

HP OpenView Select Identity

Connector for Microsoft® SQL Server

Connector Version: 3.2

Installation and Configuration Guide

Document Release Date: March 2006
Software Release Date: March 2006



Legal Notices

Warranty

The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP 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.

Copyright Notices

© Copyright 2006 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project.
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (<http://jasperreports.sourceforge.net>). Portions Copyright (C) 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright (c) 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

JAVA™ is a US trademark of Sun Microsystems, Inc.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California

UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView support web site at:

<http://www.hp.com/managementsoftware/support>

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

<http://www.managementsoftware.hp.com/passport-registration.html>

Contents

1	Introduction	7
	About HP OpenView Select Identity	7
	About Connectors	7
	About SQL Server Connector	7
2	Installing the Connector	11
	System Requirements	11
	Prerequisite	13
	Installation Procedure	13
	Deploy the Connector on Application Server	14
	Configure the Connector with OVSI	14
	Install the Agent on the Database Server	17
	Installation Using the Wizard on Windows	18
	Installed Files	26
	Starting the Agent	27
3	Uninstalling the Connector	29
	Uninstalling the Agent	30
	Using the Wizard to Remove the Agent on Windows	30
	Manually Removing the Agent	31
A	Troubleshooting	33

1 Introduction

This chapter gives an overview of the HP OpenView Select Identity connector for Microsoft SQL server. An HP OpenView Select Identity connector allows you to provision users and manage identities on Microsoft SQL server. At the end of this chapter, you will be able to know about:

- the benefits of HP OpenView Select Identity
- the role of a connector
- the connector for Microsoft SQL server

About HP OpenView Select Identity

HP OpenView Select Identity (OVSI) provides a new approach to identity management. It helps you manage the entire identity lifecycle of an enterprise application. By using OVSI, you can automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. OVSI communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and OVSI by using a connector. A connector is resource specific. It is installed on the system where OVSI is installed. The combination of OVSI and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from OVSI, but if any change takes place in resource, it cannot communicate that back to OVSI. On the other hand, a bidirectional connector can reflect the changes made on resource back to OVSI. This property of bidirectional connectors is known as **reverse synchronization**.

About SQL Server Connector

The OVSI connector for Microsoft SQL server — hereafter referred to as SQL Server connector is able to perform the following tasks on an Microsoft SQL server:

- Add, update, and remove users
- Retrieve user attributes

- Enable and disable users
- Verify a user's existence
- Change user passwords
- Reset user passwords
- Retrieve all entitlements
- Retrieve a list of supported user attributes
- Grant and revoke entitlements to users
- Add, update, and remove entitlements



This connector does not provision database system users. Rather, it provisions users into a user-defined database schema in SQL Server. To provision database system users, install the Admin SQL Server connector.

It is a bidirectional connector and the connector agent can send user changes made in Microsoft SQL server to Select Identity. The following reverse synchronization operations are supported:

- Change passwords stored in Select Identity based on changes to the passwords in the schema in Microsoft SQL server
- Add, modify, and delete users based on user additions, modifications, and deletions in the schema in Microsoft SQL server

When a user is added, modified, or deleted in the database, triggers capture the changes. The agent's reverse synchronization component then sends the changes to Select Identity's Web Service in SPML. If an error occurs during reverse synchronization, the agent stops the operation (without affecting the connector's operations). In order to achieve reverse synchronization, you must install and configure the agent. Additional steps are required to configure the agent for reverse synchronization (installing and configuring the agent is mandatory in order for the connector to support reverse synchronization).

The SQL Server connector also supports custom encryption, which enables the connector to encrypt values provisioned in the schema. Refer to *Appendix C of HP OpenView Select Identity Administrator Guide* for information on how to use this feature.

The SQL Server Admin Agent supports secure channel of communication to OVSI web service by using HTTPS. The Application Server needs to be configured with Secure Socket Layer (SSL).

Suitable settings can be made on agent by setting some properties to enable secure communication between agent and OVSI in reverse synchronization. The agent will automatically import the certificate from OVSI and initialize secure communication.

The connector can be used in three different ways.

- *Connector with agent:*
In this configuration, the connector communicates with an agent that resides in the database server. The agent uses a JDBC 2.0 compliant driver to communicate with the database. The agent can also push changes made in Microsoft SQL server to the Select Identity database (reverse synchronization). You must install the agent before configuring the connector in this mode. Refer to [Install the Agent on the Database Server](#) on page 17 for information on installing agent. In this configuration, you must fill up the fields in Resource Access Information page as mentioned in the table below.

Field	Value
Mapping File	The name of the XML file that will be generated.
Server Name	The name of the database server.
Server Port	The database server's listening port.
Username	The database user.
Password	The password of the specified user.
Agent Port	The agent's listening port.
SQL URL	The name of the JDBC driver to use to connect to the database.
Database/Service Name	The name of the database.
Database Driver String	The JDBC driver being used.

- *Connector without agent and with a JDBC data source:*
In this configuration, the connector communicates with the database directly through JDBC calls. In this case, make sure to create or identify a JDBC data source (and underlying connection pool) on the application server that can connect to the target Microsoft SQL server database.

While creating the JDBC Datasource on Weblogic:

- Uncheck the Honor Global Transactions option.
- Check the Emulate Two-Phase Commit for non-XA Driver option.

You must do this configuration to allow the newly created Datasource to co-exist with the OVSI JDBC Datasource. In this configuration, you must fill up the fields in Resource Access Information page as mentioned in the table below.

- ▶ The above mentioned Data Source is not the OVSI JDBC Data Source, but a Connection Pool and Data Source created pointing to the Target Database to which the connector has to connect and provision.

Field	Value
Mapping File	The name of the XML file that will be generated.
JDBC Datasource String	The JNDI name of the JDBC data source that was created on the Select Identity server to connect to the target database.

- *Connector without agent and with JDBC driver:*
The connector communicates to the database by using a JDBC 2.0 compliant driver; no agent is installed on the database server. In this configuration, you must fill up the fields in Resource Access Information page as mentioned in the table below.

Field	Value
Mapping File	The name of the XML file that will be generated.
Server Name	The name of the database server.
Server Port	The database server's listening port.
Username	The database user.
Password	The password of the specified user.
SQL URL	The name of the JDBC driver to use to connect to the database.
Database/Service Name	The name of the database.
Database Driver String	The JDBC driver being used.

You must install the agent to achieve reverse synchronization.



This connector can be used with OVSI 4.0 and 3.3.1.

2 Installing the Connector

The SQL Server connector is packaged in the following files and folders, which are located in the Select Identity Connector CD:

Table 1 SQL Server Connector Files

Serial Number	File Name	Description
1.0	Gen-SQL2000-Connector.rar	It is the Resource Adapter Archive (RAR) file of the connector. It contains the binaries.
2.0	SQL-Gen-AgentInstaller-Win.zip	It is a zip file that contains the installation executable for the connector agent. This is for the agent to be installed in Windows environment. It is located in Agent Installers subdirectory on the connector CD.

The SQL Server connector is not shipped with any Schema file. The mapping file for the connector must be created by using the attribute mapping utility on OVSI. Refer to *Appendix C: Attribute Mapper* in *HP OpenView Select Identity Administrator Guide* for more information on attribute mapper utility.

System Requirements

The SQL Server connector is supported in the following environment:

Table 2 Platform Matrix for SQL Server Connector

Select Identity Version	Application Server	Database
3.0.2	WebLogic 8.1.2 on Windows 2000	SQL Server 2000
	WebLogic 8.1.2 on Windows 2003	SQL Server 2000
	WebLogic 8.1.2 on Solaris 9	Oracle 9i
	WebLogic 8.1.2 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Solaris 9	DB2 8.2 (or DB2 8.1 Service Pack 7)

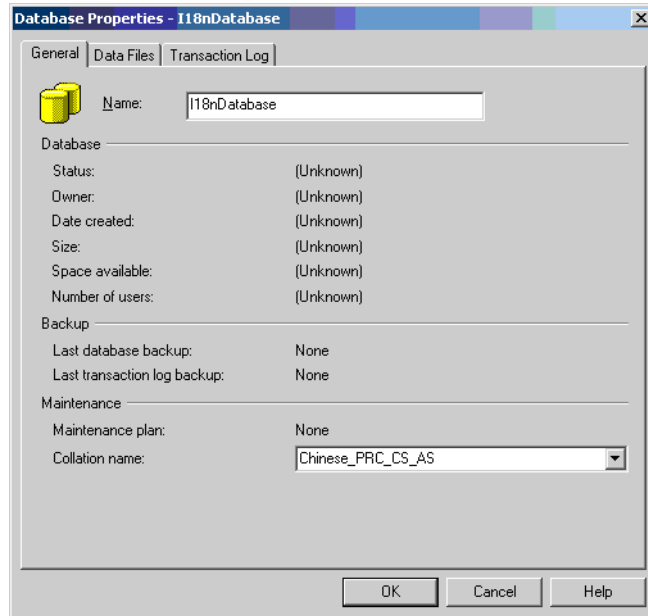
Table 2 Platform Matrix for SQL Server Connector

Select Identity Version	Application Server	Database
3.3	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
	WebLogic 8.1.4 on HP-UX 11i	Oracle 9i
3.3.1	WebLogic 8.1.4 on Windows 2003	SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
	WebLogic 8.1.4 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Windows 2003	Oracle 9i
4.0	The SQL Server connector is supported on all the platform configurations of Select Identity 4.0	

The SQL Server connector is supported for MS SQL Server 2000 on Windows 2003, Windows 2000 and Windows XP.

The SQL Server connector is internationalized and is able to operate with languages that are supported by the Java Unicode specification. If you wish to use the connector on non-English platforms, make sure that the following prerequisites are met:

- The Select Identity server is configured for internationalization. Refer to the *HP OpenView Select Identity Installation and Configuration Guide* for more information.
- SQL Server can support internationalization if the Collation Name is set appropriately when the database is created. For SQL Server 2000, the Collation Name' is set by default to the Local Language type:



Prerequisite

If using a JDBC driver to communicate with the database, copy the JDBC 2.0 compliant driver to the application server. For SQL Server, you must copy the JDBC driver files (`msbase.jar`, `mssqlserver.jar`, and `msutil.jar`). Obtain these files from your database administrator. Then, add the JDBC driver files to the application server's class path, such as by editing the `myStartWL.cmd` (for WebLogic on Windows) or `myStartWL.sh` (for WebLogic on UNIX) file.

If you intend to use a JDBC data source to communicate with the database, create or identify the data source to use.

Installation Procedure

Perform the following tasks to install SQL Server connector.

- 1 [Deploy the Connector on Application Server](#)
- 2 [Configure the Connector with OVSI](#)
- 3 [Install the Agent on the Database Server](#)

Deploy the Connector on Application Server

You must deploy the RAR file (`Gen-SQL2000-Connector.rar`) of the connector on an application server. Before deploying the RAR file, you must copy it to a local directory from the connector CD. Refer to *HP OpenView Select Identity Connector Deployment Guide* for more information on deploying a connector on an application server.

Configure the Connector with OVSI

After deploying the connector to an application server, you must configure it with Select Identity. To achieve successful configuration, you must perform the following steps.

- 1 Add a new connector – Add a new connector on OVSI. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on adding a new connector. While adding the connector, under Current Resource Connectors section in Manage Connectors page, do the following:
 - In the Connector Name text box, specify a name for the connector.
 - In the Pool Name text box, enter `eis/Gen-SQL2000Connector`.
 - Under Mapper Available section, select **Yes**.
- 2 Add a resource — You must add a resource to OVSI that uses the newly created connector. Refer to *HP OpenView Select Identity Connector Deployment Guide* for the instructions to achieve this. While entering the resource access parameters:
 - If you want to install and use the agent, enter the appropriate values in Database Driver String field and Agent Port. Leave the JDBC Datasource String field empty.
 - If you do not want to install and use the agent, leave the field Agent Port empty. Enter an appropriate value either in Database Driver String, or JDBC Datasource String.

The connector is not packaged with a mapping file. Perform the following steps to create the mapping file by using attribute mapper utility on OVSI.

- a Check the `TruAccess.properties` file, which resides in the `install_dir/sysArchive` directory on the Select Identity server, for the property `com.hp.ovsi.connector.schema.dir`. Set this property to the top-level directory where the mapping files reside, which is specified in the Base Directory field on the Attribute Mapping Utility interface.
 - ▶ If no value is specified in the Base Directory field, the `com/truologica/truaccess/connector/schema/spml` directory structure will be created in the application server's home directory.

For example, if you enter `C:\SI_3.3\schema` in the Base Directory field, the `com/truologica/truaccess/connector/schema/spml` directory structure is created under that directory, and the XML and XSL files are created there. In this example, the files reside in the directory:

```
C:\SI3.3\schema\com\truologica\truaccess\connector\schema\spml.
```

Thus, you must set the `com.hp.ovsi.connector.schema.dir` property as follows:

```
com.hp.ovsi.connector.schema.dir = C:/SI3.3/schema
```

- b Invoke attribute mapper utility to generate the XML file (mapping file) and XSL file (for reverse synchronization) for the database schema by using the utility.

- c Enter the name of this XML file in Mapping File field while entering the resource parameters.

Refer to the following table for sample values for the fields in Resource Basic Info and Resource Access Info pages.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Resource Name	<i>Gen-SQL 2000</i>	The name of the resource.
Resource Type	<i>Gen-SQL</i>	The connector that was deployed in step 1 on page 14.
Authoritative Source ^a	<i>No</i>	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. Specify Yes if the connector is enabled for reverse synchronization. If the resource is not authoritative, the resource can only modify user entitlements during reverse synchronization.
Server Name	<i>Ps0111</i>	Host name or IP address of the database server. You must specify this parameter if the agent was installed.
Server Port	<i>1433</i>	Port on which the database server is listening. You must specify this parameter if the agent was installed.
Username	<i>sa</i>	The login name of the database administrative user. You must specify this parameter if the agent was installed.
Password	<i>p4ssword</i>	Password of the database administrative user. You must specify this parameter if the agent was installed.
Agent Port	<i>5601</i>	The port where the agent listens for incoming connections. You must specify this parameter if the agent was installed.

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
SQL URL	<i>jdbc:microsoft: sqlserver</i>	URL to use to communicate with the database over a JDBC connection. You must specify this parameter if the agent was installed.
Database / Service Name	<i>testDB</i>	The database name in which to provision users. You must specify this parameter if the agent was installed.
Database Driver String	<i>com.microsoft.jdbc. sqlserver.SQLServer Driver</i>	Name of the JDBC driver to connect to the database. You must specify this parameter if the agent was installed.
Mapping File	<i>Mapping.xml</i>	Mapping file containing the mappings generated by the Attribute Mapping Utility. The mapping file must reside in the <code>install/conf/com/truologica/truaccess/connector/schema/spml</code> directory in order for the Select Identity server to find it.
JDBC Datasource String	<i>Jdbc/SQLDataSource</i>	JNDI data source name that was created or identified on the Application server that can connect to the target SQL Server database. Specify a value for this property if the agent was not installed. Note that the connection pool must be created by specifying a user with <code>adminstartor</code> privileges.
Encryption Specification Algo		Encryption algorithm specification string. Note that secure JDBC is not supported with this connector (do not specify these parameters).

Table 3 Resource Configuration Parameters

Field Name	Sample Values	Description
Encryption Algorithm		Name of the encryption algorithm. Note that secure JDBC is not supported with this connector (do not specify these parameters).
Encryption Specification Level		Encryption level specification string. Note that secure JDBC is not supported with this connector (do not specify these parameters).
Encryption Level		Encryption level. Note that secure JDBC is not supported with this connector (do not specify these parameters).

- a. Instead of creating an authoritative resource, you can create authoritative attributes (in the next step) for the attributes that will be synchronized. Entitlements are authoritative by default in a non-authoritative resource but other attributes are not.
- 3 Map the attributes – You must map the OVSI attributes to the attributes of the resource. Refer to *HP OpenView Select Identity Connector Deployment Guide* for information on mapping attributes. Add new attributes on OVSI, if necessary. Refer to *Service Studio* chapter of *HP OpenView Select Identity Administrator Guide* for information on adding new attributes on OVSI.
 - 4 Associate the newly added resource to a service. Refer to the chapter *Service Studio* of *HP OpenView Select Identity Administrator Guide* for more information on service.

Install the Agent on the Database Server

After you install the SQL Server connector on the Select Identity server, you can install the agent on the database server. This is optional; the connector can provision users in SQL Server without the agent. However, the agent enables you to send data back to Select Identity (reverse synchronization).

You can install the agent by using the installation wizard to the server.



Make sure to generate the XML and XSL mapping files before installing the agent. Copy the mapping files from the Select Identity server to the system where you will install the agent (on the database server). The agent installation requires that the mapping files are available on the local system.

Installation Using the Wizard on Windows

Complete the following steps to run the installation wizard, which installs the agent on Windows.

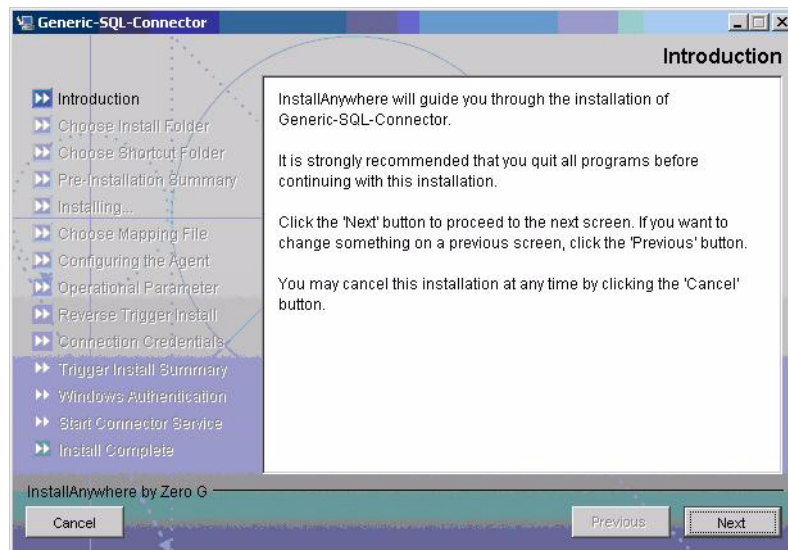


Before running the installation wizard, make sure that Java 1.4.2 (or above) is installed on the system and `%JAVA_HOME%\bin` is specified in the Path system variable.

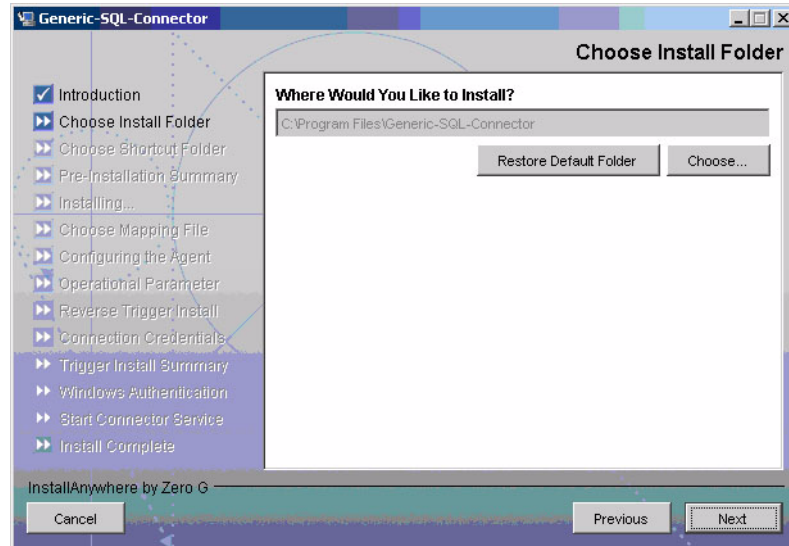
Also, you can pass the `LAX_VM` argument to point the wizard directly to the correct `java.exe` executable. Here is an example:

```
install.exe LAX_VM c:\java14\bin\java.exe
```

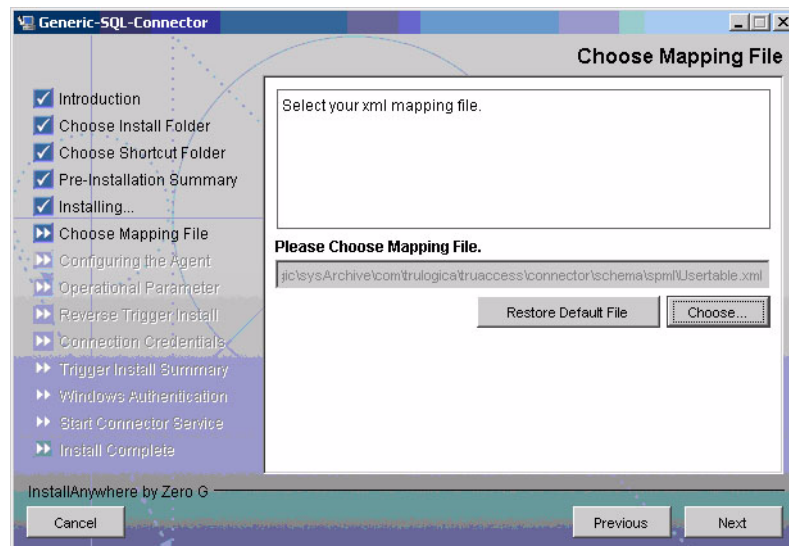
- 1 Extract the contents of the `SQL-Gen-AgentInstaller-Win.zip` file, which is located in the `Agent Installers` directory on the CD.
- 2 Run `Generic-SQL-Connector-Installer.exe`, which is located in the `target_dir\CDROM_Installers\Windows\Disk1\InstData\NoVM`. The following dialog appears:



- 3 Click **Next**.
- 4 Specify an installation directory, and then click **Next**. By default, the agent is installed in `C:\Program Files\SQL_CONN_AGENT`.

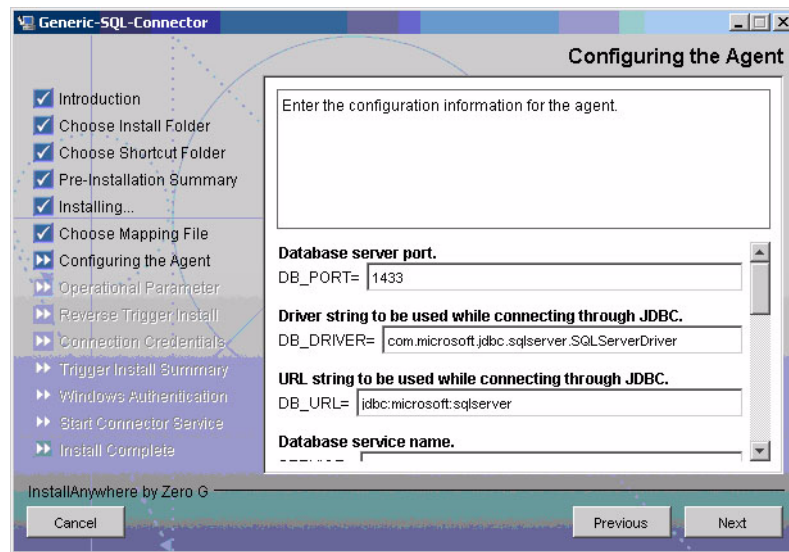


- 5 Select the location(s) where the product icons will be installed, and then click **Next**.
- 6 Verify the pre-installation summary. If you wish to make changes, click **Previous**, and then edit the chosen options. To install the agent, click **Install**.
- 7 On the Set CLASSPATH dialog, click **Next** after you verify that the database driver files (`msbase.jar`, `mssqlserver.jar`, and `msutil.jar`) is in the database server's System class path.
- 8 Click **Choose** to browse and select the mapping file. This will copy the mapping file to the `install_dir/conf/com/truologica/truaccess/connector/schema/spml` directory, where `install_dir` is the installation folder.



Then, click **Next**.

- 9 On the Configuring the Agent dialog, specify the requested information:



The following gives a description of the configuration options:

Option	Description	Example Value
DB_PORT	The port on which the database server is listening.	1433
DB_SERVER	The IP address or name of the database server.	localhost
DB_DRIVER	The JDBC driver for the database connection.	com.microsoft.jdbc.sqlserver.SQLServerDriver
DB_URL	The JDBC URL string used for the database communication.	jdbc:microsoft:sqlserver
SERVICE	The database name.	SI_DB
SERVER_SECURE	Whether communication between the agent and Select Identity must be secure. By default, non-secure communication is used. 0 - HTTP is used. 1 - Secure HTTPS communication is used.	Must be checked if the secure communication is required.

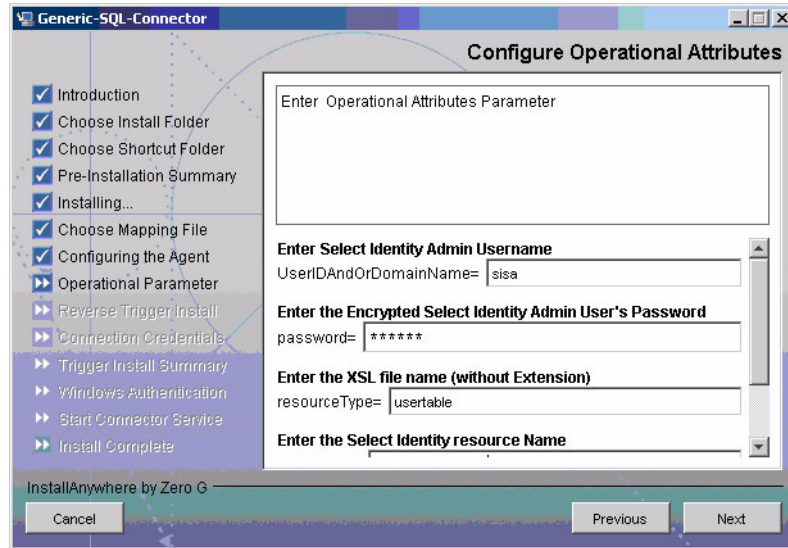
Option	Description	Example Value
CONCERO_SERVER_URL	The URL of the Select Identity Web Service. If the SERVER_SECURE is checked, the SI webservice should be running on SSL* and the protocol will be 'https'. If the SERVER_SECURE is checked, the SI webservice should be running on SSL* and the protocol will be 'https'.	If running on SSL https://host:port/lmz/webservice else http://host:port/lmz/webservice
PollDelay	The polling delay for reverse polling (in seconds).	10
AGENT_PORT	The port on which the agent listens for user provisioning requests from Select Identity.	5601
SPML_DELAY	The delay (in milliseconds) between successive SPML requests sent from the agent. Increase this delay if the network or Select Identity server is performing slowly.	10000
NO_OF_RETRIES	The number of times the agent will retry sending SPML requests in case of failure.	10
DELAY_BETWEEN_RETRIES	The delay (in milliseconds) between each retry.	10000



To edit any of these values after installation, you can edit the `properties.ini` file, which resides in `install_dir\conf`.


After specifying these values, click **Next**.

- 10 Provide the operational attributes that are sent to the Select Identity server during reverse synchronization requests.



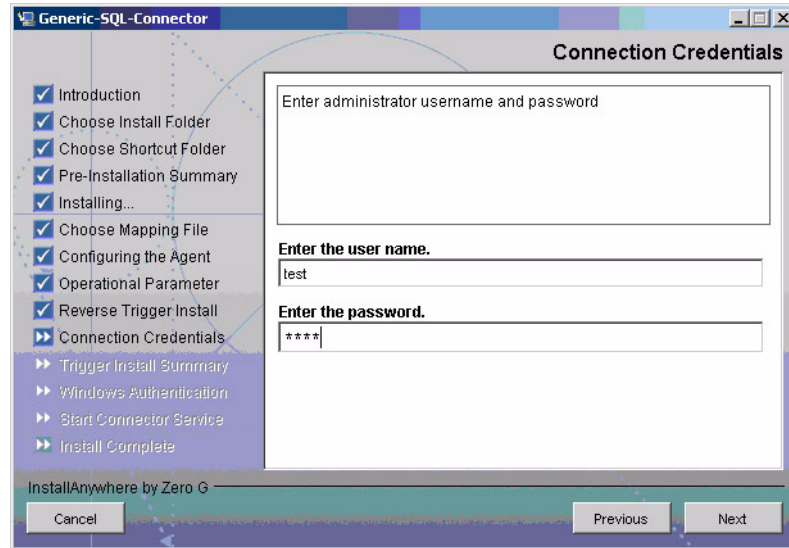
The table below gives a description of the attributes

Parameter	Sample Values	Description
urn:oasis:names:tc:SPML:1:0# UserIDAndOrDomainName	Sisa	User ID of the administrative user on Select Identity.
urn:trulogica:concerro:2.0# password	*	Password of the administrative user. This password is automatically encrypted by the agent installer.
urn:trulogica:concerro:2.0# reverseSync	true	Set to true if you want to enable reverse synchronization.
urn:trulogica:concerro:2.0# resourceType	SQLSvr	The name of the XSL file (without the .xsl extension) that is used during reverse synchronization.
urn:trulogica:concerro:2.0# resourceId	SQLSvr	The name of the Select Identity resource that is created for the SQL Server connector.

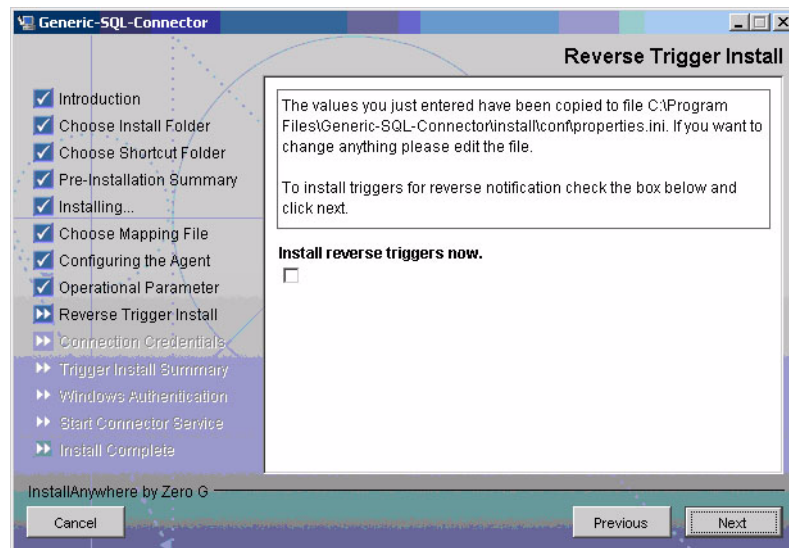
 To edit any of these values after installation, you can edit the `opAttributes.properties` file, which resides in `install_dir\conf`.

After specifying the values, click **Next**.

- 11 Provide the username and password of the SQL Server user with administrator privileges on the Database. This information is used to check the login to database.

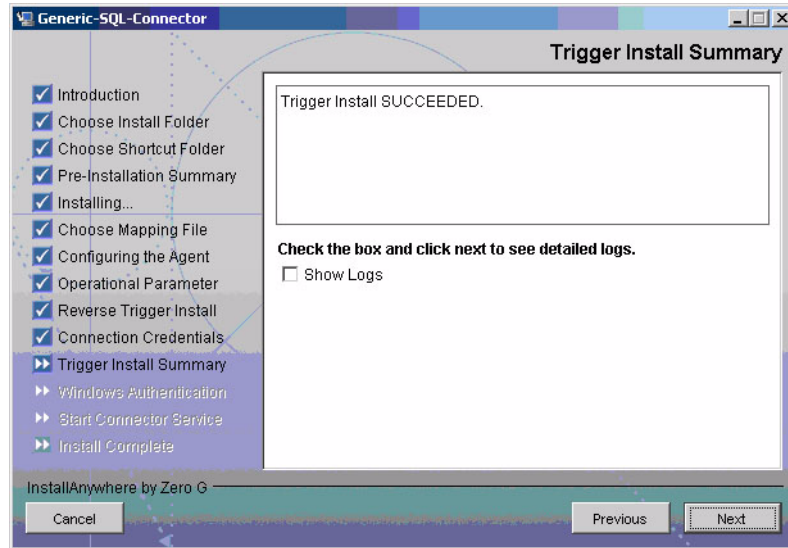


- 12 To enable reverse synchronization, you must install the reverse triggers. Select the **Install Triggers Now** option to install the triggers. Then, click **Next** and proceed to the next step.

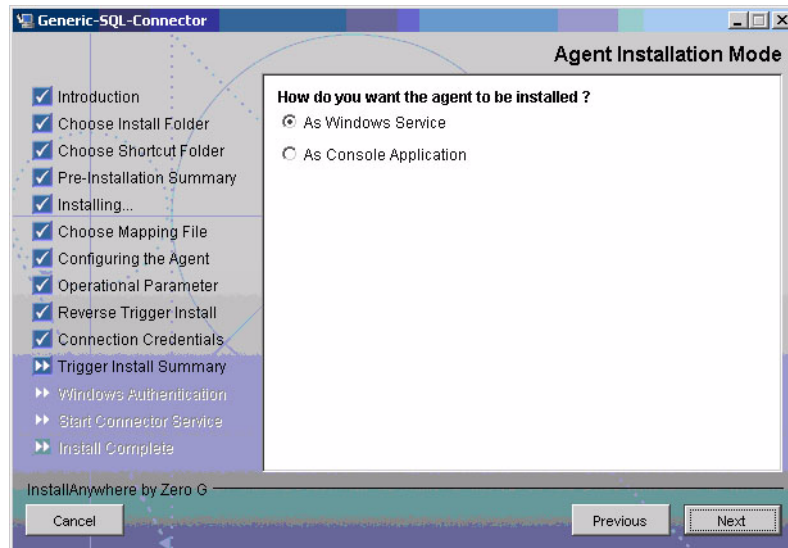


If you choose not to install the reverse triggers, skip to [step 16](#) on page 24.

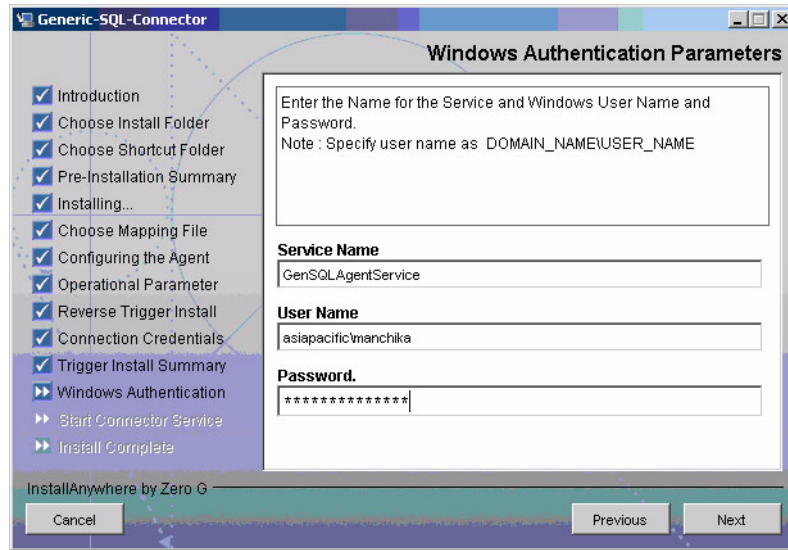
- 13 If you selected the Install Reverse Triggers now option on the Reverse Trigger Install dialog, the triggers are installed for the schema specified by the mapping file.
- 14 Review the installation summary for the triggers. If you wish to make changes, or if the trigger installation failed, click **Previous**, and then edit the chosen options, such as the credentials. You can also select the Show Logs option to review the trigger installation log files. Then, click **Next**.



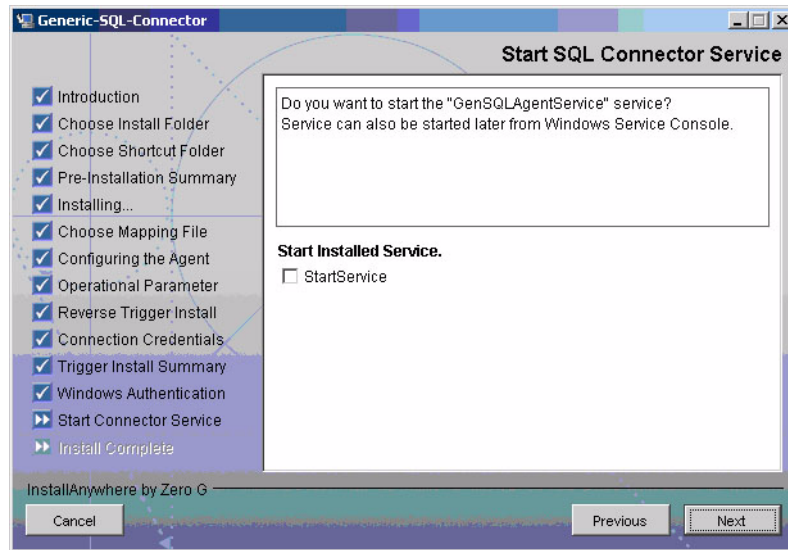
- 15 If you select the **Show Logs** option, the Detailed Logs dialog appears. Review the log entries, and then click **Next**.
- 16 Select if you want to run the SQL Generic Connector Agent as a Console application or a Windows Service.



- 17 If you select As Windows Service, provide the Service Name and Windows user account with privileges to register the service. If you select As Console Application, skip this step.



- 18 After the agent is successfully registered as service, if you want to start the service, check the option StartService.



- 19 When the installation wizard completes, click **Done** on the Install Complete dialog to close the installation program.

Installed Files

The following provides a listing of the directories and files installed for the agent:

Directories and Files	Description
<i>agent_home/</i>	<p>Contains the following files:</p> <ul style="list-style-type: none"> • <code>AddToStartupGroup.cmd</code> — Adds icons to startup group; this file is present only if the agent was installed using the wizard • <code>CopyFile.cmd</code> — Used by agent to copy files; this file is present only if the agent was installed using the wizard • <code>DelFile.cmd</code> — Used by agent to delete files; this file is present only if the agent was installed using the wizard • <code>setup.cmd</code> — Installs the reverse triggers • <code>sqlapp.cmd</code> — Used by agent to communicate with the database • <code>SQLConnectorConsole.cmd</code> — Starts the agent • <code>uninstall.cmd</code> — Uninstalls triggers • <code>LogonTest.cmd</code> — Checks the login of user on database. • <code>passwordEncrypt.cmd</code> — Encrypts the DB user and SI Admin password in the property files. • <code>PortTest.cmd</code> — Checks if the agent port given is available.
<i>agent_home/conf/</i>	<p>Contains the following files:</p> <ul style="list-style-type: none"> • <code>properties.ini</code> — Provides configuration settings for the agent • <code>opAttributes.properties</code> — Provides configuration settings for reverse synchronization • <code>log4j.properties</code> — Provides settings for logging. • <code>serviceName.conf</code> — The configuration file for Agent service. • <code>wrapper.conf</code> — The configuration file for the Agent Service wrapper.
<i>agent_home/conf/com/</i>	Contains the <code>trologica/truaccess/connector/schema/spml</code> directory structure where the XML mapping file is stored
<i>agent_home/lib/</i>	Contains JAR files used by the agent.
<i>agent_home/logs</i>	Contains log files produced by the agent.
<i>agent_home /bin</i>	Contains <code>wrapper.exe</code> , which is the utility used for registering the agent as service.
<i>agent_home/Uninstall_SQL_CONN_AGENT/</i>	Contains files for uninstalling the agent. This subdirectory is created only if the agent is installed using the installation wizard.

Starting the Agent

To start the agent as a console application, run `SQLConnectorConsole.cmd` (on Windows), which resides in the agent's home directory. This program logs in to the database server using the user name and password of a user who has administrative privileges on the database.

If you start the agent before or without configuring reverse synchronization (the reverse triggers), a message is displayed stating that reverse notification is disabled.

3 Uninstalling the Connector

If you want to uninstall SQL connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from OVSI.
- Delete the connector from application server.
- Uninstall the agent.

See *HP OpenView Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and OVSI.

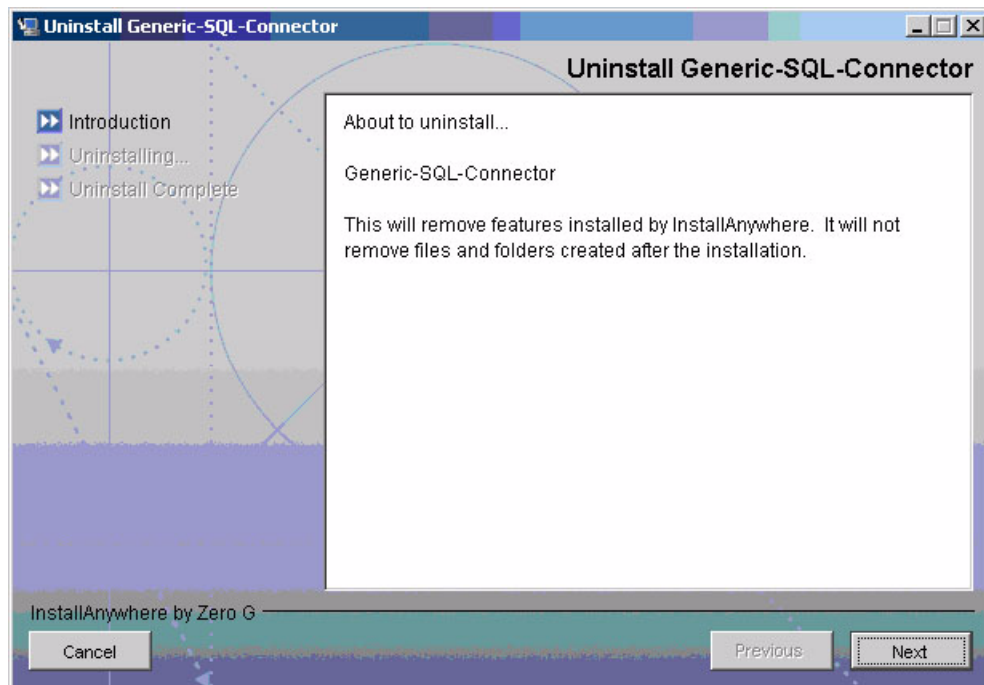
Uninstalling the Agent

The following sections describe how to remove the agent, which you can do using a wizard or manually.

Using the Wizard to Remove the Agent on Windows

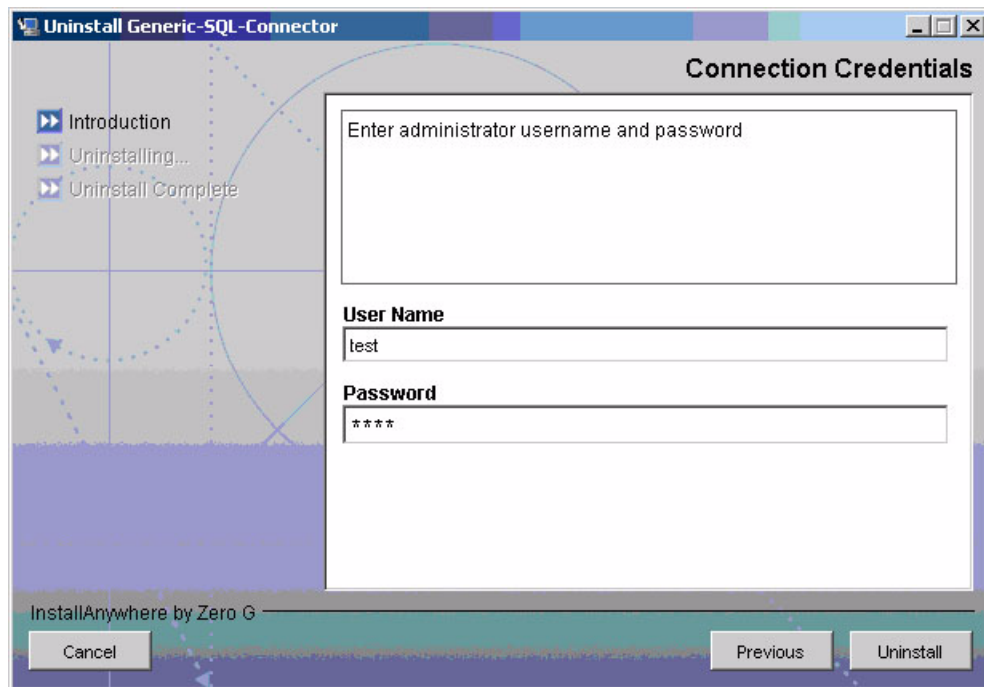
Perform the following steps to delete the agent on the Windows server:

- 1 Select **Programs** → **SQL_CONN_AGENT** → **Uninstall Agent** from the Start menu. The wizard appears.

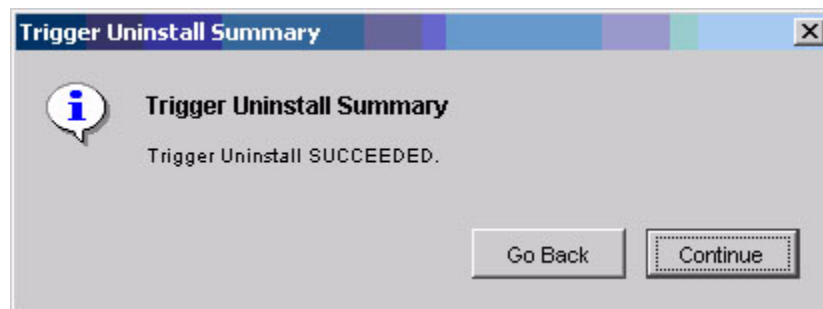


- 2 Click **Next** on the introductory dialog.

- 3 Provide the database credentials to uninstall the reverse triggers, if they were installed, and then click **Uninstall**.



- 4 Click **Continue** when the pop-up dialog indicates that the triggers were successfully uninstalled.



- 5 Click **Done** on the Uninstall Complete dialog to close the wizard.

Manually Removing the Agent

Perform the following steps to manually remove the agent:

- 1 Make sure that the `agent_home\conf\properties.ini` file retains the same values used during the installation of the reverse triggers.
- 2 Make sure that the mapping file during the installation of the agent is available in the `agent_home\conf\com\trulogica\truaccess\connector\schema\spml` subdirectory.
- 3 Run the `uninstall.cmd` file.

- 4 Provide the database login credentials when prompted.
- 5 Delete the agent files and directory structure, if you want.

A Troubleshooting

This appendix describes common problems encountered during the installation and use of the connector and its agent.

Connector Installation

This section lists the common problems encountered during installation and use of the connector.

- After redeploying the connector, Select Identity does not display the current connector information.

Possible Cause: The application is using a cached connector file.

Solution: Restart the application server.

- Select Identity does not display the most current mapping file information.

Possible Cause: The application server is using a cached mapping file.

Solution: Restart the application server.

- The mapping file of an existing resource is changed and, when you attempt to modify the resource to add a new mapping file, the following error displays:

```
Application cannot be modified at this time
```

Possible Cause: Major differences may exist between the old and new mapping files.

Solutions:

- Create a new resource with the new mapping file.
 - Unmap all attributes in the current resource and modify the resource to reference the new mapping file. You cannot use this second solution, however, if users were provisioned using this resource.
- Select Identity can successfully add a user but the new user is not shown in the resource's database table.

Possible Causes:

- The mapping file lacks the Create operation for the Key attribute.
- The Create operation for the User entity is not added in the XML file.
- The XML parser files may be missing from the `BEA_HOME/jdk_1.4.1/jre/lib/endorsed` folder (on WebLogic).
- A database exception occurred.

Solutions:

- Add the Create operation or add the relevant JARs to the path. Refer to the *HP OpenView Select Identity Attribute Mapping Utility User's Guide* for details on how to add create operations for an entity.

- If a database exception occurred, refer to the logs for details of the exception. Common exceptions include size mismatches for columns and foreign key constraint violations. Refer to the database documentation for more information on the database exceptions.

Agent and Trigger Installation

This section lists the common problems encountered while installing and configuring reverse synchronization.

- An error message similar to one of the following is displayed while installing the agent:

```
Object already exists
```

```
Table_Audit (or Column_Audit) already exists
```

Possible Cause: Triggers or audit tables exist, possibly from a prior attempt to install and configure the agent.

Solution: Run `uninstall.cmd` (on Windows) or `uninstall.sh` (on UNIX), which removes the triggers from the database. Verify that the `Table_Audit`, `Column_Audit`, and `SID_TAB` tables were removed from the database. If removal was not successful, delete the tables manually before installing the agent triggers.

- A `NullPointerException` occurs

Possible Cause: The specified mapping file is not available in the class path.

Solution: Make sure that the file is placed in the `Install/conf` directory. Ensure the name of the file specified in `properties.ini` is spelled correctly. Note that it is case sensitive. Also, check the format of the mapping file.

- The agent installation wizard fails to start and displays an error message.

Possible Cause: The JVM is not in the System Path environment variable or Java 1.4 is not available.

Solution: Add the Java 1.4 to the System Path.

- While deploying the reverse synchronization triggers, the installation stops and displays an exception.

Possible Cause: A version of Java that is older than 1.4 is the default JDK in use.

Solution: Set the `JAVA_HOME_14` variable to the path of Java version 1.4.

Agent Execution

This section lists the common problems encountered while running the agent.

- An exception similar to the following is displayed:

```
java.net.BindException: Address in use: JVM_Bind
```

Possible Cause: The listening port on the agent's system is in use, possibly by another invocation of the agent.

Solution: Stop the older invocation and run the agent again.

- An error message similar to the following is displayed:

```
Invalid Object schema.tableName
```

Possible Cause: The schema specified in the mapping file is incorrect.

Solution: Check the mapping file. For more information on the format of mapping file, see the *HP OpenView Select Identity Attribute Mapping Utility User's Guide*.

- An error message similar to the following is displayed:

Invalid Object Table_Audit or Column_Audit

Possible Cause: Audit tables are deleted or moved, or they are inaccessible to the triggers. If a trigger fails, the operation that caused the trigger is also rolled back.

Solution: Make sure that the audit tables (Table_Audit, Column_Audit) are available. If that does not work and the connector's operations are failing, triggers and audit tables can be uninstalled, though this will cause reverse synchronization to stop.

- The agent console shows a Log4jFactory exception when started.

Possible Cause: The agent cannot find the `log4j-1.2.8.jar` in the classpath.

Solution: Add the JAR to the class path.

