Oracle® Identity Manager

Connector Guide for Siebel User Management

Release 9.0.4

E10445-06

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for Siebel User Management, Release 9.0.4

E10445-06

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Devanshi Mohan, Lyju Vadassery

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface

This guide provides information about Oracle Identity Manager Connector for Siebel User Management.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/oim.html

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at

http://www.oracle.com/technology/documentation/index.html

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in Oracle Identity Manager Connector for Siebel User Management?

This chapter provides an overview of the updates made to the software and documentation for the Siebel User Management connector in release 9.0.4.8.

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following sections discuss updates made from release 9.0.4 to the current release of the connector:

- Software Updates in Release 9.0.4.1
- Software Updates in Release 9.0.4.1_6713023
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.8

Software Updates in Release 9.0.4.1

The following is a software update in release 9.0.4.1:

- Changes in the Directory Structure of the Connector Files on the Installation Media

Changes in the Directory Structure of the Connector Files on the Installation Media

The `xlSiebel.jar` file has been split into two files, `xlSiebel.jar` and `SiebelRecon.jar`. Corresponding changes have been made in the following sections:

- Files and Directories on the Installation Media
- Determining the Release Number of the Connector
- Copying the Connector Files
- Running Test Cases

Software Updates in Release 9.0.4.1_6713023

The following are issues resolved in release 9.0.4.1_6713023:

Bug Number	Issue	Resolution
6713023	User reconciliation and provisioning did not work due to connection failure.	The issue has been resolved.

Software Updates in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7014401	Time zone values that you set during provisioning was not displayed on the target system.	This issue has been resolved. The time zone value is correctly stored during provisioning.

Software Updates in Release 9.0.4.3

The following are software updates implemented in release 9.0.4.3:

- Using the Connector Installer

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-4 for details.

Software Updates in Release 9.0.4.4

The following are issues resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
7308907	Incremental reconciliation failed if the target system database was set to any time zone other than GMT. For example, if the time zone of the target system database was set to GMT+08:00, then incremental reconciliation would fail.	This issue has been resolved. The `SiebelDatabaseTimeZone` attribute has been added to the `Siebel Recon` scheduled task. You can use this attribute to specify the time zone of the target system database. See "User Reconciliation Scheduled Task" on page 3-5 for more information about the `SiebelDatabaseTimeZone` attribute.

Software Updates in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
7308907	The connector uses the time stamp stored in the TimeStamp IT resource parameter to identify target system records that must be reconciled. However, daylight savings time was not taken into account.	This issue has been resolved. The DayLightSaving attribute has been added to the SiebelRecon task. You use this attribute to specify the time (in minutes) that must be added to the time stamp. Sample value: `60` With this sample value, 60 minutes are added to the time stamp stored in the TimeStamp parameter, and the new time stamp is used to identify records that have been created or modified after the last reconciliation run. Default value: `0` **Note:** The SiebelDatabaseTimeZone attribute of the SiebelRecon scheduled task has been renamed to SiebelServerTimeZone.
7163582	The following issue was observed when the target system was Siebel 8.0: In a provisioning operation, if you tried to assign a responsibility to a user who had no responsibilities, then the connection exception was encountered.	This issue has been resolved. In a provisioning operation, you can now assign responsibilities to a user who does not have any responsibilities.
7561587	You could not set a primary responsibility to a user through a provisioning operation.	This issue has been resolved. You can now use the PrimaryResponsibility lookup field to set a primary responsibility during provisioning. **See Also:** Bug 7703095 in the "Known Issues" chapter for information about an issue related to this feature.
6847114	On the target system, if a position name was used across more than one division, then only one occurrence of the position name was reconciled into the Lookup.Siebel.Position lookup definition.	This issue has been resolved. Position names are reconciled according to their unique IDs on the target system. The following are sample entries from the Lookup.Siebel.Position lookup definition: Code Key1: `0-55RNY` Decode1: `Finance, General Manager` Code Key2: `0-57T1J` Decode2: `Sales, General Manager`
7668306	If a responsibility name reconciled from the target system contained a special character, then that responsibility could not be assigned to a user through a provisioning operation.	This issue has been resolved. Responsibilities whose names contain special characters, except the single quotation mark character ('), can now be assigned to user through provisioning. **Note:** A responsibility whose name contains the single quotation mark (') character cannot be assigned to a user through provisioning. This is because the target system cannot search for a responsibility name if it contains a single quotation mark.
7667566	An exception was encountered if you deleted a user's position through a provisioning operation.	This issue has been resolved. You can delete a user's responsibility through provisioning.

Bug Number	Issue	Resolution
7673332	A user's status was Inactive even when one or more responsibilities were assigned to the user through provisioning.	This issue has been resolved. If a user has no responsibilities assigned, then the status of the user is set to Inactive. If you assign responsibilities to the user through provisioning, then the status is changed to Active.

Software Updates in Release 9.0.4.6

The following are software updates implemented in release 9.0.4.6:

- Support for Siebel 8.1.1
- Resolved Issues in Release 9.0.4.6

Support for Siebel 8.1.1

From this release onward, the connector supports Siebel 8.1.1. This is mentioned in the "Verifying Deployment Requirements" section.

Resolved Issues in Release 9.0.4.6

The following table describes issues resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
8223113	When you assign a primary position to an employee through a provisioning operation on Oracle Identity Manager, the change is correctly reflected in the Administration – User module on the target system. However, in the Administration – Group module, the check box designating that the position is primary for that particular employee remains deselected.	This issue has been resolved. The relationship between an employee and a primary position is correctly shown in the Administration – Group module. The "Assigning a Position to Users" section has been removed from the connector guide.

Software Updates in Release 9.0.4.7

The following table describes issues resolved in release 9.0.4.7:

Bug Number	Issue	Resolution
7579522	When you assigned a primary position to an employee through a provisioning operation on Oracle Identity Manager, the employee became the primary user for the position. When you assigned the same primary position to another employee, this employee became the new primary user for the position. In this way, the primary user of the position kept changing with each assignment of the position.	This issue has been resolved. The first employee to whom the position is assigned remains the primary user of the position.

Software Updates in Release 9.0.4.8

The following table describes issues resolved in release 9.0.4.8:

Bug Number	Issue	Resolution
8362522	The connector did not work correctly if Oracle Identity Manager and Oracle Access Manager both used the same object manager (CommunicationsObjMgr_enu). The following error was encountered during password operations:	This issue has been resolved. The connector functions as expected even if Oracle Identity Manager and Oracle Access Manager are using the same object manager.
	`The password you have entered is not correct. Please enter your password again.(SBL-DAT-00569)`	The `SSO` and `Trusted Token` parameters have been added in the IT resource definition.

Documentation-Specific Updates

The following sections discuss documentation-specific updates in the guide:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.6
- Documentation-Specific Updates in Release 9.0.4.7
- Documentation-Specific Updates in Release 9.0.4.8

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.6

The following documentation-specific updates have been made in the guide from release 9.0.4.1 through 9.0.4.6:

- The external code files for Siebel 7.6, 7.7, and 7.9 have been documented in the following sections:
  - Verifying Deployment Requirements section on page 2-1
  - Copying the Connector Files section on page 2-8
- In the "Reconciled Resource Object Fields" section, the following fields have been added:
  - Extension
  - HomePhone
  - WorkPhone
  - MPosition
  - Title

  The `Phone` and `PersonalTitle` fields have been removed from the list.
- In the "Importing the Connector XML Files" section, the `SiebelServerPort` parameter has been renamed to `GatewayServerPort`.
- In the "Partial Reconciliation" section:
  - All occurrences of `givenname` have been replaced with `First Name`.
  - All occurrences of `sn` have been replaced with `Last Name`.
- In the "Known Issues" chapter, limitations of the target system have been separated from the known issues of the connector.
- The "Creating the Target System User Account for Connector Operations" has been added.

Documentation-Specific Updates in Release 9.0.4.7

In the "Configuring the Connector" chapter, the "Configuring the Connector for Multiple Installations of the Target System" section has been removed. This feature is not supported by default.

Documentation-Specific Updates in Release 9.0.4.8

The following documentation-specific updates have been made in the guide for release 9.0.4.8:

- The following sections have been added:
  - Adding the Dependent (LDAP Connector) Resource Object for Provisioning
  - Additional Configuration Steps and Guidelines for the Target System
- In the "Multilanguage Support" section, Arabic has been added to the list of languages that the connector supports.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with Siebel Enterprise Applications.

This chapter contains the following sections:

Note: In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

At some places in this guide, Siebel Enterprise Applications has been referred to as the *target system*.

1.1 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

See Also: The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about reconciliation configurations

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

1.1.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields:

- Lookup.Siebel.TimeZone
- Lookup.Siebel.PreferredCommunications
- Lookup.Siebel.Position
- Lookup.Siebel.EmployeeTypeCode
- Lookup.Siebel.Responsibility
- Lookup.Siebel.PersonalTitle
- Lookup.Siebel.UserType

1.1.2 User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

1.1.2.1 Reconciled Resource Object Fields

The following fields are reconciled:

- UserID
- First Name
- Last Name
- Middle Name
- Alias
- JobTitle
- EmployeeType
- Title
- E-mail
- Fax
- Time Zone
- Position
- Responsibility
- Primary Responsibility
- Preferred Communications
- Extension
- HomePhone
- WorkPhone
- MPosition

1.1.2.2 Reconciled Xellerate User (OIM User) Fields

The following fields are reconciled only if reconciliation is implemented in trusted mode:

- UserID
- FirstName
- LastName

- Email
- Organization
- User Type
- Employee Type

1.2 Provisioning Module

Provisioning involves creating or modifying a user's account on the target system through Oracle Identity Manager. You use the Oracle Identity Manager Administrative and User Console to perform provisioning operations.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- UserID
- First Name
- Last Name
- Middle Name
- Alias
- Job Title
- EmployeeType
- PersonalTitle
- E-mail
- Fax
- Phone
- Time Zone
- Position
- Primary Responsibility
- Responsibility
- Preferred Communications
- IT Resource Type

1.3 Supported Functionality

The following table lists the functions that are available with this connector.

Function	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Add Position to User	Provisioning	Adds a position to a user

Function	Type	Description
Add User Responsibility	Provisioning	Adds a responsibility to a user
Delete User Position	Provisioning	Deletes the position of a user
Delete User Responsibility	Provisioning	Deletes the responsibility of a user
Primary Position Updated	Provisioning	Updates the Primary Position of a user
Primary Responsibility Updated	Provisioning	Updates the Primary Responsibility of a user
Time Zone Updated	Provisioning	Updates the time zone of a user
Email Updated	Provisioning	Updates the e-mail address of a user
Alias Updated	Provisioning	Updates the alias of a user
MI Updated	Provisioning	Updates the middle name of a user
Work Phone Updated	Provisioning	Updates the work phone number of a user
First Name Updated	Provisioning	Updates the first name of a user
Last Name Updated	Provisioning	Updates the last name of a user
Title Updated	Provisioning	Updates the title of a user
Home Phone Updated	Provisioning	Updates the home phone number of a user
Fax Updated	Provisioning	Updates the fax number of a user
Preferred Communications Updated	Provisioning	Updates the preferred communications setting of a user
Extension Updated	Provisioning	Updates the extension number of a user
Employee Type Updated	Provisioning	Updates the role of a user
Job Title Updated	Provisioning	Updates the job title of a user
Reconciliation Delete Received	Reconciliation	Deletes the user from Oracle Identity Manager if the user has been deleted from the target system
Reconciliation Insert Received	Reconciliation	Inserts a user in Oracle Identity Manager
Reconciliation Update Received	Reconciliation	Updates a user in Oracle Identity Manager

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and the target system.

1.4 Multilanguage Support

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese

- Korean
- Portuguese (Brazilian)
- Spanish

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

1.5 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`configuration/SeibelConnector-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/xlSiebel.jar`	This JAR file contains the class files that are required for provisioning. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/JavaTasks`
`lib/SiebelRecon.jar`	This JAR file contains the class files that are required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*`/xellerate/connectorResources` **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`Troubleshoot/TroubleShootingUtility.class`	This is the standalone class that interacts with the target system. This class contains the code for running the troubleshooting test cases.
`Troubleshoot/global.properties`	This file contains the connection details that are required to connect to the target system. It also contains details about the commands to be run.

Table 1–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`Troubleshoot/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`xml/SiebelEmpResourceObject.xml`	This XML file contains definitions for the following connector components: ■ IT resource type ■ Process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Pre-populate rules
`xml/SiebelEmpXLResourceObject.xml`	This file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the `Troubleshoot` directory are used only to run tests on the connector.

1.6 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME`/xellerate/JavaTasks/xlSiebel.jar`

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xlSiebel.jar` file.

   In the `manifest.mf` file, the release number of the connector is displayed as the value of the Version property.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Using External Code Files
- Creating the Target System User Account for Connector Operations
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x
- Configuring the Oracle Identity Manager Server
- Configuring the Target System for Encryption

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	Siebel 7.5 through Siebel CRM 8.1.1

External code	For Siebel 7.5 through 7.7:
	`SiebelJI.jar`, `SiebelJI_Common.jar`, and `SiebelJI_enu.jar`
	For Siebel 7.8 through 8.1.1:
	`Siebel.jar` and `SiebelJI_enu.jar`

Target system user account	Create a target system user account with the rights required to perform reconciliation and provisioning operations. See "Creating the Target System User Account for Connector Operations" for more information.

2.2 Using External Code Files

> **Note:** While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the `ThirdParty` directory to the corresponding directories on each node of the cluster.

If you are using Siebel 7.5 or 7.6 or 7.7, then copy the following files from the *`Siebel7.x_installation_directory`*`/siebsrvr/CLASSES` directory into the `OIM_HOME/xellerate/ThirdParty` directory:

- `SiebelJI.jar`
- `SiebelJI_Common.jar`
- `SiebelJI_enu.jar`

If you are using Siebel 7.8 or 7.9 or 8.0, then copy the following files from the *`Siebelx.x_installation_directory`*`/siebsrvr/CLASSES` directory into the `OIM_HOME/xellerate/ThirdParty` directory:

- `Siebel.jar`
- `SiebelJI_enu.jar`

2.3 Creating the Target System User Account for Connector Operations

Oracle Identity Manager uses a target system user account to provision to and reconcile data from the target system. To create this target system user account with the permissions required for performing connector operations:

> **Note:** The target system user account that you create for connector operations must also be created in the LDAP repository. As a security precaution, you must ensure that this account does not have access to areas protected by Oracle Access Manager.

1. Create the user account on Siebel as follows:
   a. Log in to Siebel.
   b. Click the Site Map icon.
   c. Click **Administration – User**.
   d. Click **Employees**.
   e. Click **New**.
   f. Enter the following details for the account that you are creating:
      – Last Name
      – First Name
      – Job Title
      – User ID
      – Responsibility: Select **Siebel Administrator**.

- Position: Select **Siebel Administrator**.
- Organization: Select **Default Organization**.
- Employee Type

2. Create the user account on the Siebel database as follows:
   a. Open the Siebel home directory.
   b. Open the `dbsrvr` directory.
   c. Open one of the following directories:

      For IBM DB2 UDB: `DB2`

      For Microsoft SQL Server: `MSSQL`

      For Oracle Database: `Oracle`
   d. Open one of the following files in a text editor:

      For IBM DB2 UDB: `grantusrdb2.sql`

      For Microsoft SQL Server: `addusrmsql.sql`

      For Oracle Database: `grantusroracle.sql`
   e. In the file that you open:

      Specify the user ID of the user that you create in Step 1.

      Set a password for the user.

      Provide other required details.
   f. Run the script.

Additional Configuration Steps and Guidelines for the Target System

You must ensure that the following prerequisites are addressed and guidelines are followed:

- Siebel must be configured to use one of the following security adapters:
  - If Microsoft Active Directory is used as the LDAP repository, then use the ADSI Security Adapter. Ensure that the Propagate Change attribute of the ADSI Security Adapter is set to False on Siebel.
  - If any other LDAP solution is used, then use the LDAP Security Adapter.

  Note: Only LDAP solutions for which there are predefined Oracle Identity Manager connectors are supported.

- Users must first be created in the LDAP repository and then created on the target system. This also means that users created through provisioning operations performed on Oracle Identity Manager must first be created in the LDAP repository and then created on the target system.
- Ensure that the credential attribute is correctly set for users created in the LDAP repository. For example, on Microsoft Active Directory the credential attribute is the Office attribute. The format for Office attribute values is as follows:

  `username=`*`USER_ID_OF_SIEBEL_ACCOUNT`* `password=`*`PASSWORD_OF_SIEBEL_ACCOUNT`*

  The following is a sample value:

```
username=jdoe password=Ke42r0s
```

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

Note: In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.4.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.
4. From the Connector List list, select **Seibel Connector *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME/xellerate/ConnectorDefaultDirectory

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **Seibel Connector *RELEASE_NUMBER*.**
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry.**
- Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed

   Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-11 for information about running the `PurgeCache` utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled tasks that are created when you installed the connector

   Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 1–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See "Files and Directories on the Installation Media" on page 1-5 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

You must specify values for the parameters of the `SIEBEL IT Resource` IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `SIEBEL IT Resource` and then click **Search**.
5. Click the edit icon for the IT resource.

6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Description	Sample/Default Value
EnterpriseServer	Name of the Enterprise server	siebel
GatewayServer	Name of the Gateway server	STS_TESTING
GatewayServerPort	Listening port number for the SCBroker component	2321
Language	Language	You can specify any one of the following: For English: ENU For Brazilian Portuguese: PTB For French: FRA For German: DEU For Italian: ITA For Japanese: JPN For Korean: KOR For Simplified Chinese: CHS For Spanish: ESP For Traditional Chinese: CHT
ObjectManager	Name of the object manager	You can specify any one of the following: For English: eSCCObjMgr_enu For Brazilian Portuguese: eSCCObjMgr_ptb For French: eSCCObjMgr_fra For German: eSCCObjMgr_deu For Italian: eSCCObjMgr_ita For Japanese: eSCCObjMgr_jpn For Korean: eSCCObjMgr_kor For Simplified Chinese: eSCCObjMgr_chs For Spanish: eSCCObjMgr_esp For Traditional Chinese: eSCCObjMgr_cht
Password	Password of the target system user account that you want to use for connector operations See "Creating the Target System User Account for Connector Operations" for more information.	sadmin
SiebelServer	Name of the target system server	STS_TESTING
UserName	User ID of the target system user account that you want to use for connector operations See "Creating the Target System User Account for Connector Operations" for more information.	sadmin

Parameter	Description	Sample/Default Value
Encryption	Type of encryption for secure communication **Note:** The value of this parameter is case-sensitive.	If encryption is required, then specify RSA. Otherwise, specify None.
Version	Version of the target system supported by this connector	7.5 or 7.8
TimeStamp	For the first reconciliation run, the times-tamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.	The following are sample timestamp values: For English: Jun 01, 2006 at 10:00:00 GMT+05:30 For French: juil. 01, 2006 at 10:00:00 GMT+05:30 For Japanese: 6 01, 2006 at 10:00:00 GMT+05:30
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.	First Name=John&Last Name=Doe
SSO	Enter yes to specify that the target system is configured to use a SSO solution for authentication. Otherwise, enter no.	no
Trusted Token	Enter the trusted token value that you specify while configuring the target system to communicate with the SSO system. If you have not configured SSO authentication, then enter no.	no

8. To save the values, click **Update**.

2.5 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.x involves the following procedures:

- Copying the Connector Files
- Importing the Connector XML Files

2.5.1 Copying the Connector Files

The connector files to be copied and the directories to which you must copy them are given in the following table.

See Also: "Files and Directories on the Installation Media" on page 1-5 for more information about these files

File in the Installation Media Directory	Destination Directory
`lib/xlSiebel.jar`	*OIM_HOME*`/xellerate/JavaTasks`
`lib/SiebelRecon.jar`	*OIM_HOME*`/xellerate/ScheduleTask`
Files in the `resources` directory	*OIM_HOME*`/xellerate/connectorResources`
Files in the `Troubleshoot` directory	*OIM_HOME*`/xellerate/Siebel/Troubleshoot`
Files in the `xml` directory	*OIM_HOME*`/xellerate/Siebel/xml`

Note: In a clustered environment, copy the JAR files and the contents of the `connectorResources` directory to the corresponding directories on each node of the cluster.

2.5.2 Importing the Connector XML Files

As mentioned in the "Files and Directories on the Installation Media" section on page 1-5, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `SiebelEmpResourceObject.xml` file, which is in the *OIM_HOME*`/xellerate/Siebel/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `SIEBEL IT Resource` IT resource is displayed.
8. Specify values for the parameters of the `SIEBEL IT Resource` IT resource. Refer to the following table for information about the values to be specified:

Parameter	Description	Sample/Default Value
`EnterpriseServer`	Name of the Enterprise server	`siebel`
`GatewayServer`	Name of the Gateway server	`STS_TESTING`
`GatewayServerPort`	Listening port number for the SCBroker component	`2321`

Parameter	Description	Sample/Default Value
Language	Language	You can specify any one of the following: For English: ENU For Brazilian Portuguese: PTB For French: FRA For German: DEU For Italian: ITA For Japanese: JPN For Korean: KOR For Simplified Chinese: CHS For Spanish: ESP For Traditional Chinese: CHT
ObjectManager	Name of the object manager	You can specify any one of the following: For English: eSCCObjMgr_enu For Brazilian Portuguese: eSCCObjMgr_ptb For French: eSCCObjMgr_fra For German: eSCCObjMgr_deu For Italian: eSCCObjMgr_ita For Japanese: eSCCObjMgr_jpn For Korean: eSCCObjMgr_kor For Simplified Chinese: eSCCObjMgr_chs For Spanish: eSCCObjMgr_esp For Traditional Chinese: eSCCObjMgr_cht
Password	Password of the target system user account that you want to use for connector operations See "Creating the Target System User Account for Connector Operations" for more information.	sadmin
SiebelServer	Name of the target system server	STS_TESTING
UserName	User ID of the target system user account that you want to use for connector operations See "Creating the Target System User Account for Connector Operations" for more information.	sadmin
Encryption	Type of encryption for secure communication **Note:** The value of this parameter is case-sensitive.	If encryption is required, then specify RSA. Otherwise, specify None.
Version	Version of the target system supported by this connector	7.5 or 7.8

Parameter	Description	Sample/Default Value
TimeStamp	For the first reconciliation run, the times-tamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of reconciliation was completed is stored in this parameter.	The following are sample timestamp values: For English: `Jun 01, 2006 at 10:00:00 GMT+05:30` For French: `juil. 01, 2006 at 10:00:00 GMT+05:30` For Japanese: `6 01, 2006 at 10:00:00 GMT+05:30`
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.	`First Name=John&Last Name=Doe`
SSO	Enter `yes` to specify that the target system is configured to use a SSO solution for authentication. Otherwise, enter `no`.	`no`
Trusted Token	Enter the trusted token value that you specify while configuring the target system to communicate with the SSO system. If you have not configured SSO authentication, then enter `no`.	`no`

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `SIEBEL IT Resource Definition` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Administrative and User Console Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

2.6 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves performing the following procedures:

> **Note:** In a clustered environment, you must perform this step on each node of the cluster.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Setting Up Lookup Definitions in Oracle Identity Manager
- Adding the Dependent (LDAP Connector) Resource Object for Provisioning

2.6.1 Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

You may require the assistance of the system administrator to change to the required input locale.

2.6.2 Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Copying the Connector Files" section on page 2-8, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, change to the *`OIM_HOME`*`/xellerate/bin` directory.

   > **Note:** You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
   >
   > *`OIM_HOME`*`/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   > **Note:** You can ignore the exception that is thrown when you perform Step 2.

In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

OIM_HOME`/xellerate/config/xlConfig.xml`

2.6.3 Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

  This level enables logging of information about error events that may allow the application to continue running.

- `FATAL`

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- `OFF`

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **Oracle WebLogic Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*`/xellerate/config/log.properties` file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SIEBEL=log_level
     ```

  2. In these lines, replace *`log_level`* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SIEBEL=INFO
     ```

  After you enable logging, log information is displayed on the server console.

- **IBM WebSphere Application Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SIEBEL=log_level
     ```

  2. In these lines, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.SIEBEL=INFO
     ```

  After you enable logging, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="XL_INTG.SIEBEL">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line of each set, replace *log_level* with the log level that you want to set. For example:

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>

     <category name="XL_INTG.SIEBEL">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SIEBEL=log_level
     ```

  2. In these lines, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

```
log4j.logger.XL_INTG.SIEBEL=INFO
```

After you enable logging, log information is written to the following file:

ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.6.4 Setting Up Lookup Definitions in Oracle Identity Manager

The following lookup definitions are created in Oracle Identity Manager when you deploy the connector:

- Lookup.Siebel.EmployeeTypeCode

  During a provisioning operation, you use this lookup definition to set one of the following employee types for the user:

  - Contractor
  - Employee
  - Intern

- Lookup.Siebel.PreferredCommunications

  During a provisioning operation, you use this lookup definition to set one of the following communication modes for the user:

  - Email
  - Fax
  - Pager
  - Phone
  - Wireless Message

- Lookup.Siebel.UserType

  During a provisioning operation, you use this lookup definition to set one of the following user types for the user:

  - Employee
  - User

You must enter values in this lookup definition before you can use it during provisioning operations. To enter values in a lookup definition:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definition.
4. Enter Code Key and Decode values for each of entry.

   For each lookup definition, the Code Key and Decode values must be items from the lists given earlier in this section. The target system supports only these values.
5. Click **Save**.

2.6.5 Adding the Dependent (LDAP Connector) Resource Object for Provisioning

Note: The connector for the LDAP solution must be installed before you can perform this procedure.

Adding the dependent (LDAP connector) resource object for provisioning as follows:

1. Log in to the Design Console.
2. Expand the **Resource Management** folder, and double-click **Resource Objects**.
3. Search for and open the **Siebel** resource object.
4. On the Depends On tab, click **Assign**.
5. In the dialog box that is displayed, select the resource object for the LDAP connector and use the right arrow icon to move it from the Unassigned Objects list to the list on the right. Then, click OK.
6. Click the Save icon, and then close the dialog box.
7. Click the Save icon on the Siebel resource object.

2.7 Configuring the Target System for Encryption

Note: Perform this procedure only if you want to use RSA encryption on the target system.

You can configure encryption to secure communication between the target system server and Oracle Identity Manager. This section discusses the following topics related to configuring encryption:

- Configuring the Target System for RSA Encryption
- Configuring the Siebel Web Server Extension for RSA Encryption
- Enabling RSA Encryption for the Siebel Call Center Application
- Starting the Siebel Software Configuration Wizard

2.7.1 Configuring the Target System for RSA Encryption

This section describes how to configure the target system to use RSA encryption for Siebel Internet Session API (SISNAPI) communication between the target system server and Oracle Identity Manager.

To enable RSA encryption for the target system:

1. Start the Siebel Software Configuration Wizard.

   This wizard is started automatically when you install the target system. If required, you can start it manually by following instructions given in the "Starting the Siebel Software Configuration Wizard" section on page 2-16.
2. On the Encryption Type page of the wizard, select the **RSA** option to specify that you want to use the RSA Security Systems 128-bit strong encryption feature for the target system components.
3. Review the settings, and exit the wizard.
4. Restart the server.

2.7.2 Configuring the Siebel Web Server Extension for RSA Encryption

After you configure the target system for RSA encryption, perform the same procedure to configure the Siebel Web Server Extension for RSA encryption.

2.7.3 Enabling RSA Encryption for the Siebel Call Center Application

To enable RSA encryption for the Siebel Call Center Application:

1. Start the Siebel Call Center Application.
2. Navigate to **Sitemap, Server Administration, Components,** and **Component Parameters.**
3. Query for **Call Center Object Manager (ENU)** in the Server Component-Parameter List applet.
4. In the applet, select the **Encryption Type** parameter and select `RSA`. If RSA encryption is not required, then select `None` instead of `RSA`.

2.7.4 Starting the Siebel Software Configuration Wizard

This section provides information about starting the Siebel Software Configuration Wizard.

The Siebel Software Configuration Wizard opens automatically after the installation of most server components. If required, you can use one of the following methods to manually start the wizard on a Microsoft Windows computer:

- From the Microsoft Windows desktop:
  1. Click **Start.**
  2. Select **Programs, Siebel Servers 7.0,** and **Configure *`Server_Type`***, where ***`Server_Type`*** is the server you want to configure. For example, ***`Server_Type`*** can be Siebel Gateway.
- From a command window:
  1. In a command window, navigate to the `bin` subdirectory component to configure components in the `SIEBEL_ROOT` directory. For example, `D://sea700/siebsrvr/bin.`
  2. Depending on the component that you want to configure, enter one of the following commands:
     - To configure the Siebel Database Server, enter the following command:

       ```
       ssincfgw -l LANGUAGE -v y
       ```

     - To configure any component except the Siebel Database Server, enter the following command:

       ```
       ssincfgw -l LANGUAGE
       ```

     In these commands, *`LANGUAGE`* is the language in which the Siebel Software Configuration Wizard must run. For example, `ENU` for U.S. English or `DEU` for German. When you run any one of these commands, a menu of configuration modules for each installed component is displayed.

3

Configuring the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

> **Note:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- Configuring Reconciliation
- Configuring Provisioning
- Activating and Deactivating Employee Accounts

3.1 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Partial Reconciliation
- Reconciliation Based on User Type
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

3.1.1 Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` IT resource parameter while configuring the IT resource.

The following table lists the target system attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query condition. You specify this query condition as the value of the `CustomizedReconQuery` parameter.

Oracle Identity Manager Attribute	Target System Attribute
User ID	Login Name
First Name	First Name
Last Name	Last Name
Email	EMail Addr
Job Title	Job Title
Middle Name	Middle Name
Organization	Organization
Responsibility	Responsibility
Position	Position
Employee Type	Employee Type
Alias	Alias

The following are sample query conditions:

- `First Name=John&Last Name=Doe`

  With this query condition, records of users whose first name is John and last name is Doe are reconciled.

- `First Name=John&Last Name=Doe|group=contractors`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  – The user's first name is `John` or last name is `Doe`.

  – The user belongs to the `contractors` group.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the target system attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.
- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  First Name=John&Last Name=Doe
  ```

  ```
  First Name= John&Last Name= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.

- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

- The query condition must be an expression without any braces.
- Searching users based on multiple value roles and groups are not supported. Only one value for roles and profiles can be queried at a time. For example, if the query condition is `Usergroup=a,b,c`, then the query generates an error.
- Searching users based on more than three user attributes are not supported. For example, if the query condition is `userid=JOHN&firstname=John&lastname=Doe&country=US`, then the query generates an error.

You specify a value for the `CustomizedReconQuery` parameter while configuring the IT resource.

3.1.2 Reconciliation Based on User Type

Siebel supports the definition of the following user types:

- Employee
- Partner User
- Customer

You can specify the user type for which reconciliation must be performed.

To specify the user type for which reconciliation must be performed, you use the UserType scheduled task attribute. This attribute is discussed in the "Specifying Values for the Scheduled Task Attributes" section on page 3-5.

3.1.3 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

Note: Skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `SiebelEmpXLResourceObject.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.
2. Set the `IsTrusted` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `SiebelEmpXLResourceObject.xml` file, which is in the *`OIM_HOME`*`/xellerate/Siebel/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrusted` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-4.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML Files" section on page 2-8, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure the scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.

- To set the task to run only once, select the **Once** option.

9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-5 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes

10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-7.

3.1.4.1 Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `Siebel LookupRecon` lookup fields reconciliation scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Default/Sample Value
`ITResource`	Name of the IT resource	`SIEBEL IT Resource`

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.1.4.1.2 User Reconciliation Scheduled Task You must specify values for the following attributes of the `Siebel Recon` user reconciliation scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Default/Sample Value
`Organization`	Oracle Identity Manager users	`OIM Users`
`Xellerate Type`	Type of Oracle Identity Manager user	`End user Administrator`
`Role`	Default employee type	`Consultant`
`ITResource`	Name of the IT resource	`SIEBEL IT Resource`
`ResourceObject`	Resource object name	`SIEBEL Resource Object`
`IsTrusted`	Specifies whether or not trusted source reconciliation must be performed This parameter is set to `True` for trusted source reconciliation. It is set to `False` for target resource reconciliation.	`False` (target resource reconciliation) `True` (trusted source reconciliation)
`isDeleteRecon`	Specifies whether or not delete users reconciliation must be performed If this parameter is set to `True`, then the users that are deleted from the target system are deleted from Oracle Identity Manager. If this parameter is set to `False`, then the users that are deleted from the target system are not deleted from Oracle Identity Manager. **Note:** This parameter is provided only for optimization, because the target system does not maintain records of deleted users.	`True` or `False`
`UserType`	Specifies the type of user that must be reconciled The Siebel user types are: ▪ `Employee`: This user is an internal employee and user who is associated with a position in a division within your company. ▪ `Partner User`: This user is an employee at a partner company (external organization) and is associated with a position in a division within that company. Therefore, a `Partner User` is also an `Employee`, but not an internal one. ▪ `Customer`: This user is a self-registered partner having no position in your company. However, this user has a responsibility that defines what application views the user can access. For information about testing reconciliation based on user type, refer to the "Testing Reconciliation Based on User Type" section on page 4-4.	`Employee`
`SiebelServerTimeZone`	Specifies the time zone of the target system database The connector uses this information to identify records that must be reconciled during incremental reconciliation.	`GMT+10:00`

Attribute	Description	Default/Sample Value
DayLightSaving	Specifies the time (in minutes) that must be added to the time stamp Sample value: `60` With this sample value, 60 minutes are added to the time stamp stored in the TimeStamp parameter, and the new time stamp is used to identify records that have been created or modified after the last reconciliation run.	Default value: `0`

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.2 Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

Note: Skip this section if either of the following conditions is true:

- You performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-4.
- You do not want to use the provisioning features of Oracle Identity Manager for this target system.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

See Also: The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- `PrePopulate SIEBEL Form`
- `Siebel Delete User`
- `Siebel Modify User`
- `Siebel Add Position`
- `Siebel Add Primary Responsibility`
- `Siebel Create User`
- `Siebel Remove Position`

Note: A user must have at least one position in Siebel. Therefore, if a user is in the last position, then the position cannot be deleted.

- `Siebel Add Responsibility`
- `Siebel Remove Responsibility`
- `Siebel Add Primary Position`

You must compile these adapters before they can be used in provisioning operations.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you import into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

   Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`OIM_HOME`*`/xellerate/Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

If you want to compile one adapter at a time, then use the Adapter Factory form.

See Also: *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

3.3 Activating and Deactivating Employee Accounts

Note: This is not part of the deployment procedure.

To activate an employee account in the target system, assign any responsibility from Oracle Identity Manager.

To deactivate an employee account in the target system, delete all responsibilities of the employee from Oracle Identity Manager.

4

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Running Test Cases
- Troubleshooting

4.1 Running Test Cases

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Copy the contents of the `Troubleshoot` directory on the installation media, to the *`OIM_HOME`*`/xellerate/Siebel/Troubleshoot` directory.
2. Specify the required values in the `global.properties` file.

   This file is in the *`OIM_HOME`*`/xellerate/Siebel/Troubleshoot` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Siebel Server Parameters	Parameters required to connect to the target system These parameters are the same as the parameters of the IT resource.
Create User Parameters	Values required to create a user
Modify User Parameters	Values required to modify a user
Delete User Parameters	User ID of the user to be deleted
Recon Parameters	Date from which modified data is to be reconciled The To Date value is taken as the current date and time.

3. Add the following to the `CLASSPATH` environment variable:

   `OIM_HOME``/xellerate/lib/xlUtils.jar`
   `OIM_HOME``/xellerate/JavaTasks/xlSiebel.jar`
   `OIM_HOME``/xellerate/ScheduleTask/SiebelRecon.jar`
   `OIM_HOME``/xellerate/lib/xlLogger.jar`
   `OIM_HOME``/xellerate/ext/log4j-1.2.8.jar`

   For Siebel 7.5, the following files from the *`OIM_HOME`*`/xellerate/ThirdParty` directory

```
SiebelJI_enu.jar
SiebelJI_Common.jar
SiebelJI.jar
```

For Siebel 7.8, the following files from the *OIM_HOME*/xellerate/ThirdParty directory

```
Siebel.jar
SiebelJI_enu.jar
```

4. Create an ASCII-format copy of the global.properties file as follows:

   Note: You must perform this procedure every time you make a change in the contents of the global.properties file.

   a. In a command window, change to the following directory:

      OIM_HOME/Xellerate/Siebel/troubleshoot

   b. Enter the following command:

      ```
      native2ascii global.properties troubleshoot.properties
      ```

      The troubleshoot.properties is created when you run the native2ascii command. The contents of this file are an ASCII-format copy of the contents of the global.properties file.

5. Perform the following tests:

   - Enter the following command to create a user:

     ```
     java
     -DTproperties=OIM_HOME/xellerate/Siebel/Troubleshoot/troubleshoot.propertie
     s
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/Siebel/Troubleshoot/log.prop
     erties TroubleShootingUtility C
     ```

   - Enter the following command to modify a user:

     ```
     java
     -DTproperties=OIM_HOME/xellerate/Siebel/Troubleshoot/troubleshoot.propertie
     s
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/Siebel/Troubleshoot/log.prop
     erties TroubleShootingUtility M
     ```

   - Enter the following command to delete a user:

     ```
     java
     -DTproperties=OIM_HOME/xellerate/Siebel/Troubleshoot/troubleshoot.propertie
     s
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/Siebel/Troubleshoot/log.prop
     erties TroubleShootingUtility D
     ```

   - Enter the following command to reconcile user information:

     ```
     java
     -DTproperties=OIM_HOME/xellerate/Siebel/Troubleshoot/troubleshoot.propertie
     s
     -Dlog4j.configuration=file:/OIM_HOME/xellerate/Siebel/Troubleshoot/log.prop
     erties TroubleShootingUtility R
     ```

4.1.1 Testing Partial Reconciliation

To test query-based reconciliation, you can specify the following types of query conditions as values for the `CustomizedReconQuery` parameter:

- Simple query with user attributes, for example:
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John`

    The users with first name `John` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `Login Name=JOHN`

    The users with login name `JOHN` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John|First Name=Jane`

    The users with first name `John` and `Jane` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John&Last Name=Doe`

    The users with the first name `John` and last name `Doe` are reconciled.
- Query based on positions and responsibilities, for example:
  - Value assigned to the CustomizedReconQuery parameter: `Position=Proxy Employee|Position=ERM AnonUser`

    All users having positions as `Proxy Employee` or `ERM AnonUser` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `Responsibility=CEO&Responsibility=Consultant`

    All users having responsibilities as `CEO` and `Consultant` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `Responsibility=CEO& Position=ERM AnonUser`

    All users having responsibility `CEO` and position as `ERM AnonUser` are reconciled.
- Complex queries, for example:
  - Value assigned to the CustomizedReconQuery parameter: `First Name=John&Position=Proxy Employee|Position=ERM AnonUser`

    All users having first name as `John` and position as `Proxy Employee`, as well as all users with position as `ERM AnonUser` are reconciled.
  - Value assigned to the CustomizedReconQuery parameter: `Last Name=Doe|Position=Proxy Employee&Responsibility=CEO`

    All users having last name as `Doe` plus all users having both Position as `Proxy Employee` and Responsibility as `CEO` are reconciled.

Note: For queries with a combination of & and `|`, the name value pairs adjacent to the & operator are taken as if they are in parenthesis by Siebel.

4.1.2 Testing Reconciliation Based on User Type

You can test reconciliation based on the type of user by specifying the following values for the `UserType` scheduled task attribute:

- `Employee`

  All information about users belonging to the `Employee` type is reconciled.

- `Partner User`

  All information about users belonging to the `Partner User` type is reconciled.

- `Customer`

  All information about users belonging to the `Customer` type is reconciled. These users belonging to the `Customer` type have `NONE` as the value for the Position field.

4.2 Troubleshooting

The following sections list solutions to some commonly encountered errors of the following types:

- Connection Errors
- Create User Errors
- Delete User Errors
- Edit User Errors

4.2.1 Connection Errors

The following table lists the solution to a commonly encountered connection error.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the target system. **Returned Error Message:** SIEBEL connection exception	▪ Ensure that the target system is running. ▪ Ensure that Oracle Identity Manager is working (that is, the database is running). ▪ Ensure that all the adapters have been compiled. ▪ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that values for all the IT resource parameters have been correctly specified.

4.2.2 Create User Errors

The following table lists the solution to a commonly encountered Create User error.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** `SIEBEL.USER_ALREADY_EXIST`	A user with the assigned ID already exists in the target system.

4.2.3 Delete User Errors

The following table lists the solution to a commonly encountered Delete User error.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist in target system **Returned Error Code:** `SIEBEL.USER_DOES_NOT_EXIST`	The specified user does not exist in the target system.

4.2.4 Edit User Errors

The following table lists the solution to a commonly encountered Edit User error.

Problem Description	Solution
Oracle Identity Manager cannot update a user. **Returned Error Message:** User does not exist in target system **Returned Error Code:** `SIEBEL.USER_DOES_NOT_EXIST`	Review the log for more details.

5

Known Issues

The following is a known issue associated with this release of the connector:

- **Bug 7703095**

  During provisioning, if you set a secondary responsibility but do not select a value from the PrimaryResponsibility lookup field, then the secondary responsibility becomes the primary responsibility on the target system.

  During provisioning, if you set the primary responsibility on the process form, then the responsibility is propagated to the child form. However, if you delete the responsibility from the child form, the change is not propagated to the process form. This change is propagated to the process form only after the next reconciliation run with the target system.

The following are limitations of the target system:

- During provisioning, the Set/Reset Password function cannot be run because the target system does not support JDB APIs.
- During reconciliation, a user's password cannot be fetched because the target system does not support JDB APIs.
- The batched reconciliation feature has not been implemented for this connector because the target system does not support JDB APIs.
- During provisioning, the primary position assigned to a user in the target system cannot be removed through Oracle Identity Manager.
- The Lock/Unlock and Disable/Enable functions cannot be run because the target system does not support these functions.
- On the target system, if you delete a position or responsibility assigned to a user, then this change is not fetched into Oracle Identity Manager during the next incremental reconciliation run. This is because the time stamp of the user record is not updated in response to these events.

A

Attribute Mappings Between Oracle Identity Manager and Siebel Enterprise Applications

The following table discusses attribute mappings between Oracle Identity Manager and Siebel Enterprise Applications:

Note: Apply the following guideline while performing provisioning operations:

Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

Oracle Identity Manager Attribute	Siebel Enterprise Applications Attribute	Description
UserID	Login Name	Login ID
LastName	Last Name	Last name
FirstName	First Name	First name
WorkPhone	Phone #	Phone number
Extension	Work Phone Extension	Extension for the phone number
Fax	Fax #	Fax number
Email	EMail Addr	E-mail address
Alias	Alias	User alias
MiddleName	Middle Name	Middle name
TimeZone	Time Zone Name - Translation	Time zone
EmployeeType	Employee Type Code	Type of employee
Title	Personal Title	Title of the user

Oracle Identity Manager Attribute	Siebel Enterprise Applications Attribute	Description
JobTitle	Job Title	Job title
PreferredCommunications	Preferred Communications	Mode of communication
MPosition	Position	Primary position
HomePhone	Home Phone #	Home telephone number
Position	Name	Multivalued attribute for position
Responsibility	Name	Multivalued attribute for responsibility
Organization	Organization	Organization name

Index

M

O

P

R

S

T

U

X