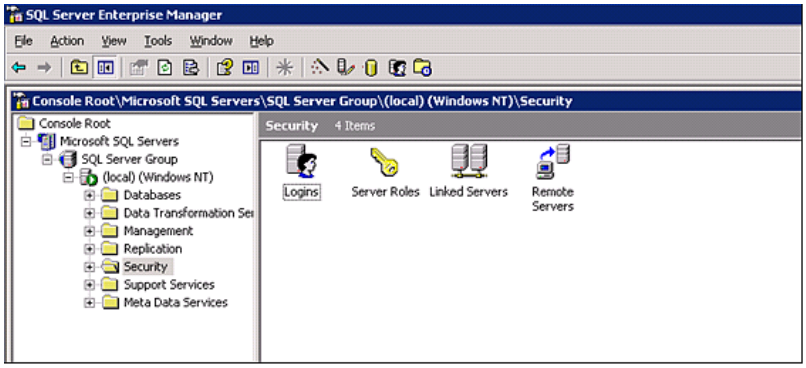
1 From the Domain Controller, access Enterprise Manager or Server Management Studio (from the Start menu, select All Programs -> Microsoft SQL Server -> Enterprise Manager | Server Management Studio).



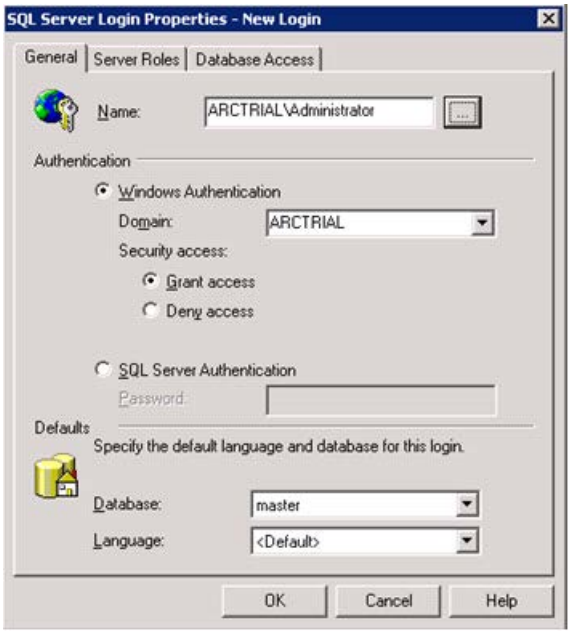
2 Open the Object Explorer for your SQL Server object.



3 Expand the **Security** folder.



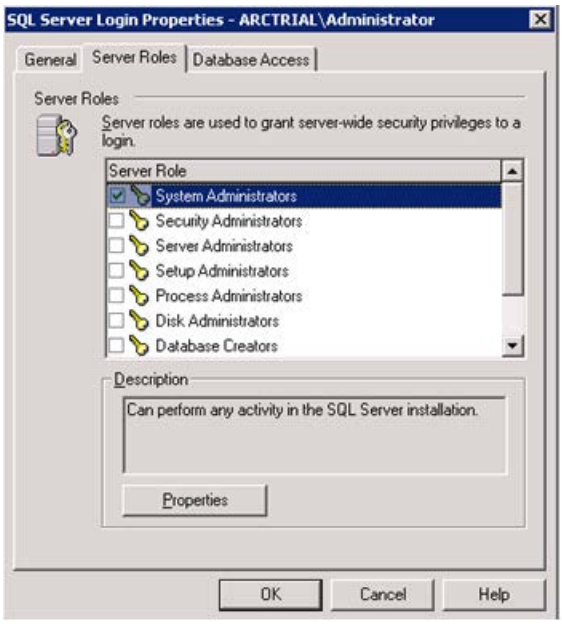
4 Right-click on the **Logins** folder; select **New Login**.



5 Select the Domain/Windows user account to be associated with the new SQL Server login.

When using SQL Authentication, check **SQL Server Authentication** and provide the password.

6 Click the **Server Roles** tab; Check **System Administrators** and click **OK**.



Enable Auditing

SQL Server provides auditing as a way to trace and record activity that has happened on each instance of SQL Server (for example, successful and failed logins). SQL Server also provides an interface, SQL Query Analyzer, for managing audit records.

Auditing can only be enabled or modified by members of the 'sysadmin' fixed security role and every modification of an audit is an auditable event.

There are two types of audit:

- **General trace auditing**, which provides some level of auditing but does not require the same number of policies as C2 auditing.
- **C2 auditing**, which requires that you follow very specific security policies.

Both kinds of auditing can be done using SQL Query Analyzer, which provides a graphical user interface to monitor an instance of SQL Server.

In "Automating SQL Server General Trace Auditing," a sample procedure is provided for you to use to enable general trace auditing for the SQL Server instance; you can run this procedure from SQL Query Analyzer.

With Windows authentication mode, the user account that runs SQL Query Analyzer must be granted permission to connect to an instance of SQL Server. For C2 auditing, sysadmin privilege is required.

You can run SQL Query Analyzer directly from inside SQL Server Enterprise Manager.

During their installation process, many applications, including SQL Server, register with the event-log subsystem. Note that **SQL Server's ability to audit login activity (including failed login attempts) to the Windows Application Log is not enabled by default**.

To configure this auditing, launch **Enterprise Manager** or **Management Studio**, select a database server, right-click **Properties**, go to the **Security** tab, and set your desired level of auditing.

If you intend to enable C2 auditing, you should not audit to the Application log, since SQL Server will write audit information about user login activity to two places simultaneously and unnecessarily degrade system performance. After you change audit settings, the database must be restarted.

Even after enabling auditing to the Application log, details about user activity such as which tables users access, which queries users run, and which stored procedures users invoke are not provided.

Although SQL Server can audit user actions, your DBA must activate this feature. DBAs have unrestricted access to databases on the database server and are responsible for database management. In many environments, the systems administrator or network administrator is also the DBA.

Use a Procedure to Enable and Configure Auditing

If SQL Server auditing has already been enabled and configured on your sever, this procedure is not required.

To enable automatic auditing upon server startup, create a procedure to enable the auditing function. Two sample procedures are provided to assist you in this task. These procedures enable auditing and specify the events to be audited.

For SQL Server 2000, see sqlserver_2000_audit_config_sample.sql for the sample procedure.

For SQL Server 2005, see sqlserver_2005_audit_config_sample.sql for the sample procedure.

For SQL Server 2008 and later, see sqlserver_2008_audit_config_sample.sql for the sample procedure.

These files are available when you download the SmartConnector configuration guides in `\agentdocinstall\AgentDocs\agentConfigDocs\attachments`.

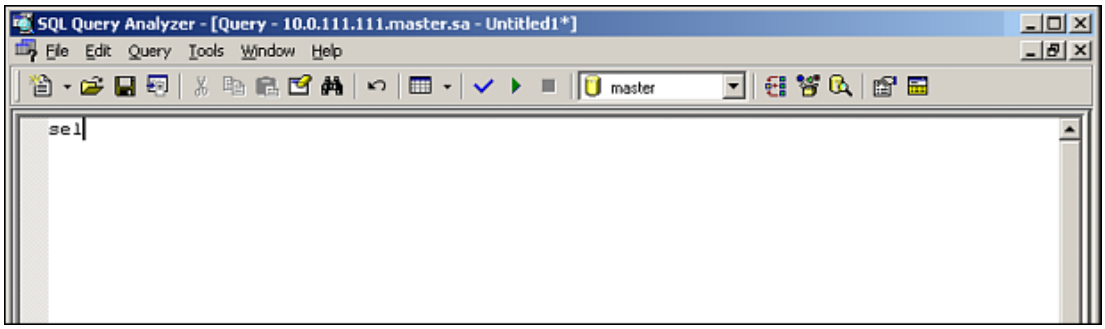
These files also are installed during SmartConnector installation to the `$ARCSIGHT_HOME\current\system\agent\config\sqlserver` directory.

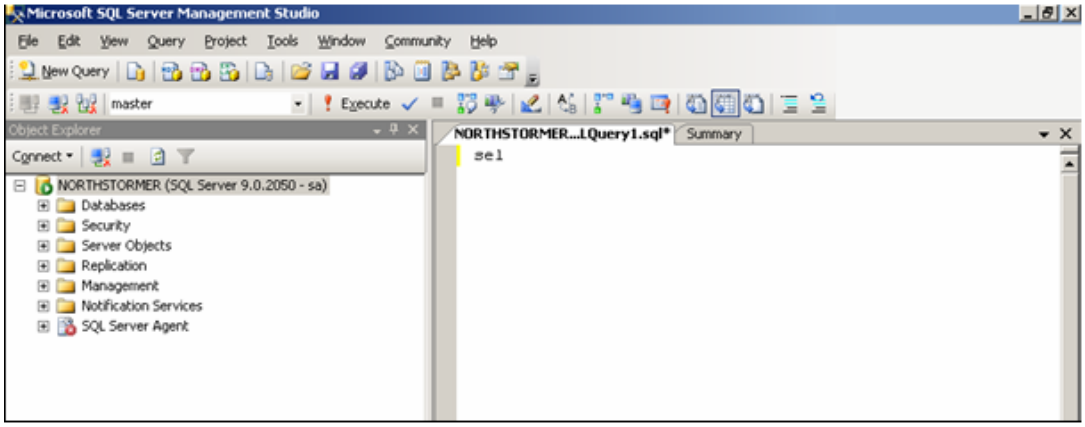
These files are also available for copying and pasting from Protect 724; look for the **Microsoft SQL Server Sample Audit Procedures** document in the Index for the SmartConnector Configuration Guides.

Within the sample procedure, be sure to replace the occurrences of the path to the trace folder with your actual path and file name (for example, `c:\sqltrace\MyTrace.trc)`. ***Be sure to use a unique file name***; if the file already exists, the SQL Server will fail when you enable the trace. See "What the Sample Procedures Collect" for an explanation of the meaning of the commands.

If you are writing from a remote server to a local drive, use the UNC path and make sure the server has write access to your network share.

1 Perform the following steps from the SQL Query Analyzer. You can run SQL Query Analyzer directly from the **Start** menu, or, for SQL Server 2005 and later, you can run it from inside SQL Server Enterprise Manager.





2 Copy the content of the procedure to the SQL Query Analyzer new query pane, saving it as `AuditTrcProc.sql`.

3 Execute the procedure with the following SQL command:

```
EXEC AuditTrcProc
```

4 Make this procedure start automatically when the SQL Server restarts by executing the following command:

```
USE master
EXEC sp_procoption 'AuditTrcProc', 'startup', 'TRUE';
```

5 Verify whether the audit is being enabled as expected by running the following query:

```
SELECT * FROM :: fn_trace_getinfo(default)
```

6 Exit from the SQL Query Analyzer.

What the Sample Procedures Collect

Each trace statement in the procedure traces an Event ID and Column ID. This applies to general auditing. C2 auditing is enabled separately; see "C2 Auditing" later in this guide.

To see the current versions of column and event IDs, use the links below to see the events for SQL Server that can be added to or removed from a trace:

- For SQL Server 2000 Event IDs, see: http://msdn.microsoft.com/en-us/library/aa260314.aspx

- For SQL Server 2005 and later (2008, 2012, 2014) Event IDs, see: http://msdn.microsoft.com/en-us/library/ms186265.aspx and select the **Other Versions** drop-down list to select the appropriate version.

The `sp_trace_setevent` command is used in the sample procedure to add an event class or data column to a trace, or to remove one from it. The `AuditTrcProc` script provided determines the events, and the columns within the events, to be traced. You can add to or delete from the events specified to be traced in the sample procedure using the `sp_trace_setevent` command.

The sp_trace_setevent format is:

```
sp_trace_setevent @traceid, <event_id> <column_id> @on
```

where the `<event ID>` and `<column ID>` to be traced have been specified. To fine-tune or modify the events to be traced, see the `sp_trace_setevent` Transact-SQL statement in *SQL Server 2005 Books Online* for all event IDs and column IDs supported.

For events to be parsed properly, be sure to select the same columns for each event type you trace.

C2 Auditing

The **c2 audit mode** option is used to review both successful and unsuccessful attempts to access statements and objects. With this information, you can document system activity and look for security policy violations.

C2 auditing tracks C2 audit events and records them to a file in the `\mssql\data` directory for default instances of SQL Server, or the `\mssql$instancename\data` directory for named instances of SQL Server. If the file reaches a size limit of 200 MB, C2 auditing will start a new file, close the old file, and write all new audit records to the new file. This process continues until SQL Server is shut down or auditing is turned off.

Implications with C2 Auditing

Note the following implications with C2 auditing:

- On a system that has limited disk space, you might find that our databases cannot grow because audit log files are consuming all the free space. Second, on a busy system, performance might suffer because both the databases and the audit logs use the same disk. In general, you should store databases and their transaction logs on separate, dedicated disk devices so you can avoid these two problems.

- SQL Server writes all auditable activity to a file with the format `audittrace_YYYYMMDDHHMMSS.trc` where `YYYYMMDDHHMMSS` is the log's creation time by year, month, day, hour, minute, and second. When a log reaches a maximum size of 200 MB, SQL Server automatically creates a new log and begins to record to the new log instead. This feature lets you safely move old log files out of the data folder or delete them.

- If SQL Server cannot write to a log file (for example, if the disk contains no more free space), it will halt all execution. SQL Server does not restart until it can resume logging. If you need to force SQL Server to run even though logging is not possible, you can use the `-f` flag to start a minimal SQL Server configuration from the command line. Using the `-m` flag with the `-f` flag starts the

database in single-user mode, preventing clients from connecting to the database and performing transactions while auditing is disabled.

Enabling C2 Auditing from Command Line

Run the following query:

```
USE master
EXEC sp_configure 'show advanced option','1'
RECONFIGURE
GO
USE master
EXEC sp_configure 'c2 audit mode','1'
RECONFIGURE
```

After executing the procedure, stop and restart the server for C2 audit mode to take effect.

Enabling C2 Auditing with SQL Query Analyzer

Before enabling C2 auditing, note the following:

- You must be a member of the sysadmin role to enable or disable C2 auditing.
- C2 audit mode is an advanced option. If you are using the `sp-configure` system stored procedure to change the setting, you can change C2 audit mode only when 'show advanced options' is set to '1.'

You can enable C2 auditing with the SQL Query Analyzer. Sysadmin privilege is required to enable or disable this option.

1. In the SQL Query Analyzer, enable the `show advanced options` configuration option using the following command:

```
USE master
EXEC sp_configure 'show advanced option', '1'
RECONFIGURE
```

2. To enable the feature, set `c2 audit mode` to `1` using the following command:

```
sp_configure 'c2 audit mode', 1
go
```

3. To disable the feature, set `c2 audit mode` to `0`:

```
sp_configure 'c2 audit mode', 0
go
```

After setting the value, stop and restart the server for C2 audit mode to take effect.

After you enable C2 auditing for the default database or for an instance, the database server will log all activity to the data directory you specified during the installation process. (SQL Server does not let you

log auditable events to an alternative location.) This directory holds the databases that SQL Server initially created. This directory is also the default location for all new databases and their transaction log files.

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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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

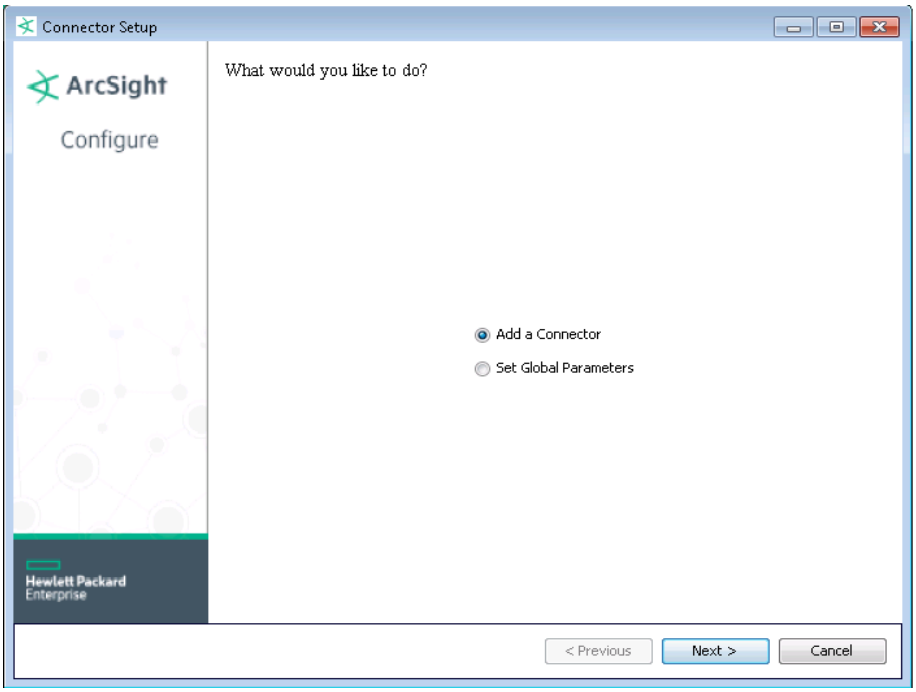
Install Core Software

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)

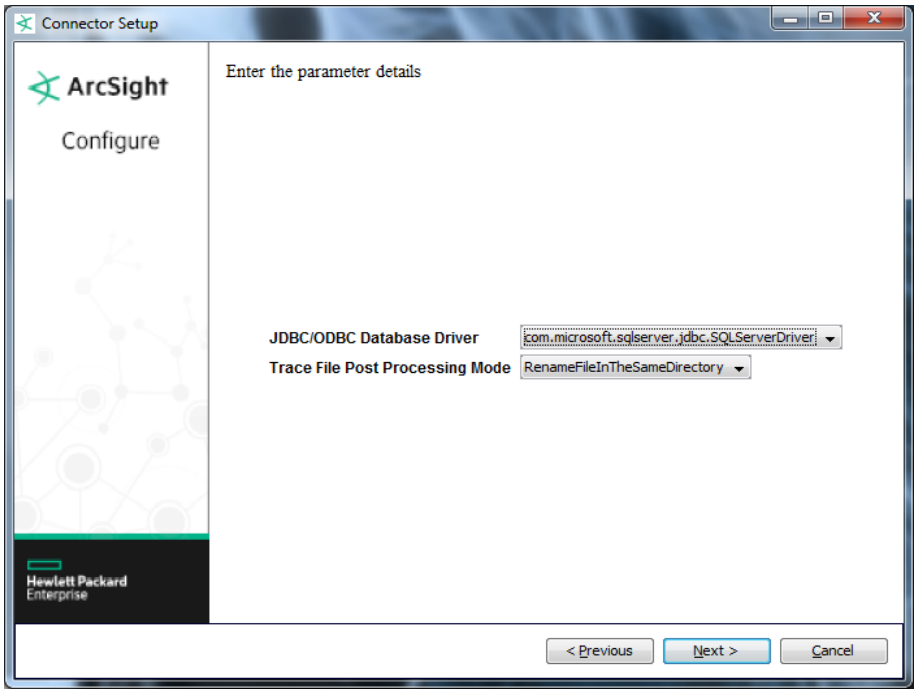
If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters:

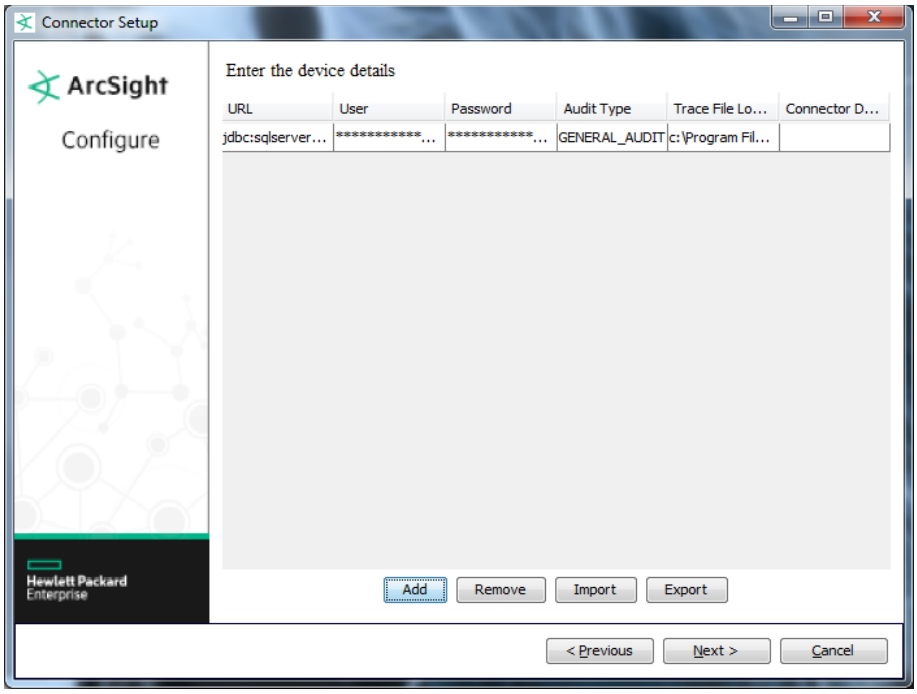
Global Parameter	Setting
Set FIPS mode	Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'.
Set Remote Management	Set to 'Enable' to enable remote 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 SQL Server Multiple Instance Audit DB** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.





Parameter	Description
Windows Share Domain	Not shown for Windows platforms. Enter the name of the domain to be shared.
Windows Share User	Not shown for Windows platforms. Enter the name of the user for the Share Domain.
Windows Share Password	Not shown for Windows platforms. Enter the password for the Windows Share User.
JDBC/ODBC Database Driver	On the first parameter entry screen, select the database driver ('com.microsoft.sqlserver.jdbc.SQLServerDriver').
Trace File Post Processing Mode	Values that can be set for this field are 'RenameFileInTheSameDirectory', 'DeleteFile', or 'PersistFile'. The connector performs some tests during configuration to make sure the folder on the SQL Server Instance containing the trace files has permissions to perform the post processing operation "DeleteFile' or 'RenameFileInTheSameDirectory'. If Post Processing Mode is set to one of these values and the trace file folder does not have permissions, the configuration setup warns you. It performs the same checks when the connector is run, and the connector will not process any trace files if the trace file folder does not have permissions for the post processing mode selected. This parameter has been implemented to prevent kernel panic on the Connector Appliance caused by read-only CIFS shares containing the trace files. The default value is 'RenameFileInTheSameDirectory'. The following parameters appear as a table on the second screen for parameter entry to provide room to specify parameters for multiple databases. Enter the parameters for each database this connector will query.
URL	Click 'Add' on the next parameter entry screen to have the wizard display a table row with default values already entered. 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>. If you are configuring additional databases, click 'Add' each time you want to enter a new row for each new database or instance. Change the URL for the database driver and the other values as appropriate.

Parameter	Description
	NOTE: With Windows authentication, the local and remote machines must be on the same domain, and the user must have full control permissions to access the trace file folder on the remote machine.
User	Enter the login name of the user you created on the DC machine in "Create a Domain User from the Domain Controller."
Password	Enter the password assigned to the DC SQL Server user.
Audit Type	Select C2_AUDIT or GENERAL_AUDIT. If you want both types of audit on the same database instance, add one row to the parameter entry table selecting GENERAL_AUDIT and another row specifying the same database instance, but with C2_AUDIT selected.
Trace File Local Folder	Enter the path specifying the local folder on the SQL Server machine (for example, c:\sqltrace) to which the SQL Server Audit trace files are written. When typing back slashes in the file path, it is not necessary to escape them in the Installation Wizard. They are automatically escaped. If you enter the file path in the Agent Configuration Wizard later, the backslashes must be escaped.
Connector Data Folder	Enter the path specifying the local folder on the SmartConnector machine to which the SQL Server Audit trace files are written. Scenario #1: When SQL Server and the SmartConnector are installed on the same machine, enter the same folder path specified for the "Trace Local Folder" parameter. (For example: c:\sqltrace.) Scenario #2: When the SmartConnector is installed on a Windows machine separate from the SQL Server, map a network drive on the SmartConnector machine to the shared folder on the SQL Server machine. (For example, map c:\sqltrace on SQL Server machine to z:\ on the SmartConnector machine.) Then, type the network share drive (z:\) as the value in the Connector Data Folder field. Note: When running the SmartConnector as a service, mapped drives do not work. For a service, use the remote network shared drives in the UNC Notation (For example \\servername.name.domain.com\foldername). When typing back slashes in the file path, it is not necessary to escape them in the Installation Wizard. They are automatically escaped. If you enter the file path in the Agent Configuration Wizard later, the backslashes must be escaped. Scenario #3: When installing the SmartConnector on Linux, use a mounted drive (e.g. /mnt/mssql) as the value in the “Connector Data Folder” field. Please see the “Mount a Drive on Linux Platforms” for more information. NOTE: If you use mapped drives, be aware of potential problems after a system reboot when SQL Server is started automatically. SQL Server will often start before the shares have been mapped and can cause a warning of a potential problem that occurs because the database engine could not open the database files. To solve this, restart SQL Server to reset the suspect flag or flags. If you use mapped files, it is a good idea to configure SQL Server to start manually after a system reboot.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

Select a Destination

1. The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2. Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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 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.

Run the Connector with a Standard Domain User Account

A Standard Domain User account can be used to run the connector only when the Microsoft SQL Server is set to Windows Authentication mode. Certain limitations apply related to the choice of the connector installation host, which are explained below. Configuration steps are required from the Domain Controller, the Microsoft SQL Server 2005 Host, and on the connector host, as described in the following sections.

On the Domain Controller

1. Create a new user account (for example, ***arcsight***).
2. Add this new user to the **Remote Desktop Users** group.

On the Microsoft SQL Server 2005 Host

1. Open the MS SQL Server Management Studio to set the MS SQL Server to Windows Authentication mode.
2. From Object Explorer in the left pane, select the MS SQL Server host of interest; right-click and select **Properties**.
3. Click the **Security** tab and set the Server Authentication to Windows Authentication mode. Click **OK**.
4. Restart the MS SQL Server service.
5. Return to the MS SQL Server Management Studio to set the appropriate permissions for the Standard Domain User ***arcsight***.
6. From Object Explorer in the left pane, select the MS SQL Server host of interest and expand its tree.
7. Go to **Security -> Logins**; right-click and select **New Login**.
8. Click the **General** tab. Populate the **Login Name** box by using **Search** to select the new domain user ***arcsight***. The option of Windows Authentication is automatically selected. The default database is automatically set to ***master***.
9. Click the **User Mapping** tab. Select the ***master*** database.
10. Click the **Status** tab. **Permission to connect to database engine** is automatically set to **Grant** and **Login** is automatically set to **Enabled**. Click **OK**.
11. Go to **Databases -> System Databases**, right-click on ***master*** and select **Properties**.
12. Click the **Permissions** tab. From the **Users or roles** table, select the domain user ***arcsight***.

13 From the **Explicit Permissions** table, select the **Grant** option for the **Connect, Execute, Select**, and **View** database state permissions. Click **OK**.

14 Select the MS SQL Server host of interest, right-click and select **Properties**.

15 Click the **Security** tab. In the **Server proxy account** section, select **Enable server proxy account**. Set the **Proxy account** and **Password** fields to the domain user ***arcsight*** and its password. Click **OK**.

16 Click the **Permissions** tab and select the domain user ***arcsight*** from the **Logins or roles** table.

17 From the **Explicit Permissions** table, select the **Grant** option for the **Alter trace**, **Connect SQL**, and **View server state** permissions. Click **OK**.

18 In Windows Explorer, go to the folder where the trace files are being logged (for example, `c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG)`. Right-click and select **Sharing and Security**.

19 Click the **Sharing** tab and select **Share this folder**. Provide a share name if one is not present (for example, **LOG**). Click **Apply**.

20 Click the **Security** tab and go to the **Group or user names** table. Using **Add**, add the domain user ***arcsight*** and select that user.

21 For the selected ***arcsight*** user, go to the **Permissions for** table and select all the permissions available, including **Full Control**. Click **Apply**.

22 Now click **Advanced** and a new window entitled **Advanced Security Settings for** is displayed.

23 Go to the **Permission entries** table and select the user ***arcsight***. Click **Edit** and ensure that all the permissions are **Allowed for This folder, subfolders and files**. Click **OK**.

24 For the selected ***arcsight*** user, select the option **Replace permission entries on all child objects with entries shown here that apply to child objects**. Click **Apply**. A new dialog box displays the message "This will remove explicitly defined permissions on all child objects and enable propagation of inheritable permissions to those child objects. Only inheritable permissions propagated from <share name> will take effect. Do you wish to continue?" Click **Yes**. Click **OK**.

25 Click **OK**.

On the Connector Host

When using Windows Authentication mode on the MS SQL Server, access to the SQL Server is possible only from Windows hosts belonging to the same domain as the domain of the MS SQL Server host. Using Windows hosts whose domain has a trust relationship with the domain of the MS SQL Server host has not been verified.

Using a non-Windows host with the Windows authentication mode enabled is not supported, even when you are using a JDBC driver, because that non-Windows host is not part of a Windows domain, which is a requirement.

Be sure to log in to the connector host with the same Standard Domain User account ***arcsight***, for which all the permissions to access the MS SQL Server trace files have been set.

Create the Trace File Access Share

If you have already mapped a Network drive to access the trace files on the MS SQL Server, disconnect and remove that share. Create the network share again to access the Trace files on the MS SQL Server. Ensure that you can rename any old trace file and set it back to its original file name.

Change the Name of Processed Files

To change the name of processed trace files:

1. Open a DOS window and go to the `$ARCSIGHT_HOME/current/bin` directory.
2. Run the command `Arcsight connectorsetup`; then choose **No** to start advanced settings.
3. Select the connector and choose Show internal parameters from the **Options** menu.
4. Locate the `mode` and `modeoptions` parameters. Change the mode to `RenameFileInTheSameDirectory` to rename the file.

Specifying 'DeleteFile' will cause the file to be deleted; specifying 'RenameFileInTheSameDirectory' will cause the file to be renamed in the same directory; 'PersistFile' will cause the file to be persisted (remembered).

5. Enter a string for the `modeoptions` parameter; this string will be the suffix. For example, if you enter `processed`, the file name is renamed to `xxxx.processed`.

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.

SQL Server Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Destination Host Name	ServerName
Destination NT Domain	NTDomainName
Destination Process Name	SPID
Destination User Name	LoginName
Destination User Privileges	Permissions
Device Action	EventClass
Device Custom Number 1	Duration
Device Custom Number 2	Reads
Device Custom Number 3	Writes
Device Custom String 1	ObjectName
Device Custom String 2	DatabaseName
Device Custom String 3	FileName
Device Custom String 4	OwnerName
Device Custom String 5	LoginSid
Device Custom String 6	_DB_NAME

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	EventClass | Success | EventSubClass
Device External ID	DatabaseID
Device Host Name	One of (_DB_HOST, _DB_DSN)
Device Product	'SQL Server'
Device Receipt Time	StartTime
Device Severity	EventClass | Success | EventSubClass
Device Vendor	'Microsoft'
Event Outcome	One of ('Success', 'Failure')
Flex Number 1	CPU
Message	TextData
Reason	errorCode
Source Host Name	HostName
Source Process Name	ClientProcessID
Source Service Name	ApplicationName
Target Host Name	ServerName

Audit Events 104, 105, 106, 107

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetLoginName
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	One of (SessionLoginName, LoginName)

Audit Event 108

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetLoginName
Device Custom String 6	RoleName
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	One of (SessionLoginName, LoginName)

Audit Event 109

ArcSight ESM Field	Device-Specific Field
Destination User ID	TargetLoginName
Destination User Name	TargetUserName
Device Custom String 6	RoleName
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID

ArcSight ESM Field	Device-Specific Field
Source User Name	One of (SessionLoginName, LoginName)

Audit Event 110

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 6	RoleName
Source Host Name	Servername
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	One of (SessionLoginName, LoginName)

Audit Event 111

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	RoleName

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.

"If multiple SQL DB instances on the same host are depositing their Trace files into a common folder, will one MS SQL connector instance retrieve all audit events?"

Yes. But there must be a separate table entry for each instance and the trace files from each of the instances must be identified somehow uniquely; for example, by the instance name itself. Then the wildcard parameter could be specified separately for each of the entries. If the wildcard is not unique, there would be a problem because the connector launches multiple threads monitoring the same folder and processing the same files. The behavior would be somewhat unpredictable.

"I started the connector and there is no error in agent.log, but I did not get any events. Why is that?"

First check whether you did enable the audit by querying the database (as indicated in "Configuration"). If you did enable the audit, you may not have received any events because the SQL Server will hold the trace file until the file reaches the 1 MB size, then rotate. If you did not audit a number of high traffic events, chances are that you will wait for some time. Try to look at the folder on the machine the connector is monitoring.

"Why do I receive a 'the trace file is not ready for processing' message?"

This message is normal for the trace file to which SQL Server is currently writing because that file is not finished yet and hence not ready for processing. If it is occurring for all the trace files, there usually is a permission problem wherein the connector does not have the permission to rename the trace file. If you do not want the files renamed, you can change the **Trace File Post Processing Mode** parameter to `PersistFile`, in which case the connector just remembers the files it has processed. To do this:

1 From a DOS prompt, go to the `$ARCSIGHT_HOME\current\bin directory`.

2 Double-click `runagentsetup.bin`.

3 Select **Modify Connector**; click **Next**.

4 Select **Modify connector parameters**; click **Next**.

5 Select **PersistFile** for the **Trace File Post Process Mode** parameter.

6 Click **Next** to continue. Click **Next** on the **Modify table parameters** window.

7 Click **Next** on the **Successfully updated parameters** window, and then check Exit and click **Next** to exit the wizard.

You can have the connector delete rather than rename the trace file by changing the mode value to 'DeleteFile'.

8 Restart the SmartConnector for your change to take effect.

"Why did I receive a message that the xp_cmdshell module has been turned off?"

With Microsoft SQL Server 2005, the xp_cmdshell module is turned OFF by default. To turn it on, there is a "Surface Area Configuration" tool in Microsoft SQL Server Programs group that will let you configure this, or you can enter the following commands in SQL Query Analyzer:

```
EXECUTE sp_configure 'show advanced options', 1
RECONFIGURE WITH OVERRIDE
GO
EXECUTE sp_configure 'xp_cmdshell', '1'
RECONFIGURE WITH OVERRIDE
GO
EXECUTE sp_configure 'show advanced options', 0
RECONFIGURE WITH OVERRIDE
GO
```

"What is the recommended configuration?"

It depends upon the case. For example, say we have an SQL Server machine (named S) and a connector machine (named A). If the database is busy, remotely install the connector; then, with the connector installed in A, monitor the folder remotely.

"What is the default size the SQL Server rotates for C2 Audit as well as for general auditing?"

C2 auditing rotation size is 200 M, which cannot be changed. General auditing rotation size is from 1 M to 5 M (the sample SQL above is configured to 1 M because we want the events loaded and sent to ArcSight Manager as quickly as possible).

"I run my connector as a service through the UNC path for access and DSN. The service failed to start, why is that?"

First, check the case we answered in the first question, then make sure to right-click on the Connector service name to make sure the Windows user can access the remote SQL Server Windows machine,

and that this user can start the local Windows service. You can always right-click on the service name, select Properties, and change "Log on as" to "This account" to use a different user for test.

One use case is that if you configure the SQL Server to log trace to c:\trace (for example), you set up a scheduled job to move the trace files from time-to-time to c:\tmpdata (for example), and then you let the Connector in machine A monitor the \\S\tmpdata folder. In this case, when you configure the Connector, you would set the parameter as follows:

```
Folder of Trace Data File (Read by connector)  \\S\tmpdata
Trace File Folder on Local SQL Server Machine  C:\tmpdata
```

The cronjob can be as simple as (for example): `Move c:\trace\sessiontrace*.trc c:\tmpdata`

Note that the latest file is always held by the SQL Server until it reaches a certain size, then is rotated.

Another use case is to monitor the c:\trace above directly, whether locally or remotely. For example, if the connector monitors the folder remotely, then the folder of trace data files (read by the connector) is **\\S\trace**. The trace file folder on the local SQL Server machine is **C:\trace**.