

HP Select Identity Software

Connector for Oracle® 9i and 10g (Administration)

Connector Version: 3.71

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007



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 2006-2007 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 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 © 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 © 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

You can visit the HP software support web site at:

<http://www.hp.com/go/hpsoftwaresupport>

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into 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 sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Documentation Map	7
2	Introduction	9
	About HP Select Identity	9
	About Connectors	9
	About Oracle Admin Connector	9
	High-Level Architecture	10
	Overview of Installation Tasks	12
3	Installing the Connector	13
	Oracle Admin Connector Files	13
	Planning the Installation	14
	Plan 1: Connector with the Agent	14
	Plan 2: Connector Without the Agent and with JDBC Data Source	14
	Plan 3: Connector Without the Agent and with JDBC Driver	15
	System Requirements	16
	Pre-Installation Task	17
	Enable JDBC Driver Based Communication	17
	Enable JDBC Data Source Based Communication	18
	Extracting Contents of the Schema File	18
	WebLogic	18
	WebSphere	18
	Installing the Connector RAR	19
	Configuring Oracle to Support Secure JDBC	19
4	Configuring the Connector with Select Identity	21
	Configuration Procedure	21
	Add a New Connector	21
	Add a New Resource	21
	Map Attributes	24
5	Installing the Agent	27
	About the Agent	27
	Installing the Agent on the Oracle Database Server	27
	Pre-Installation Tasks	27
	Install the Agent	28
	Windows	28
	UNIX (Solaris or HP-UX)	37
	Installed Files	43
	Starting the Agent	44

Operating the Agent Daemon	44
Modifying the Database Account and Select Identity Passwords	44
6 Uninstalling the Connector	47
Uninstalling the Agent on Windows	47
Uninstalling the Agent on UNIX (Solaris or HP-UX)	47
A Troubleshooting	49
Connector Installation	49
Agent and Reverse Notification Table Installation	49
Agent Execution	52
B Connector Behavior	53

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

[Figure 1](#) illustrates the documentation map for Select Identity connector. For a list of available product documentation, refer to the [Table 1](#).

Figure 1 Documentation Map

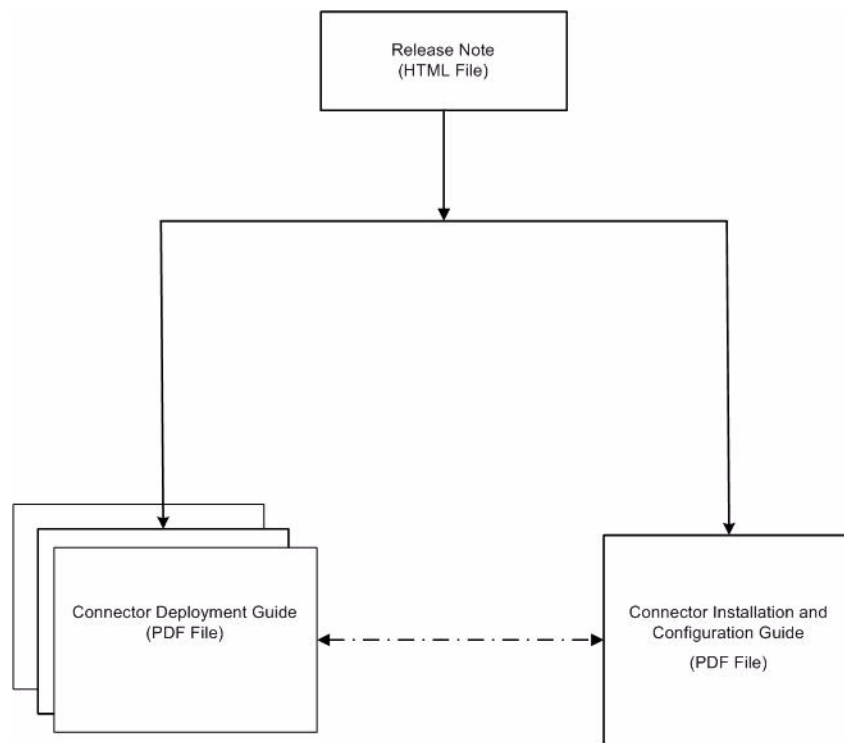


Table 1 Connector Documentation

Document Title and Filename	Contents	Location
<i>Release Note</i> Oracle Admin Connector v3.71 Release Note.htm	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	/Docs/ subdirectory under the connector directory.
<i>Connector Deployment Guide (for Select Identity 4.20)</i> connector_deploy_SI4.20.pdf	Connector deployment guides provide detailed information on: <ul style="list-style-type: none"> • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	/Docs/ root directory on the product's CD media.
<i>Connector Deployment Guide (for Select Identity 4.10-4.13)</i> connector_deploy_SI4.13.pdf		
<i>Connector Deployment Guide (for Select Identity 4.0-4.01)</i> connector_deploy_SI4.pdf		
<i>Connector Deployment Guide (for Select Identity 3.3.1)</i> connector_deploy_SI3.3.1.pdf		
<i>Connector Installation and Configuration Guide</i> Oracle Admin_guide.pdf	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	/Docs/ subdirectory under the connector directory.

2 Introduction

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

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for Oracle database.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity 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 Select Identity by using a connector. A connector is resource specific. The combination of Select Identity 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 Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About Oracle Admin Connector

The connector for Oracle database administration — hereafter referred to as the Oracle Admin connector — enables Select Identity to administer the database server by provisioning database user information in system schemas.. The Oracle Admin connector supports two types of database users, Password Authentication and External Authentication users. The Oracle Admin connector can perform the following operations in the database schema on the Oracle database server:

- For Password Authentication users:
 - Add, update, and remove users
 - Retrieve user attributes
 - Enable and disable users
 - Reset Password
 - Change Password
 - Verify a user's existence
 - Retrieve all entitlements
 - Retrieve a list of supported user attributes
- For External Authentication users:
 - Add, update, and remove users
 - Retrieve user attributes
 - Verify a user's existence
 - Enable and Disable User status
 - Retrieve all entitlements
 - Retrieve a list of supported user attributes
 - Grant and revoke entitlements to and from users

The connector also provides an agent that can send changes made to the data in Oracle database server to Select Identity. The following reverse synchronization operations are supported:

- Add, modify, and delete users based on user additions, modifications, and deletions in the schema in Oracle
- Assign and revoke entitlements for users

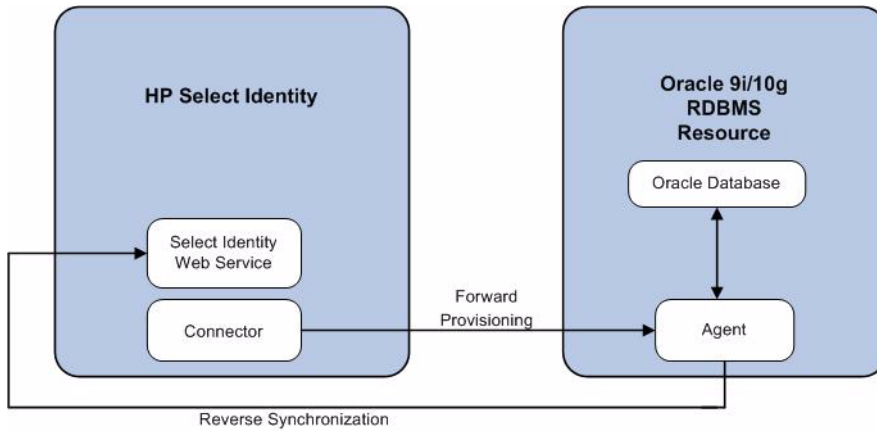


This connector can be used with Select Identity 3.3.1-4.20.

High-Level Architecture

Figure 2 illustrates a high-level architecture of Oracle Admin connector. You must install the connector on Select Identity server and the agent on resource system. The agent helps synchronizing the changes made on Oracle Admin server with Select Identity.

Figure 2 High-Level Architecture of the Connector



To perform forward provisioning operation on Oracle database server, the connector communicates either directly with the database or with the agent. The agent detects the changes on the host (Oracle database) resource and sends SPML notifications to Select Identity to synchronize the changes. Thus, the Oracle Admin connector enables data to flow in both the directions, as illustrated in [Figure 2](#).

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements (hardware and software) and all the installation prerequisites are met. Refer to the [Table 2](#) for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 13.
	— Plan your installation setup.	See Planning the Installation on page 14.
	— Meet the system requirements.	See System Requirements on page 16.
	— Pre-installation task: Enable JDBC driver or JDBC data source based on your requirement.	See Pre-Installation Task on page 17.
	— Extract contents of the Schema file (the file that contains the mapping XML and XSL files).	See Extracting Contents of the Schema File on page 18.
	— Deploy the connector Resource Adapter Archive (RAR) file on an application server.	See Installing the Connector RAR on page 19.
	— Configure Oracle to support secure JDBC communication.	See Configuring Oracle to Support Secure JDBC on page 19.
2	Configure the connector with Select Identity	See Configuring the Connector with Select Identity on page 21.
3	Install the agent on Oracle database server.	See Installing the Agent on page 27.
	— Perform the pre-installation tasks.	See Pre-Installation Tasks on page 27.
	— Install the agent by using the installation wizard.	See Install the Agent on page 28.

3 Installing the Connector

This chapter elaborates the procedure to install the Oracle Admin connector on the Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the Oracle Admin connector.
- Pre-installation tasks.
- Procedure to install the Oracle Admin connector.

Oracle Admin Connector Files

The Oracle Admin connector is packaged in the following files and folders, which are located in the Oracle RDBMS - Admin directory on Select Identity Connector CD:

Table 3 Oracle Admin Connector Files

Serial Number	File Name	Description
1	Admin-Oracle-Connector.rar	The RAR file contains the binaries for the connector.
2	AdminOracleSchema.zip	The Schema file contains the mapping files (XML and XSL files) of the connector.
3	Oracle-Admin-AgentInstaller-Win.zip	A ZIP file that contains the installation executable for the connector agent. It is located in the Agent Installers directory of the CD.
4	Oracle-Admin-AgentInstaller-Solaris.tar	A TAR file that contains the installation executable for the connector agent to be used for Solaris platform. It is located in the Agent Installers directory of the CD.
5	Oracle-Admin-AgentInstaller-HPUX.tar	A TAR file that contains the installation executable for the connector agent to be used for HP-UX platform. It is located in the Agent Installers directory of the CD.

Planning the Installation

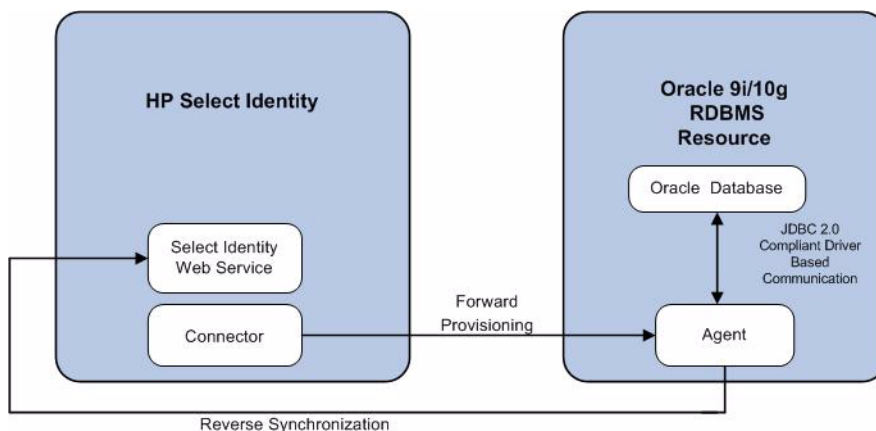
You can install the Oracle Admin connector in three possible ways.

- Connector with the agent.
- Connector without the agent and with a JDBC data source.
- Connector without the agent and with a JDBC driver.

Plan 1: Connector with the Agent

In this configuration, the connector communicates with an agent that resides on 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 Oracle Admin to the Select Identity database (reverse synchronization).

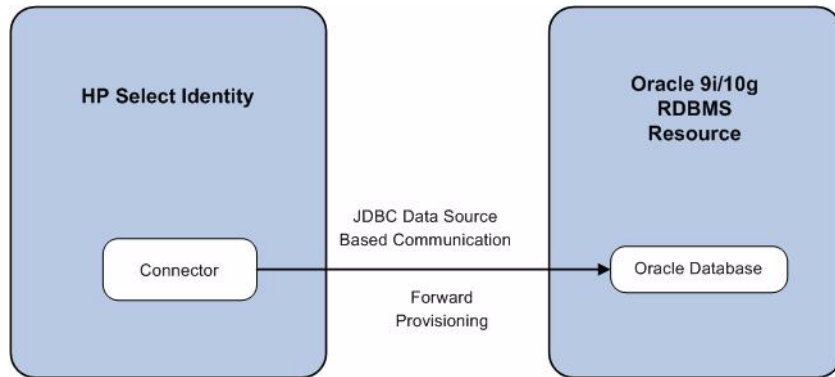
Figure 3 Connector Installed with Agent



Plan 2: Connector Without the Agent and with JDBC Data Source

In this configuration, the connector communicates with the database directly through JDBC calls. You must create or identify a JDBC data source (and underlying connection pool) on the application server hosting Select Identity and the connector that can connect to the target Oracle Admin database. Reverse synchronization is not achieved in this configuration.

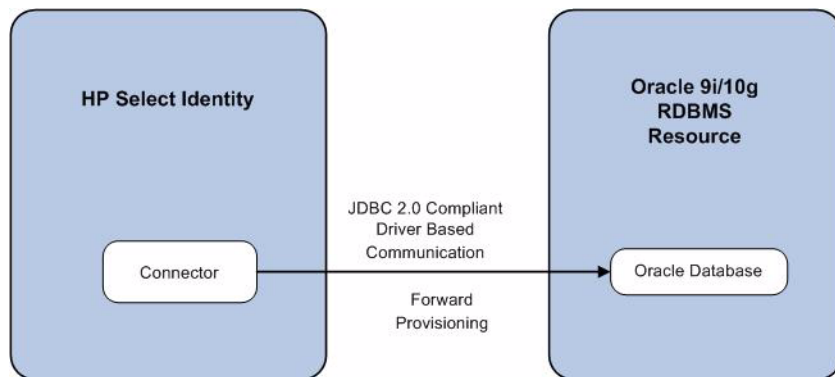
Figure 4 Connector Without Agent: JDBC Data Source Based Communication



Plan 3: Connector Without the Agent and with JDBC Driver

In this configuration, the connector communicates with the database by using a JDBC 2.0 compliant driver; no agent is installed on the database server. Reverse synchronization is not achieved in this configuration.

Figure 5 Connector Without Agent: JDBC 2.0 compliant Driver Based Communication



System Requirements

The Oracle Admin connector is supported in the following environment:

Table 4 Platform Matrix for Oracle Admin Connector

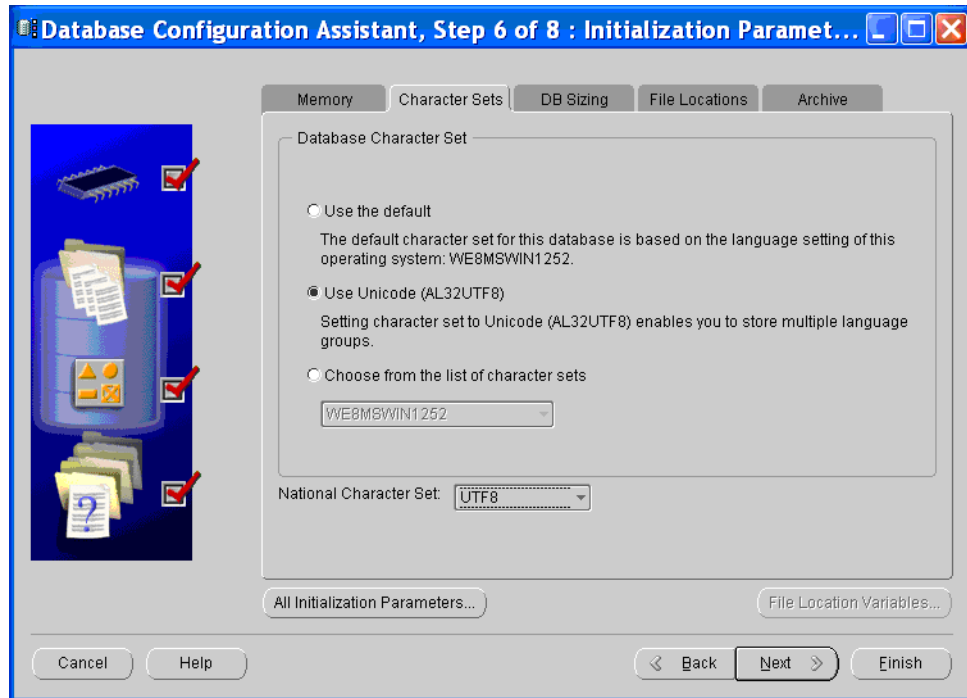
Select Identity Version	Application Server	Database
3.3.1	WebLogic 8.1.4 on Windows 2003	Microsoft SQL Server 2000
	WebLogic 8.1.4 on Solaris 9	Oracle 9i
	WebLogic 8.1.4 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on HP-UX 11i	Oracle 9i
	WebSphere 5.1.1 on Windows 2003	Oracle 9i
4.0-4.20	Oracle Admin connector is supported on all the platform configurations of Select Identity 4.0-4.20.	

The Oracle Admin connector is supported for Oracle 9i and 10g Database Servers on Windows 2003, Solaris 9, and HP-UX 11i.

For secure communication, this connector supports secure JDBC for database communication. See [Configuring Oracle to Support Secure JDBC](#) on page 19 for configuration information.

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

- The Select Identity server should be configured for internationalization. Refer to the *HP Select Identity Installation Guide* for more information.
- The Oracle database must be configured to support internationalization. The database must be in the UTF-8 encoding format. To configure the database for UTF-8 support, create or modify the database with the following settings for Character Sets using the Database Configuration Assistant tool:
 - Database Character Set: Use Unicode (AL32UTF8)
 - National Character Set: UTF8



Pre-Installation Task

Before you start installing, you must enable the communication mode between the connector and Oracle database according to you installation plan.

Enable JDBC Driver Based Communication

If Select Identity is deployed on WebSphere with Oracle as the backend database, skip this procedure as the Oracle JDBC Driver is already added to WebSphere CLASSPATH during Select Identity installation. You can obtain the SQL URL and the Driver String from the driver documentation (JDBC driver that has been used for Select Identity installation) and provide the same during resource creation on Select Identity.

To enable a JDBC 2.0 compliant driver based communication for any other deployment scenario, you must copy the file `classes111.zip` (or `classes111.jar`) on the Select Identity server. Perform the following steps to enable JDBC driver based communication:

- 1 Obtain the file `classes111.zip` or `classes111.jar`.
- 2 For Select Identity on WebLogic:
 - a Copy the files to a location on the Select Identity server.
 - b Add the file to the application server's CLASSPATH. To add the files to the application server's CLASSPATH:
 - Edit the startup script `myStartWL.cmd` for WebLogic on Windows.
 - Edit the startup script `myStartWL.sh` for WebLogic on UNIX.

- 3 For Select Identity on WebSphere (with Microsoft SQL Server as backend database, copy the JDBC driver file to `%WAS_HOME%/lib/ext/` where `%WAS_HOME%` is a location like `D:\WebSphere\AppServer`.

Enable JDBC Data Source Based Communication

To enable a JDBC data source based communication between the connector and the Oracle Admin database, you must create a new or use an existing JDBC data source and an underlying connection pool on the application server that hosts Select Identity.

While creating a new JDBC data source on WebLogic, you must do the following:

- Cancel the selection Honor Global Transactions.
- Select the option Emulate Two-Phase Commit for non-XA Driver.

While creating a new JDBC data source on WebSphere, you must do the following:

- Create the data source as J2C Authentication Data Entry for the target Oracle database user ID.
- Deploy the JDBC Provider. You must use only XA type driver to connect to the database (a non-XA driver conflicts with the existing JDBC data source of Select Identity).
- Create a data source for the JDBC Provider and provide a suitable JNDI name, which will be used during resource creation on Select Identity.



The target database must support (or must be configured to support) the connectivity through XA type driver. For example, you must install JTA related stored procedures on a target Microsoft SQL Server 2000 to create a JDBC provider by using an XA driver from WebSphere.

If the target database does not support this, JDBC driver based installation is recommended.

Extracting Contents of the Schema File

The Schema file (`AdminOracleSchema.zip`) contains the mapping information of the connector. Extract contents of this file to a location on the Select Identity server. You will obtain an XML file (`adminoracle.xml`) and an XSL file (`adminoracle.xsl`). Perform one of the following procedures depending on the application server ([WebLogic](#) or [WebSphere](#)) on which the connector will be deployed.

WebLogic

- 1 Identify a directory that is available in WebLogic CLASSPATH.
- 2 Place the XSL file under this directory.
- 3 Place the XML file in the path `com\trulogica\truaccess\connector\schema\spml` under this directory.

WebSphere

- 1 `<WebSphere_Install_Dir>/AppServer/lib/ext` is the default directory in WebSphere CLASSPATH. Place the XSL file directly under it.

- 2 Place the XML file in the path `com\trulogica\truaccess\connector\schema\spml` under the `<WebSphere_Install_Dir>/AppServer/lib/ext` directory.

Installing the Connector RAR

To install the RAR file of the connector (`Admin-Oracle-Connector.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.

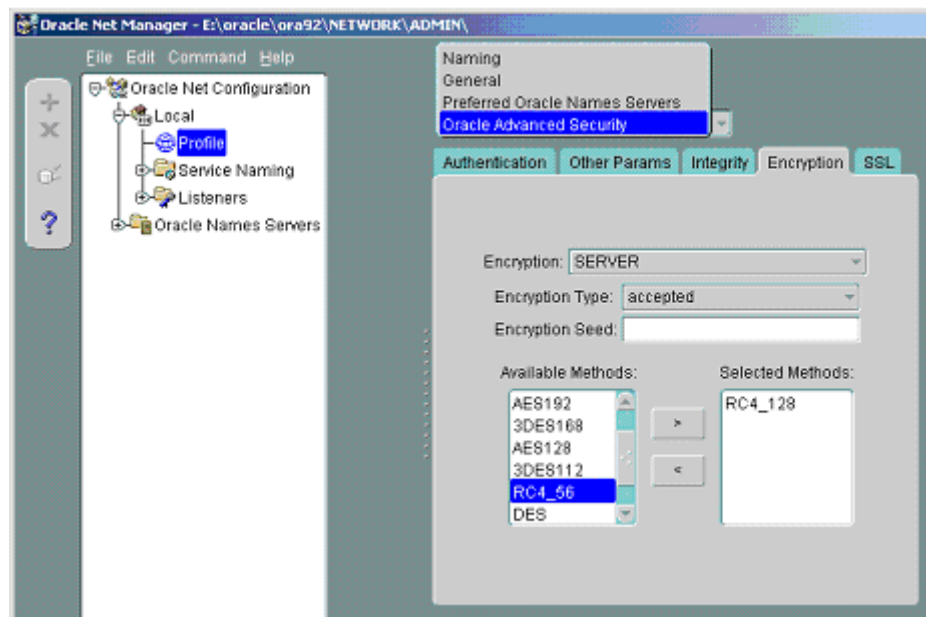


While deploying the RAR on WebSphere, enter the JNDI Pool Name as `eis/Admin-OracleConnector`.

Configuring Oracle to Support Secure JDBC

Perform the following steps to configure the Oracle server to support secure JDBC:

- 1 Start the Oracle Net Manager by entering the following command from `$ORACLE_HOME/bin`:
run netmgr
- 2 In the Navigator window, expand **Local** → **Profile**.
- 3 Select Oracle Advanced Security from the drop-down menu in the upper right side of the frame. The Oracle Advanced Security tabbed window appears.



- 4 Click the Encryption tab.
- 5 Select SERVER from the drop-down menu.
- 6 Select accepted from the Encryption Type drop-down menu.

- 7 Move the desired method(s) from the Available Methods list to the Selected Methods list.
- 8 For each method selected, ensure that you specify the same encryption method which will be entered in the Encryption Algorithm field while creating the connector resource (Table 5 on page 22). The following table illustrates the resulting security settings when the server-side settings for the accepted methods overlap with the client-side encryption settings. Ensure that the client and server settings are set such that an ON condition results.

	Client-Rejected	Client-Accepted (Default)	Client-Requested	Client-Required
Client-Rejected	OFF	OFF	OFF	Connection Fails
Client-Accepted (Default)	OFF	OFF	ON	ON
Client-Requested	OFF	ON	ON	ON
Client-Required	Connection Fails	ON	ON	ON

ON — Secure JDBC connection

OFF — Non-secure JDBC connection

Connection Fails — The connection between client and the server fails.

- 9 Select **File** → **Save Network Configuration**. The `sqlnet.ora` file is updated.

Make sure to enable SSL on the application server. For example, on WebLogic, select the currently running server and select the SSL Listener check box on the Security tab. You must restart the application server after enabling SSL.

4 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the Oracle Admin connector with Select Identity. At the end of this chapter, you will know the procedure to configure the Oracle Admin connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the Oracle Admin connector with Select Identity.

- 1 Add a New Connector
- 2 Add a New Resource
- 3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter `eis/Admin-OracleConnector`.
- Select **Yes** for the Mapper Available section.

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	Admin-Oracle	The name of the resource.	
Connector Name	AdminOracle	The newly deployed connector.	Known as Resource Type in Select Identity 3.3.1.
Authoritative Source*	No	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.	
Associate to Group		Whether the system uses the concept of groups. For this connector, select this option.	Applicable only for Select Identity 3.3.1.
Server Name	HP0111	Host name or IP address of the database server. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication.
Server Port	1521	Port on which the database server is listening. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication
Username	SYS AS SYSDBA	The login name of the database administrative user. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication
Password	P4ssword	Password of the database administrative user. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Agent Port	5601	The port where the agent listens for incoming connections. You must specify this parameter if the agent was installed.	Leave the field empty if you install the connector without agent
SQL URL	jdbc:oracle:thin	URL to use to communicate with the database over a JDBC connection. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication
Database / Service Name	testDB	The database name in which to provision users. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication
Database Driver String	oracle.jdbc.driver.OracleDriver	Name of the JDBC driver to connect to the database. You must specify this parameter if the agent was installed.	Leave the field empty if you configure the connector without agent for a JDBC data source based communication
Mapping File	adminoracle.xml	The XML mapping file, which must reside in <code>install/conf/com/truologica/truaccess/connector/schema/spml</code> directory in order for the Select Identity server to find it.	
JDBC Datasource String	Jdbc/SQLDataSource	JNDI data source name that was created or identified on the Select Identity server that can connect to the target Oracle database. Specify a value for this property if the agent was not installed.	Leave the field empty if you configure the connector for JDBC driver based communication (with or without agent).
Encryption Specification Algo	oracle.net.encryption_types_client	Encryption algorithm specification string.	

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Encryption Algorithm	RC4_128	Name of the encryption algorithm.	
Encryption Specification Level	oracle.net.encryption_client	Encryption level specification string. Specify this parameter if you wish to use secure communication with Oracle.	
Encryption Level	ACCEPTED	Encryption level. Specify this parameter if you wish to use secure communication with Oracle.	

*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.

Map Attributes

After successfully adding a resource for Oracle Admin connector, you must map the resource attributes to Select Identity attributes. Add new attributes to Select Identity if necessary.

While mapping the attributes, refer to the following table for Oracle attribute mapping information.

Table 6 Oracle Admin Mapping Information

Select Identity Resource Attribute	Attribute on Connector	Attribute on Physical (Oracle) Resource	Description
DefaultTablespace	DEFAULT_TABLESPACE	DEFAULT_TABLESPACE	The Default Tablespace name for the Database User being created. If no value is provided, the database default values are given to the user.
TemporaryTablespace	TEMPORARY_TABLESPACE	TEMPORARY_TABLESPACE	The TemporaryTablespace name for the Database User being created. If no value is provided, the database default values are given to the user.
Profile	PROFILE	PROFILE	The Profile that the user should be assigned to when being created on the database. If no value is provided, the database default values are given to the user.
External	EXTERNAL	EXTERNAL	The flag to identify whether the user is a 'Password Authentication' user or a 'External Authentication' user. 'Password Authentication' user-type is signified by FALSE (case-insensitive) or no-value is provided for 'External' attribute. When the value TRUE is given, the user is created as 'External Authentication' user.
UserName	USERNAME	USERNAME	The username of the account being created in Database. (mandatory field).
Password	PASSWORD		

Refer to the *HP Select Identity Connector Deployment Guide* for more information on mapping and creating attributes.

After mapping the attributes, you can use the connector to create a service, or you can associate the connector with an existing service. Refer to the *Service Studio* chapter of the *HP Select Identity Administration Online Help* for information on Select Identity services.

5 Installing the Agent

This chapter gives an overview of the agent for Oracle Admin connector and the procedure to install the agent on an Oracle database server. At the end of the chapter, you will be able to know about:

- The role of an agent.
- The procedure to install the agent.

About the Agent

The Oracle Admin connector agent performs forward provisioning operations on the resource and sends back any changes made on Oracle database to Select Identity web service in the form of SPML requests and sends back any changes made on Oracle database to Select Identity web service in the form of SPML requests. The connector is packaged with agent installers for the Windows, HP-UX, and Solaris platform.

When a user is added, modified, or deleted in the database, the agent captures the change from reverse notification table. The agent's reverse synchronization component then sends the change 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.

The Oracle Admin agent supports secure channel of communication to Select Identity web service by using HTTPS. You must configure the application server with Secure Socket Layer (SSL). You configure the agent to enable secure communication between agent and Select Identity in reverse synchronization. The agent automatically imports the certificate from Select Identity and initializes secure communication.

Installing the Agent on the Oracle Database Server

After you install the Oracle Admin connector on the Select Identity server, you can install the agent on the database server depending on your installation plan. If you do not need reverse synchronization ([Plan 2](#) and [Plan 3](#)), you can skip this chapter. However, agent installation is mandatory if you need reverse synchronization ([Plan 1](#)). The agent enables you to send data back to Select Identity.

Pre-Installation Tasks

Before you start installing the agent on Oracle database, make sure the following prerequisites are met:

- Copy the mapping files to the resource (Oracle database server) system as the agent installation requires the mapping files to be available on the local system.
- Copy the database driver file `classes111.zip` to the Oracle database system and they must be in the database server's `CLASSPATH`.
- Make sure that Java 1.4.2 (or above) is installed on the system and the `JAVA_HOME` environment variable is set. Also, ensure that `%JAVA_HOME%\bin` is specified in the `PATH` system variable.

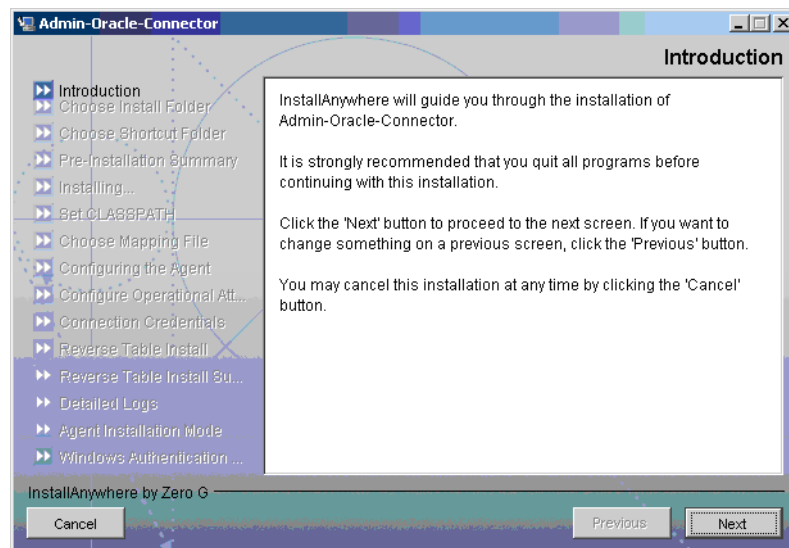
Also, you can pass the `LAX_VM` argument to point the wizard directly to the correct `java.exe` executable. For example: `install.exe LAX_VM c:\java14\bin\java.exe`

Install the Agent

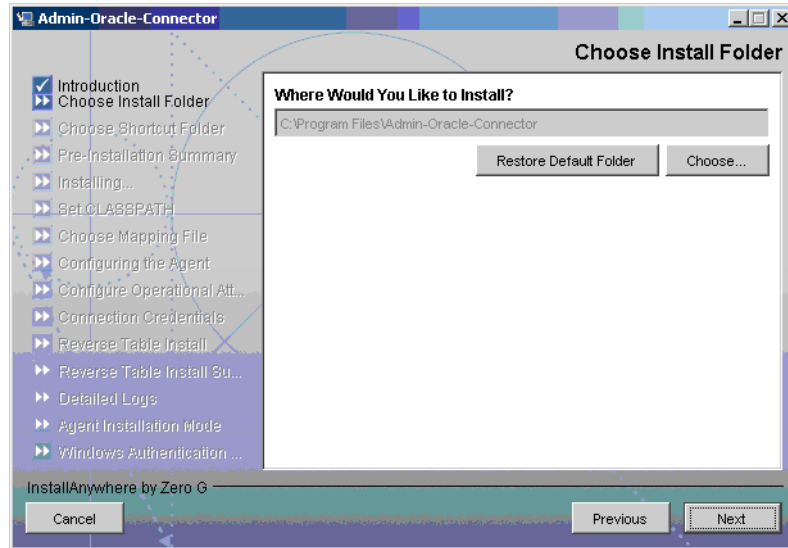
You can install the agent by using the installation wizard. The wizard is packaged in the file `Oracle-Admin-AgentInstaller-Win.zip` for installation on Windows, in the file `Oracle-Admin-AgentInstaller-Solaris.tar` for installation on Solaris, and in the file `Oracle-Admin-AgentInstaller-HPUX.tar` for installation on HP-UX. Perform the following steps to run the installation wizard and install the agent:

Windows

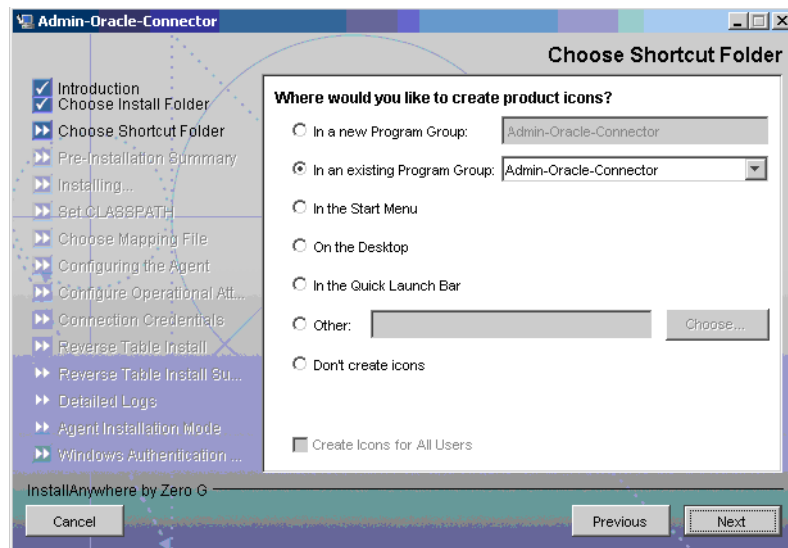
- 1 Extract the contents of the `Oracle-Admin-AgentInstaller-Win.zip` file, which is located in the Agent Installers directory on the CD.
- 2 Run `Admin-Oracle-Connector-Installer.exe`, which is located in the `target_dir\CDROM_Installers\Windows\Disk1\InstData\NoVM`. The Introduction screen appears:



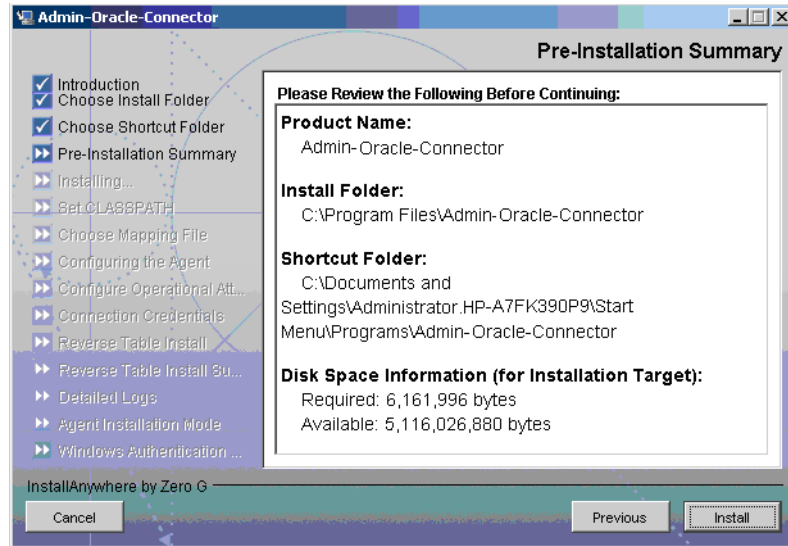
- 3 Click **Next**. The Choose Install Folder screen appears.



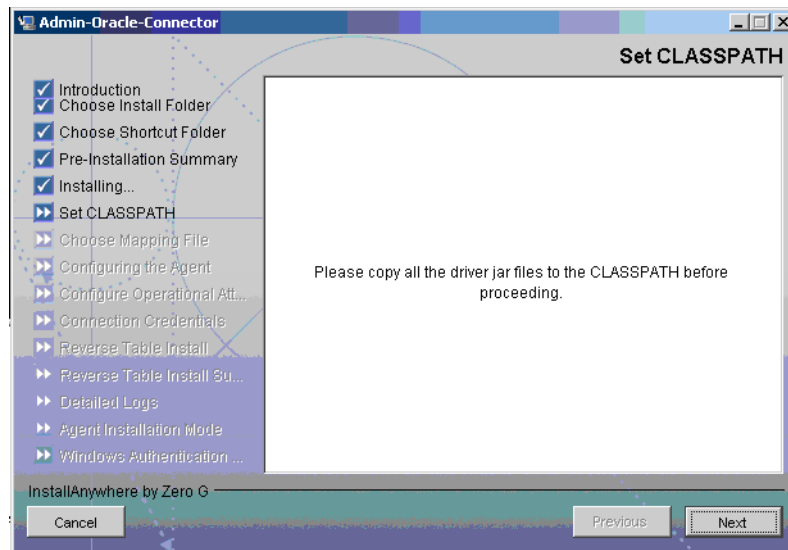
- 4 Keep the default location or click **Choose** to change the location, specify an installation directory, and then click **Next**. The Choose Shortcut Folder screen appears.



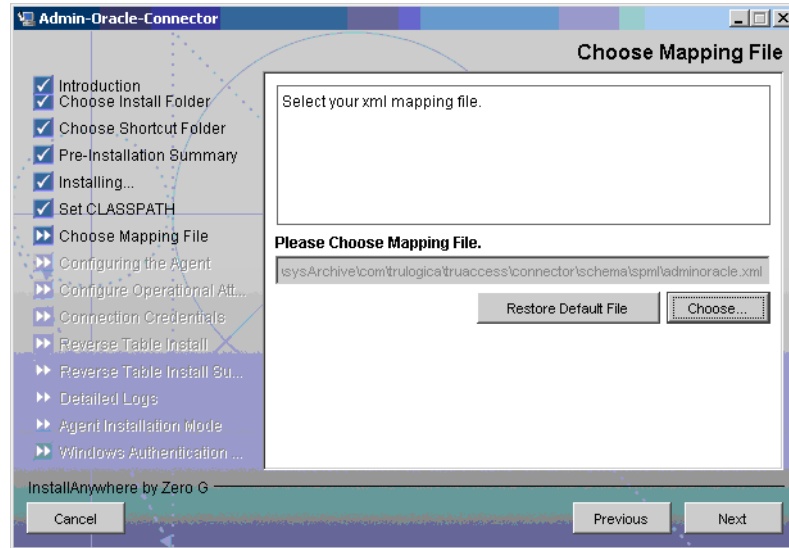
- 5 Select the location(s) where the product icons will be installed, and then click **Next**. The Pre-Installation screen appears.



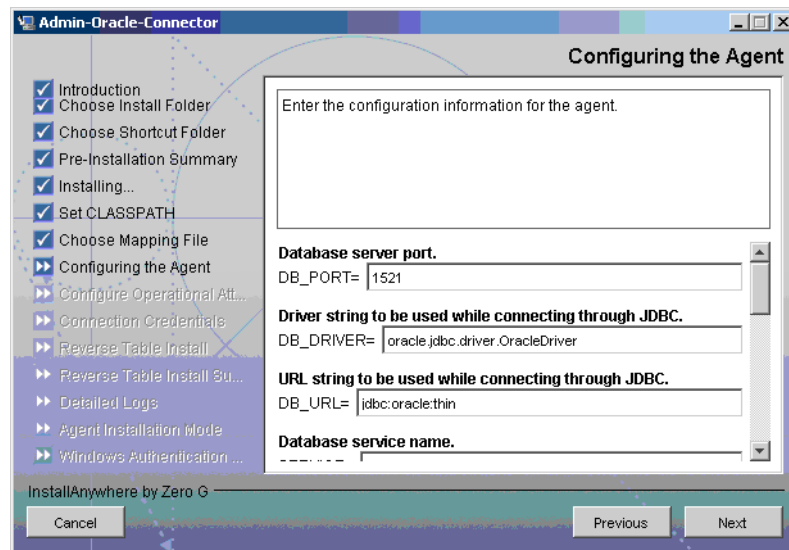
- 6 Review the pre-installation summary, click **Previous** if you want to change any setting, and then click **Install** to begin installation. During the course of installation, the Set CLASSPATH screen appears.



- 7 Verify that the database driver file (`classes111.zip`) is in the database server's system classpath, and then click **Next**. The Choose Mapping File screen appears.



- 8 Click **Choose** to browse for and select the mapping file. This will copy the mapping file to the `<install_dir>/conf/com/trulogica/truaccess/connector/schema/spml` directory, where `<install_dir>` is the installation folder.
- 9 Click **Next**. The Configuring the Agent screen appears.



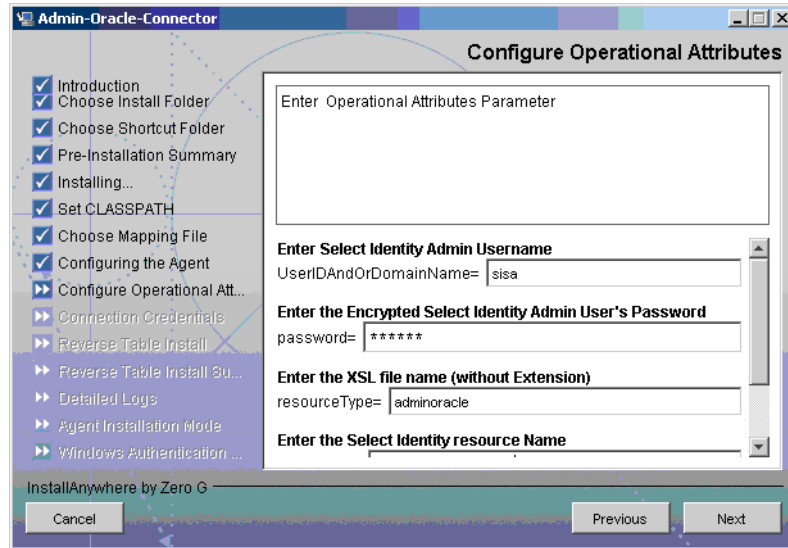
- 10 On the Configuring the Agent dialog, specify the configuration parameters, which are explained in the table below:

Parameter	Description	Example Value
DB_PORT	The port on which the database server is listening.	1521
DB_DRIVER	The JDBC driver for the database connection.	oracle.jdbc.driver.OracleDriver
DB_URL	The JDBC URL string used for the database communication.	jdbc:oracle:thin
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.	Select this check box if you want to establish a secure communication (HTTPS).
CONCERO_SERVER_URL	The URL of the Select Identity Web Service.	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
MAPPING_FILE	The XML mapping file.	adminoracle.xml
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**. The Configure Operational Attributes screen appears.

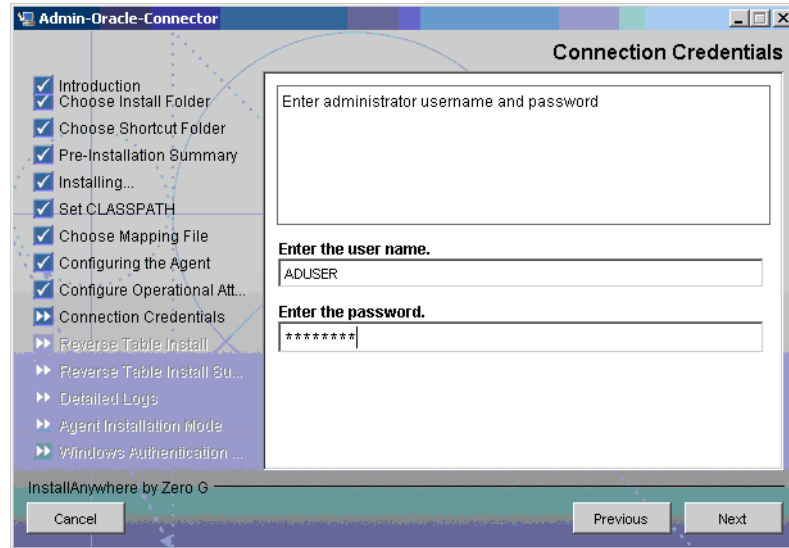


- 11 Provide the operational attributes that are sent to the Select Identity server during reverse synchronization requests. The table below gives a description of the attributes:

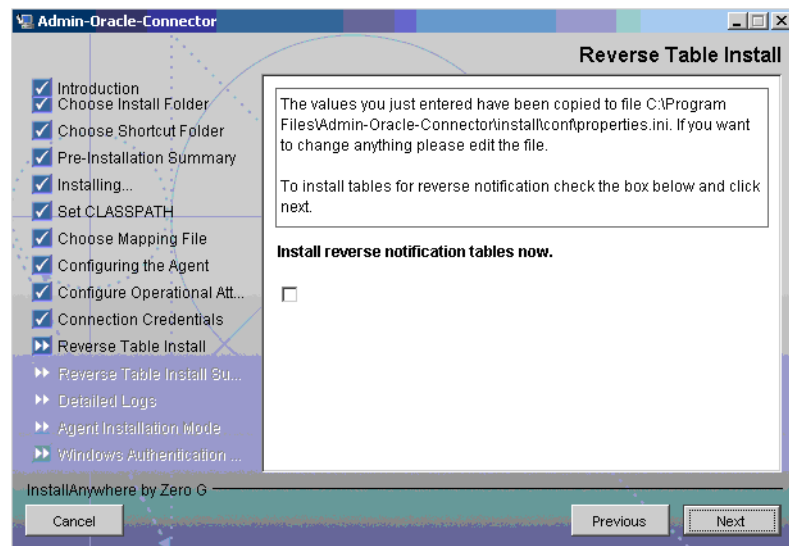
Attribute	Description
UserIDAndOrDomainName	User ID of the administrative user on Select Identity. For example, sisa.
password	Password of the administrative user.
reverseSync	Select this check box to enable reverse synchronization.
resourceType	The name of the XSL file (without the .xsl extension) that is used during reverse synchronization. For example, adminOracle.
resourceId	The name of the Select Identity resource that is created for the Oracle Admin connector. For example, AdminOracle-Resource.

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

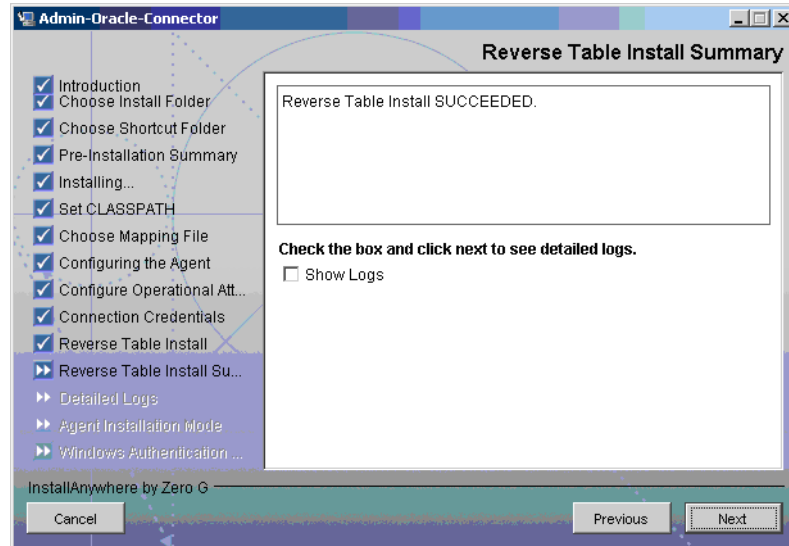
After entering the attributes, click **Next**. The Connection Credentials screen appears.



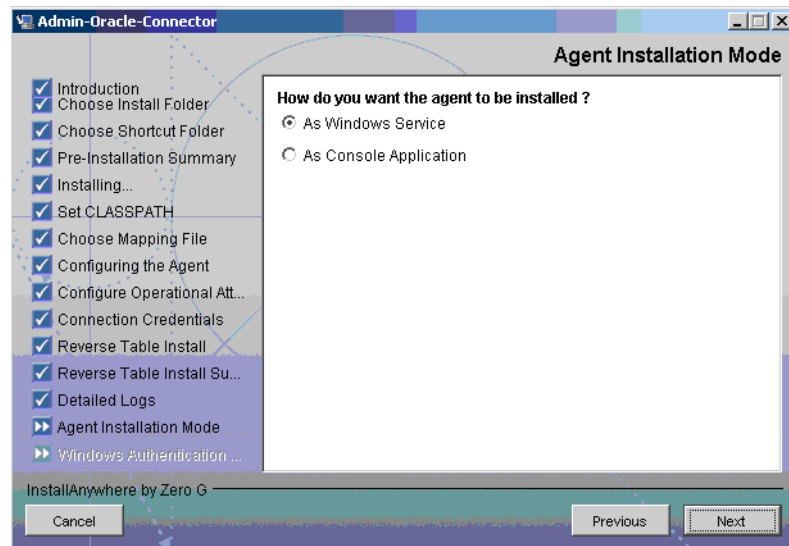
- 12 Enter Username/password for the Oracle database user with which the agent can connect to the Database. This user should have admin privileges, and then click **Next**. The Reverse Table Install screen appears.



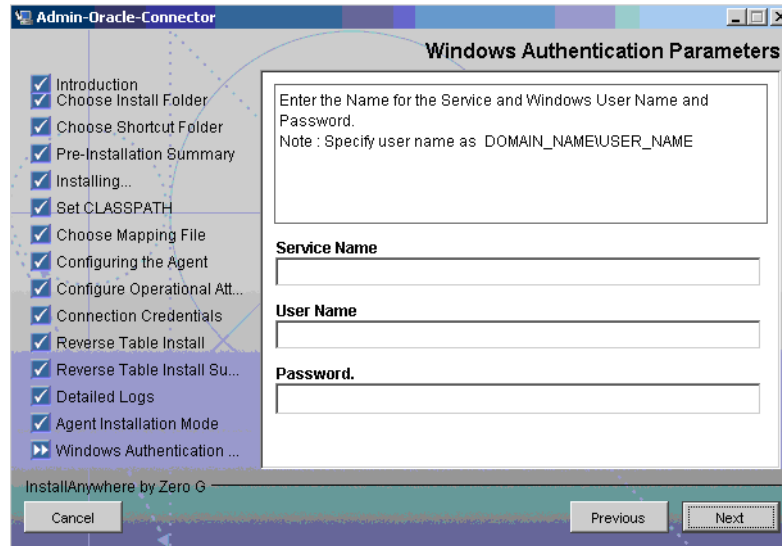
- 13 To enable reverse synchronization, select the Install reverse notification tables now check box, and then click **Next**. The Reverse Table Install Summary table appears.



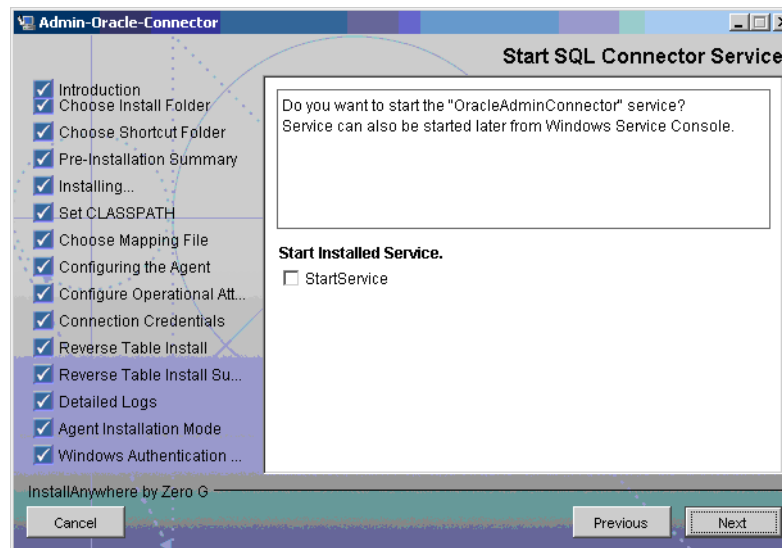
- 14 Select the ShowLog check box to view the detailed log, and then click **Next**. The Detailed Logs screen appears.
- 15 Click **Next**. The Agent Installation Mode screen appears.



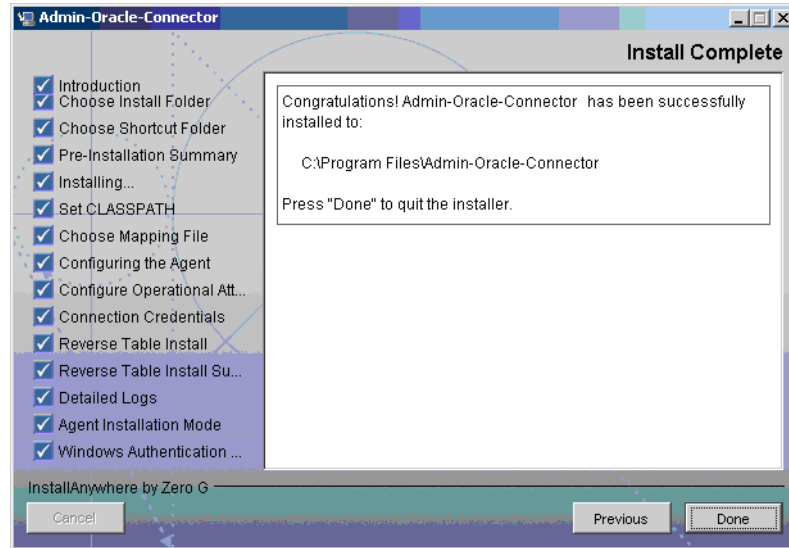
- 16 In the Agent Installation Mode screen, perform one of the following:
 - To run the agent as a Windows service, select the As Windows Service radio button, and then click **Next**. The Windows Authentication Parameters screen appears (step 17).
 - To run the agent as a console application, select the As Console Application radio button, and then click **Next**. The Install Complete screen appears (step 20).
- 17 The Windows Authentication Parameters screen displays the fields to enter the Windows username and password with administrative privilege, and the agent service name.



- 18 Type the agent service name and the administrative username and password for the Windows, and then click **Next**. The Start SQL Connector Service appears.



- 19 Select the StartService check box to start the agent service immediately after installation and **Next**. The Install Complete screen appears.



20 In the Install Complete screen, click **Done**.

UNIX (Solaris or HP-UX)

- 1 **Extract the contents of the** Oracle-Admin-AgentInstaller-HPUX.tar **or** Oracle-Admin-AgentInstaller-Solaris.tar **file (depending on the operating system on resource server), which are located in the Agent Installers directory on the CD, to a directory that will server as the agent's home directory. (Use** `tar xvf` **to extract the contents of the TAR file.) This will create the required directory structure in the Oracle-Gen-AgentInstaller-Solaris or Oracle-Gen-AgentInstaller-HP-UX subdirectory of the home directory.**

- 2 **Start the wizard by running the following command:**

```
agent_home/Oracle-Admin-AgentInstaller-Solaris.tar/  
AdminOracleConnector.bin
```

or

```
agent_home/Oracle-Admin-AgentInstaller-HPUX.tar/AdminOracleConnector.bin
```

The following message appears:

```
=====
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
Launching installer...
Preparing CONSOLE Mode Installation...
=====
```

```
(created with InstallAnywhere by Zero G)
```

```
-----
Choose Install Folder
-----
```

Where would you like to install?

Default Install Folder: /Admin-Oracle-Connector

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

- 3 **Specify the installation location of the agent. Enter a path and press** **ENTER**, **or press** **ENTER** **to accept default path. The following message appears:**

```

=====
Choose Link Location
-----
Where would you like to create links?
->1- Default: /
2- In your home folder
3- Choose another location...
4- Don't create links
ENTER THE NUMBER OF AN OPTION ABOVE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:

```

- 4 Select where you would like the agent shortcut location to be created. Select the number of the desired option as shown and press **ENTER**, or simply press **ENTER** to accept the default. The following message appears:

```

=====
Pre-Installation Summary
-----
Please Review the Following Before Continuing:
Product Name:
Admin-Oracle-Connector
Install Folder:
/install_dir
Link Folder:
/
Disk Space Information (for Installation Target):
Required: xxx bytes
Available: yyy bytes
PRESS <ENTER> TO CONTINUE:

```

- 5 Verify the pre-installation summary and press **ENTER**. The following message appears:

```

=====
Installing...
-----
[=====|=====|=====|=====]
[-----|-----|-----|-----]
=====
Configuring the Agent
-----
Enter the port number where database server listens. Hit <ENTER>
to accept default.
Enter DB_PORT : (DEFAULT: 1521 ):

```

- 6 Specify the database port number and press **ENTER** to continue, or simply press **ENTER** to accept the default. The following message appears:

```

=====
Configuring the Agent
-----
Enter the driver string (Driver string to be used by Java
program to connect to the database).
Enter the database driver : (DEFAULT: oracle.jdbc.driver.OracleDriver):

```

- 7 Enter the database driver and press **ENTER** to continue, or simply press **ENTER** to accept the default. The following message appears:

```

=====
Configuring the Agent

```

```
-----  
Enter the driver URL (URL to be used by Java program to connect  
to the database).  
Enter the database URL : (DEFAULT: jdbc:oracle:thin):
```

- 8 Enter the JDBC URL and press **ENTER** to continue, or simply press **ENTER** to accept the default. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the database service name.  
Enter the service name : (DEFAULT: ): SIDB
```

- 9 Enter the database name and press **ENTER** to continue, or press **ENTER** to accept the default. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enable Server Secure (Y/N) ?  
Enable Server Secure : (DEFAULT: N) : y
```

- 10 To enable secure communication, enter y and press **ENTER** to continue, or press **ENTER** to accept the default. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the URL where spml is to be sent by reverse sync.  
Enter the concero server URL : (DEFAULT: ): http://  
localhost:7001/lmz/webservice
```

- 11 Enter the URL of the Select Identity Web Service, which is where SPML requests are sent and press **ENTER** to continue. (If secure communication is enabled, you must specify the Web Service URL with HTTPS.), or press **ENTER** to accept the default. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the interval (in seconds) at which polling is desired for  
reverse sync.  
Enter poll delay : (DEFAULT: 10):
```

- 12 Enter the polling interval (in seconds) that is used by the agent to check for changes on the resource that must be sent to the Select Identity server (during reverse synchronization), and then press **ENTER**, or press **ENTER** to accept the default. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the port where the agent should listen.  
Enter the agent port : (DEFAULT: ):6000
```

- 13 Enter the listening port number for the agent and press **ENTER**, or simply press **ENTER** to accept the default and continue. The following message appears:

```
=====  
Configuring the Agent
```

```
-----  
Enter the time (in milli seconds) for which the agent should  
wait before sending SPML.  
Enter the spml delay : (DEFAULT: 100):
```

- 14 Specify the delay (in milliseconds) that the agent will wait before sending SPML requests to the Select Identity server and press **ENTER**, or simply press **ENTER** to accept the default and continue. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the Number of Retries to send SPML  
Number of Retries to send SPML : (DEFAULT: 3): 5
```

- 15 Specify the number of times agent will attempt to send SPML requests after a failure to the Select Identity server, and then press **ENTER**, or simply press **ENTER** to accept the default and continue. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter the time (in milliseconds) This is Delay Between Retries  
(Number of mSec the agent will wait before going to next Retry)  
Enter the spml retry delay : (DEFAULT: 100): 10000
```

- 16 Specify the delay (in milliseconds) for which agent should wait before attempting to send SPML requests again after a failure to the Select Identity server, and then press **ENTER**, or simply press **ENTER** to accept the default and continue. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter Directory Path of the XML mapping file. (e.g. If the  
mapping file is "/osd5/truologica/xxx.xml", enter "/osd5/  
truologica/" including slashes)  
Directory Path of the XML mapping file. (DEFAULT: ): /opt/
```

- 17 Enter the path to the mapping file (include trailing slashes but do not include the file name) and press **ENTER**, or simply press **ENTER** to accept the default setting. The following message appears:

```
=====  
Configuring the Agent  
-----  
Enter name of the XML mapping file. (Enter extension also.)  
Name of the XML mapping file. (Enter extension also.) (DEFAULT:  
) : adminoracle.xml
```

- 18 Enter the name of the mapping file and press **ENTER**, or simply press **ENTER** to accept the default setting. The following message appears:

```
=====  
XML Mapping Path  
-----  
This is your directory path of Mapping File  
"/opt/"  
This is the Mapping File  
"adminoracle.xml"  
Is it Correct Path?(Y/N) (DEFAULT: Y): y
```


- 19 Press **ENTER** to accept the default setting (**y**) or enter **n** and press **ENTER** to change the values. If you enter **y**, the following message appears:

```
=====
Configure Operation Attribute Parameter
-----
Enter Select Identity Admin Username
Select Identity Admin Username : (DEFAULT: ): sisa
```

- 20 Specify the Select Identity administrator's user name and press **ENTER**. The following message appears:

```
=====
Configure Operation Attribute Parameter
-----
Please Enter the Encrypted Select Identity Admin User's
Password: abc123
```

- 21 Enter the administrator's password and press **ENTER**. The following message appears:

```
=====
Configure Operation Attribute Parameter
-----
Enter the XSL file name (without Extension)
XSL file name (without Extension): (DEFAULT: ): adminOracle
```

- 22 Enter the name of XSL file on Select Identity server. Make sure that the extension (.xsl) is not specified, and then press **ENTER**. The following message appears:

```
=====
Configure Operation Attribute Parameter
-----
Enter the Select Identity resource name
Select Identity resource name : (DEFAULT: ): AdminOracleResource
```

- 23 Enter the name of the Select Identity Oracle database server resource and press **ENTER**. The following message appears:

```
=====
Configure Operation Attribute Parameter
-----
do you want to Enable Reverse Sync(true/false)?
Enable Reverse Sync? (Y/N) (DEFAULT: Y): y
```

- 24 Specify whether you want to enable reverse synchronization. Enter **n** or **y**, and then press **ENTER**. The following message appears:

```
=====
Connection Credentials
-----
Enter resource user name.
Enter Resource UserName: (DEFAULT: ): SYS as sysdba
=====
Connection Credentials
-----
This installation requires a password to continue.
Enter Resource Password : : password
```

- 25 Enter the Database User Account information to connect to the database and press **ENTER**. This user should have admin privileges. After entering the username and password, the agent installer attempts to connect to the database. If the connection is successfully established, the entries are written to the property files, and the following message appears:

```
=====
Reverse Notification Tables Install
-----

The values you just entered have been copied to file\
Admin-Oracle-Connector\conf\properties.ini. If you want to change
anything please edit the file.
Do you want to install reverse notification tables now? (Y/N)
(DEFAULT: Y) : y
```

- 26 To enable reverse synchronization, you must install the reverse notification tables. Enter **y** and press **ENTER** to install the tables (or simply press **ENTER** to accept the default setting), or enter **n** and press **ENTER** to bypass this installation. If you enter **y**, the following message appears:

```
=====
Reverse Notification Tables Install Summary
-----

Reverse Notification Tables Install SUCCEEDED.
PRESS <ENTER> TO CONTINUE:
```

- 27 Press **ENTER** to continue. The following message appears:

```
=====
View Logs
-----

Do you want to see detailed logs? (Y/N) (DEFAULT: Y): y
```

- 28 If you wish to view the installation log file, enter **y** and press **ENTER**. Otherwise, enter **n** and press **ENTER**. The following message appears:

```
=====
Agent Installation Mode
-----

Do you want to install agent as a Daemon process? (DEFAULT: Y)
```

- 29 To install the agent as a UNIX daemon, enter **y**, and then press **ENTER**. If you enter **y**, the following message appears:

```
=====
Get User Input
-----

Enter requested information
Enter Application Name for Daemon (DEFAULT: ): OracleAdminAgent
```

- 30 Enter the daemon name and press **ENTER**. The following message appears:

```
=====
Daemon Status
Starting OracleAdminAgent...
PRESS <ENTER> TO ACCEPT THE FOLLOWING (OK):
=====

Summary
-----

Congratulations! Admin-Oracle-Connector has been successfully installed
```

to:
 /space/Admin-Oracle-Connector
 PRESS <ENTER> TO CONTINUE:

31 To exit the installation wizard, press **ENTER**.

Installed Files

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

Directories and Files	Description
agent_home/	Contains the following files: <ul style="list-style-type: none"> • AddToStartupGroup.cmd/sh — Adds icons to startup group. • CopyFile.cmd/sh — Used by agent to copy files. • DelFile.cmd/sh — Used by agent to delete files. • AdminSetup.cmd/sh — Installs the reverse notification tables. • sqlapp.jar — Agent library JAR. • SQLConnectorConsole.cmd/sh — Starts the agent. • AdminUninstall.cmd/sh — Uninstalls reverse notification table. • passwordEncrypt.cmd/sh — Utility to populate Properties.ini and opAttributes.properties file with encrypted password. • PortTest.cmd/sh — The utility to check the availability of the port number mentioned in Properties.ini for agent. • LogonTest.cmd/sh — Utility to check the database connectivity.
agent_home/conf/	Contains the following files: <ul style="list-style-type: none"> • properties.ini — Provides configuration settings for the agent. • opAttributes.properties — Provides configuration settings for reverse synchronization. • log4j.properties — Provides settings for logging.
agent_home/conf/com	Contains the trulogica/truaccess/connector/schema/spml directory structure where the XML mapping file is stored.

Directories and Files	Description
agent_home/lib/	Contains JAR files used by the agent.
agent_home/logs	Contains log files produced by the agent.
agent_home/Uninstall_Admin-Oracle-Connector /	Contains files for uninstalling the agent.

Starting the Agent

To start the agent, run `SQLConnectorConsole.cmd` (on Windows) or `SQLConnectorConsole.sh` (on Solaris or HP-UX), 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.

The following is an example you can use on Windows:

```
<agent_home>/SQLConnectorConsole.cmd
```

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

Operating the Agent Daemon

If you install the agent on HP-UX or Solaris platform, perform the following steps to start or stop the daemon of the agent:

- 1 Go to the `<agent_home>/bin` directory.
- 2 Run the following command to start the daemon:

```
$ ./SQLConAgent start
```
- 3 Run the following command to stop the daemon:

```
$ ./SQLConAgent stop
```
- 4 Run the following command to view the status of the daemon:

```
$ ./SQLConAgent status
```

Modifying the Database Account and Select Identity Passwords

After the agent is installed, if you change the database account password or the Select Identity administrative password, you must update the agent with the change.

Perform the following steps on Oracle database server machine to update password change to the agent.

- To update the change in database password, run the following command on the Windows command prompt:

```
<install_dir>\passwordEncrypt.cmd -r <db-password>
```

where `<install_dir>` is the location of the agent and `<db-password>` is the new database password.

- To update the change in Select Identity administrative password, run the following command on the Windows command prompt:

```
<install_dir>\passwordEncrypt.cmd -s <ovsi-password>
```

where *<install_dir>* is the location of the agent and *<ovsi-password>* is the new Select Identity password.

6 Uninstalling the Connector

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

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

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

Uninstalling the Agent on Windows

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

- 1 Select **Programs** → **Admin-Oracle-Connector** → **Uninstall Agent** from the Start menu. The wizard appears.
- 2 Click **Next** on the introductory screen.
- 3 Provide the database credentials to uninstall the reverse tables, if they were installed.
- 4 Click **Uninstall**.
- 5 Click **Continue** when the pop-up dialog indicates that the reverse notification tables were successfully uninstalled.
- 6 Click **Done** on the Uninstall Complete screen to close the wizard.

Uninstalling the Agent on UNIX (Solaris or HP-UX)

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

- 1 Start the wizard by running the following command:
**agent_home/Uninstall_Admin-Oracle-Connector/
Uninstall_Admin-Oracle-Connector**

The following message appears:

```
=====
Preparing CONSOLE Mode Installation...
=====
(created with InstallAnywhere by Zero G)
-----
```

```
=====
Uninstall Admin-Oracle-Connector
-----
```

```
About to uninstall...
Admin-Oracle-Connector
This will remove features installed by InstallAnywhere. It will
not remove files and folders created after the installation.
PRESS <ENTER> TO CONTINUE:
```

- 2 Press **ENTER** to continue. The following displays:

```
=====
Get User Input
-----
Enter requested information
Enter user name : (DEFAULT: ): TEST
```

- 3 Enter the database user name and press **ENTER**. The following displays:

```
=====
Get User Input
-----
Enter requested information
Enter password : (DEFAULT: ): password
```

- 4 Enter the user's password and press **ENTER**. The installer removes the reverse notification tables (if installed) and displays a success or failure message, as follows:

```
=====
Executed the command
-----
"/Admin-Oracle-Connector/Uninstall.sh" -userName "TEST" -password
"password"
Reverse Notification Tables Uninstall Summary
Reverse Notification Tables Uninstall SUCCEEDED.
```

- 5 To view the log file, select the Show Logs and press **ENTER**.
- 6 Press **ENTER** to exit the wizard.

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.

Agent and Reverse Notification Table Installation

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

- 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 following error message is displayed:

Can't create view dbo.DBA_USERS Message received from the database: There is already an object named ... Cannot proceed.

Possible Cause: You are attempting to reinstall the agent without removing previously installed database tables.

Solution: Uninstall the agent as documented in [Uninstalling the Connector](#) on page 47. This removes previously installed tables. Then, run the agent installation wizard again.

- The following error message is displayed:

```
Exception occurred while starting reverse. Error message
receive: Io exception: Connection
refused(DESCRIPTION=(TMP=) (VSNNUM=135295488) (ERR=12505) (ERROR_S
TACK=(ERROR=(CODE=12505) (EMFI=4))))Error in logon. Can not
proceed.
```

Possible Cause: The wrong database service name was entered.

Solution: Verify the database service name in the `properties.ini` for correctness and ensure that the case of the name is correct (the name is case-sensitive).

- 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 tables, 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` variable to the path of Java version 1.4.

- An error message appears displaying JZ006 Exception. Cannot connect to database.

Possible Cause: The hostname may not be resolved to proper IP address of the database server.

Solution: Provide the proper IP address.

- During agent installation, error message appears displaying Invalid Login credentials even though correct values are provided for database username and password.

Possible Causes:

- `JAVA_HOME` environment variable is not set correctly or not set at all.
- The JDBC driver JARs are not placed in system `CLASSPATH`.
- The `commons-logging.jar` is present in the `JAVA_HOME/jre/lib/ext` folder.
- Other reasons that are not displayed in the log file.

Solutions:

- Set the `JAVA_HOME` up to the path from where the `bin` folder containing the `java.exe` file is accessible.
- Update the system `CLASSPATH` with paths JDBC Jars.

- Place the `log4j-1.2.8.jar` file along with the `commons-logging.jar` file in the same path.
- If the possible solutions mentioned above do not work, use `LogOnTest.cmd/sh` utility provided with the agent to debug the issue. You must run the utility from the command prompt as:

```
<agent_home_folder>/LogonTest.cmd -userName <db_username> -Password
<db_password>
```

This will try to establish connection to the database and display the result/error on the command window.

- While registering the Agent as a service, the Windows account name given is not accepted.

Possible Causes:

- The complete Windows account name (`<Domain_Name>/<user name>`) is not given.
- The local account is given in the form `localhost\administrator`.

Solutions:

- The installer needs the complete Windows username (with Domain Name) for registering the agent as service.
- The account names with `localhost` are not supported. Instead, machine name can be prefixed for local accounts. For example, `machine1\Administrato`

- An error message appears displaying `CREATE VIEW permission denied` in database while deploying the agent.

Possible Causes: The database user account used does not have all the necessary privileges to the database.

Solution: Select a user with proper privileges to install the agent.

- An error message appears displaying `Class Not Found Exception` caught `Can not establish connection to the DB` while deploying the agent.

Possible cause: The JDBC Driver files are not in system CLASSPATH of database server machine.

Solutions: Place the JDBC JAR files in system CLASSPATH.

- The agent service is registered but not starting.

Possible Causes:

- The user account provided does not have sufficient privileges.
- Multiple instances of JVM are running on the machine and agent is being invoked by an unsupported version of JRE (1.3 or 1.5). In this case, the logs show the following error:

```
Wrapper Started as Service
Launching a JVM...

| WrapperSimpleApp: Unable to locate the class
com.truologica.sql.conncore.commanager.ComManager:
java.lang.UnsupportedClassVersionError: com/truologica/truaccess/
connector/exception/TACConnectorException (Unsupported major.minor
version 48.0)
```

Solutions:

- Go to the Services window, right-click on the newly registered agent service, go to Properties, and then go to the LogOn tab. If This Account option is selected, cancel that selection and select the Local System Account option.
- Check the system if JREs of different versions are installed. Make sure that only JRE 1.4 is running and available in system PATH variable and JAVA_HOME.

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.
- 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.
- The following error is displayed:


```
SQLException occurred while adding element into SNAPSHOT_TAB. Message received from the database: table or view does not exist
```

Possible Cause: The agent is installed without the reverse notification tables.

Solution: Install the tables by running the installation, then run the agent.
- Error message appears displaying The system cannot find the path specified while running/starting the agent.

Possible Cause: The agent is not able to find JAVA in system PATH.

Solutions: Make sure that JAVA_HOME variable is set on database server machine and JAVA is available in system PATH.

B Connector Behavior

The following key behaviors are observed during forward provisioning:

- When certain optional attribute values are not specified when a user is added, the default database values are assigned to these fields. For example, for Profile, if the attribute is mapped and no value is specified during the addition of the user, the default value for this field (generally DEFAULT) is assigned to the user. In the same way, when no value is specified for any optional field during user modification, the previous value is retained.
- The OTHER_GROUPS consumer group cannot be linked to a user. An error appears displaying `cannot grant/revoke switch privilege for OTHER_GROUPS`.
- Some entitlements can be retrieved from the database but cannot be assigned to a user on the database. They are shown through the connector because they are present in the system tables. When such entitlements are linked from the connector, the database throws an exception that is caught by the connector and the operation will fail.
- When a user is added through forward provisioning, the UNLIMITED TABLESPACE entitlement is automatically linked to the user, which is reported to Select Identity in the form of SPML if the agent is running.
- When a user is linked to a consumer group, the stored procedure to link the user to the group automatically converts the user name to upper case; this leads to unexpected behavior. Hence, when any consumer group is assigned to a user that has a user name in lowercase characters, any further operation for that consumer group fails.
- CONSUMER GROUPS are not shown on the Enterprise Console of Oracle 10g. However, they are available in the system tables and, hence, the connector displays them with the list of entitlements and can be assigned to the user.
- The connector supports the creation of uppercase and lowercase user names on Oracle.
- The user's LOCK and UNLOCK options on Oracle are the STATUS attributes. These options are set when Enable All Services or Disable All Services are performed on Select Identity.

The following key behaviors are observed during reverse provisioning:

- A user that is connecting to the database through the agent should have the CREATE ANY VIEW entitlement, DBA role, and SELECT privilege on SYS.DBA_ROLE_PRIVS, SYS.DBA_SYS_PRIVS, and SYS.DBA_RSRC_CONSUMER_GROUP_PRIVS.
- The connector does not support the Expire Password operation on the Oracle database for a user.
- No SPML is generated for the Password Change operation on Oracle for a user. Hence, a user that is added through reverse synchronization from Oracle to Select Identity will have the default password, which is provided in the XSL file.

