

Oracle® Identity Manager

Connector Guide for Siebel Enterprise Applications

Release 9.0.2

B32174-01

September 2006

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States 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, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vii
Conventions	vii
 What's New in the Oracle Identity Manager Connector for Siebel Enterprise Applications?	ix
Software Updates	ix
Documentation-Specific Updates.....	x
 1 About the Connector	
Supported Functionality	1-1
Multilanguage Support	1-2
Reconciliation Module	1-2
Lookup Fields Reconciliation	1-2
User Reconciliation	1-3
Reconciled Resource Object Fields	1-3
Reconciled Xellerate User Fields.....	1-3
Provisioning Module	1-4
Files and Directories That Comprise the Connector	1-4
Determining the Release Number of the Connector	1-5
 2 Deploying the Connector	
Step 1: Verifying Deployment Requirements	2-1
Step 2: Copying the Connector Files and External Code	2-2
Step 3: Configuring the Oracle Identity Manager Server	2-2
Changing to the Required Input Locale.....	2-3
Clearing Content Related to Connector Resource Bundles from the Server Cache	2-3
Step 4: Importing the Connector XML Files	2-4
Defining IT Resources	2-4
Step 5: Configuring Reconciliation	2-5
Configuring Trusted Source Reconciliation	2-6
Creating the Reconciliation Scheduled Tasks	2-6

Specifying Values for the Scheduled Task Attributes	2-7
Lookup Fields Reconciliation Scheduled Task.....	2-7
User Reconciliation Scheduled Task	2-7
Step 6: Compiling Adapters	2-8
Step 7: Configuring the Target System for Encryption.....	2-9
Configuring Siebel Enterprise Applications for RSA Encryption.....	2-9
Configuring the Siebel Web Server Extension for RSA Encryption	2-10
Enabling RSA Encryption for the Siebel Call Center Application	2-10
Starting the Siebel Software Configuration Wizard.....	2-10
Configuring the Connector for Multiple Installations of the Target System	2-11
Activating and Deactivating Employee Accounts	2-12

3 Testing and Troubleshooting

Running Test Cases	3-1
Troubleshooting.....	3-3
Connection Errors	3-3
Create User Errors.....	3-3
Delete User Errors	3-4
Edit User Errors	3-4

4 Known Issues

A Attribute Mappings Between Oracle Identity Manager and Siebel Enterprise Applications

Index

Preface

Oracle Identity Manager Connector Guide for Siebel Enterprise Applications provides information about integrating Oracle Identity Manager with Siebel enterprise applications.

Note: Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for Siebel enterprise applications.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Guide for BMC Remedy User Management*
- *Oracle Identity Manager Connector Guide for CA-ACF2 Advanced*
- *Oracle Identity Manager Connector Guide for CA-Top Secret Advanced*
- *Oracle Identity Manager Connector Guide for Database Application Tables*
- *Oracle Identity Manager Connector Guide for Database User Management*
- *Oracle Identity Manager Connector Guide for IBM RACF*
- *Oracle Identity Manager Connector Guide for IBM RACF Advanced*
- *Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*
- *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 2000 and 2003*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 5.5*
- *Oracle Identity Manager Connector Guide for Microsoft Windows 2000*
- *Oracle Identity Manager Connector Guide for Microsoft Windows NT 4.0*
- *Oracle Identity Manager Connector Guide for Novell eDirectory*
- *Oracle Identity Manager Connector Guide for Novell GroupWise*
- *Oracle Identity Manager Connector Guide for Oracle e-Business Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for Oracle e-Business User Management*
- *Oracle Identity Manager Connector Guide for Oracle Internet Directory*
- *Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation*

- *Oracle Identity Manager Connector Guide for PeopleSoft User Management*
- *Oracle Identity Manager Connector Guide for Siebel Enterprise Applications*
- *Oracle Identity Manager Connector Guide for RSA Authentication Manager*
- *Oracle Identity Manager Connector Guide for RSA ClearTrust*
- *Oracle Identity Manager Connector Guide for SAP CUA*
- *Oracle Identity Manager Connector Guide for SAP Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for SAP Enterprise Portal*
- *Oracle Identity Manager Connector Guide for SAP User Management*
- *Oracle Identity Manager Connector Guide for Sun Java System Directory*
- *Oracle Identity Manager Connector Guide for UNIX SSH*
- *Oracle Identity Manager Connector Guide for UNIX Telnet*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.2 connector documentation set, 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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	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 the Oracle Identity Manager Connector for Siebel Enterprise Applications?

This chapter provides an overview of the updates made to the connector and documentation for Siebel Enterprise Applications in release 9.0.2 of the Oracle Identity Manager connector pack.

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

These include major changes made to the connector documentation. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

This section discusses the following software updates implemented in this release of the connector.

Incorporation of Multilanguage Support

In addition to English, this release of the connector supports the French and Japanese languages. The following are documentation updates pertaining to the incorporation of this feature:

- The installation media directory includes resource bundle files for the languages supported by the connector. These resource bundle files are described in the "[Files and Directories That Comprise the Connector](#)" section on page 1-4.
- The "[Step 2: Copying the Connector Files and External Code](#)" section on page 2-2 specifies the destination directory into which you must copy the resource bundle files during the deployment procedure.
- The "[Step 3: Configuring the Oracle Identity Manager Server](#)" section on page 2-2 describes the procedure to change to the required input locale and to clear content related to connector resource bundles from the server cache.
- Changes have been made in the procedure described in the "[Running Test Cases](#)" section on page 3-1 to accommodate the multilanguage support feature.

- [Chapter 4, "Known Issues"](#) discusses a new issue related to the use of non-English locales.

Determining the Release Number of the Connector

Instructions to determine the release number of the connector are given in the ["Determining the Release Number of the Connector"](#) section on page 1-5.

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- In the ["Supported Functionality"](#) section on page 1-1, the descriptions of some of the functions have been reworded.
- Oracle Identity Manager uses a Siebel Enterprise Applications user account to connect to and exchange data with Siebel Enterprise Applications. The ["Step 1: Verifying Deployment Requirements"](#) section on page 2-1 provides information about the minimum rights that must be assigned to this user account.
- Instructions to copy the connector JAR files and adapter files to all the nodes of a clustered environment have been added in the following sections:
 - [Step 2: Copying the Connector Files and External Code](#) on page 2-2
 - [Step 3: Configuring the Oracle Identity Manager Server](#) on page 2-2
 - [Step 6: Compiling Adapters](#) on page 2-8
- Instructions and pointers to information about configuring trusted source reconciliation have been moved to the ["Configuring Trusted Source Reconciliation"](#) section on page 2-6.
- Instructions to use Oracle Identity Manager for linking multiple installations of Siebel Enterprise Applications are given in the ["Configuring the Connector for Multiple Installations of the Target System"](#) section on page 2-11.
- [Appendix A](#) provides information about attribute mappings between Oracle Identity Manager and Siebel Enterprise Applications.

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. The connector for Siebel Enterprise Applications is used to integrate Oracle Identity Manager with Siebel Enterprise Applications.

Note: Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Reconciliation Module](#)
- [Provisioning Module](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

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
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
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

Function	Type	Description
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 employee type 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 Siebel Enterprise Applications.

Multilanguage Support

In addition to English, this release of the connector supports the following languages:

- French
- Japanese

Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

Reconciliation can be divided into the following types:

- [Lookup Fields Reconciliation](#)
- [User Reconciliation](#)

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

User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

Reconciled Resource Object Fields

The following fields are reconciled:

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

Reconciled Xellerate User Fields

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

- UserID
- Password
- Organization
- FirstName
- LastName
- Xellerate Type
- Xellerate
- Role

Provisioning Module

The following fields are provisioned:

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

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the following ZIP file on the installation media:

Enterprise Applications\Siebel Enterprise Applications\Siebel User Management Rev 1.1.0.zip

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\SiebelEmpResourceObject.xml	This XML file contains definitions for the following connector components: <ul style="list-style-type: none">■ IT resource type■ Custom 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. You must import this file only if you plan to use the connector in trusted source reconciliation mode.
lib\xlSiebel.jar	This JAR file contains connector code that is used to interact with the target system for provisioning and reconciliation.

File in the Installation Media Directory	Description
Files in the <code>resources</code> directory	Each of these files contains locale-specific information that is used by the connector.
<code>Troubleshoot\global.properties</code>	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.
<code>Troubleshoot\log.properties</code>	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 troubleshooting utility.
<code>Troubleshoot\TroubleShootingUtility.class</code>	This is the standalone class that interacts with the target system. This class contains the code for running the troubleshooting test cases.
<code>docs\B32174_01.pdf</code>	This guide, which provides instructions to deploy the connector.

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

The "[Step 2: Copying the Connector Files and External Code](#)" section on page 2-2 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can determine the release number of the connector at any of the following stages:

Before Deployment

To determine the release number of the connector before you deploy it:

1. Extract the contents of the `xlSiebel.jar` file. This file is in the `lib` directory inside the installation media directory.
2. Open the `manifest.mf` file in a text editor, which 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.

Note: If you maintain a copy of the `xlSiebel.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. However, after you deploy the connector, it is recommended that you use the [After Deployment](#) method.

During Deployment

To determine the release number of the connector while deploying the connector, refer to Step 4 of the procedure described in the "[Step 4: Importing the Connector XML Files](#)" section on page 2-4.

After Deployment

To determine the release number of the connector after deploying the connector:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

Deploying the Connector

Deploying the connector involves the following steps:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Copying the Connector Files and External Code](#)
- [Step 3: Configuring the Oracle Identity Manager Server](#)
- [Step 4: Importing the Connector XML Files](#)
- [Step 5: Configuring Reconciliation](#)
- [Step 6: Compiling Adapters](#)
- [Step 7: Configuring the Target System for Encryption](#)

This chapter also discusses the following topic:

- [Configuring the Connector for Multiple Installations of the Target System](#)
- [Activating and Deactivating Employee Accounts](#)

Step 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 or later
Target systems	Siebel 7.5 or Siebel 7.8
External code	For Siebel 7.5: SiebelJI.jar, SiebelJI_Common.jar, and SiebelJI_enu.jar For Siebel 7.8: Siebel.jar and SiebelJI_enu.jar
Target system user account	To create a target system user account with the required rights: <ol style="list-style-type: none">1. Create a user account.2. Assign this user account the ERM Employee View responsibility. <p>You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-4.</p>

Step 2: Copying the Connector Files and External Code

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

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following ZIP file on the installation media:

Enterprise Applications\Siebel Enterprise Applications\Siebel User Management Rev 1.1.0.zip

Refer to the ["Files and Directories That Comprise the Connector"](#) section on page 1-4 for more information about these files.

File in the Installation Media Directory	Destination Directory
Files in the xml directory	<i>OIM_home</i> \xellerate\Siebel11.0.0\xml
lib\xlSiebel.jar	<i>OIM_home</i> \xellerate\JavaTasks
If you are using Siebel 7.5, then copy the following files from the <i>Siebel7.5_installation_directory</i> \siebsrvr\CLASSES directory: SiebelJI.jar SiebelJI_Common.jar SiebelJI_enu.jar	<i>OIM_home</i> \xellerate\JavaTasks
If you are using Siebel 7.8, then copy the following files from the <i>Siebel7.8_installation_directory</i> \siebsrvr\CLASSES directory: Siebel.jar SiebelJI_enu.jar	
Files in the resources directory	<i>OIM_home</i> \xellerate\connectorResources
Files in the Troubleshoot directory	<i>OIM_home</i> \xellerate\Siebel11.0.0\Troubleshoot
docs\B32174_01.pdf	<i>OIM_home</i> \xellerate\docs\Siebel11.0.0

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 connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves 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](#)

Changing to the Required Input Locale

Changing to the required input locale involves installing the required fonts and setting the required input locale.

To set the required input locale:

Note: Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle file in the `OIM_home\xellerate\connectorResources` directory or make a change in an existing resource bundle file, 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.
2. Enter one of the following commands:

Note: You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

```
OIM_home\xellerate\bin\batch_file_name
```

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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
```

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

Step 4: Importing the Connector XML Files

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 locating files is displayed.
4. Locate and open the `SiebelEmpResourceObject.xml` file, which is in the `OIM_home\xellerate\Siebel1.0.0\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 table in the ["Defining IT Resources"](#) section on page 2-4 for information about the values to be specified.
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 Tools Reference 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. Remove these nodes by right-clicking each node and then selecting **Remove**.

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

After you import the connector XML files, proceed to the ["Step 5: Configuring Reconciliation"](#) section on page 2-5.

Defining IT Resources

You must specify values for the `SIEBEL IT Resource` IT resource parameters listed in the following table.

Parameter	Description	Sample/Default Value
<code>EnterpriseServer</code>	Name of the Enterprise server	<code>siebel</code>
<code>GatewayServer</code>	Name of the Gateway server	<code>STS_TESTING</code>
<code>GatewayServerPort</code>	Port of the Gateway server	<code>2320</code>

Parameter	Description	Sample/Default Value
Language	Language	You can specify any one of the following: For English: enu For French: fr For Japanese: ja
ObjectManager	Name of the object manager	You can specify any one of the following: For English: SCCObjMgr_enu For French: SCCObjMgr_fr For Japanese: SCCObjMgr_ja
Password	Password of the Siebel Enterprise Applications administrator	sadmin
SiebelServer	Name of the Siebel Enterprise Applications server	STS_TESTING
UserName	User name of the Siebel Enterprise Applications administrator	sadmin
Encryption	Type of encryption for secure communication Note: The value of this parameter is case-sensitive.	RSA (if encryption is required) or None (if encryption is not required)
Version	Version of Siebel Enterprise Applications supported by this connector	7.5 or 7.8
TimeStamp	For the first reconciliation run, the timestamp 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

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

Step 5: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- [Configuring Trusted Source Reconciliation](#)

- [Creating the Reconciliation Scheduled Tasks](#)

Configuring Trusted Source Reconciliation

Note: Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `SiebelEmpXMLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

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 locating files is displayed.
4. Locate and open the `SiebelEmpXMLResourceObject.xml` file, which is in the `OIM_home\xellerate\Siebel11.0.0\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**.

Then, set the value of the `IsTrusted` reconciliation scheduled task attribute to `True` while performing the procedure described in the following section.

Creating the Reconciliation Scheduled Tasks

To create the scheduled tasks for lookup fields and user reconciliations:

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 `ERROR` 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 2-7 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 ["Step 6: Compiling Adapters"](#) section on page 2-8.

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](#)

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the 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.

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.

User Reconciliation Scheduled Task You must specify values for the following attributes of the 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.

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 role	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 <code>True</code> for trusted source reconciliation. It is set to <code>False</code> for target resource reconciliation.	False (Nontrusted reconciliation) True (Trusted reconciliation)
Password	Password of the Oracle Identity Manager user	Dummy123
isDeleteRecon	Specifies whether or not delete users reconciliation must be performed If this parameter is set to <code>True</code> , then the users that are deleted from the target system are deleted from Oracle Identity Manager. If this parameter is set to <code>False</code> , 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 Siebel Enterprise Applications does not maintain records of deleted users.	True or False

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

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

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

You must compile these adapters before you can use them to provision accounts on the target system.

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. Then, restart each node.

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.

Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 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 Siebel Enterprise Applications server and Oracle Identity Manager. This section discusses the following topics related to configuring encryption:

- [Configuring Siebel Enterprise Applications 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](#)

Configuring Siebel Enterprise Applications for RSA Encryption

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

To enable RSA encryption for Siebel Enterprise Applications:

1. Start the Siebel Software Configuration Wizard.
This wizard is started automatically when you install Siebel Enterprise Applications. If required, you can start it manually by following instructions given in the ["Starting the Siebel Software Configuration Wizard"](#) section on page 2-10.
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 Siebel Enterprise Applications components.
3. Review the settings, and exit the wizard.
4. Restart the server.

Configuring the Siebel Web Server Extension for RSA Encryption

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

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**.

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.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of Siebel Enterprise Applications. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

To configure the connector for multiple installations of the target system:

1. Create and configure one resource object for each target system installation.

The Resource Objects form is in the Resource Management folder. The `SIEBEL Resource Object` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

The IT Resources form is in the Resource Management folder. The `SIEBEL IT Resource` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

- `UD_SIEBEL` (main form)
- `UD_SIEBEL_P` (child form for multivalue attributes)
- `UD_SIEBEL_R` (child form for multivalue attributes)

You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

The Process Definition form is in the Process Management folder. The `Siebel Process` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

- From the **Object Name** lookup field, select the resource object that you create in Step 1.

- From the **Table Name** lookup field, select the process form that you create in Step 3.
 - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.
5. Configure reconciliation for each target system installation. Refer to the "[Step 5: Configuring Reconciliation](#)" section on page 2-5 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:
- `ITResource`
 - `ResourceObject`
 - `IsTrusted`

Set the `IsTrusted` attribute to `True` for the Siebel Enterprise Applications installation that you want to designate as a trusted source. You can designate either a single or multiple installations of Siebel Enterprise Applications as the trusted source. For the remaining Siebel Enterprise Applications installations, set this attribute to `False`.

6. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Siebel Enterprise Applications installation to which you want to provision the user.

Activating and Deactivating Employee Accounts

Note: This is not part of the deployment procedure.

To activate an employee account in Siebel Enterprise Applications, assign any responsibility from Oracle Identity Manager.

To deactivate an employee account in Siebel Enterprise Applications, delete all responsibilities of the employee from Oracle Identity Manager.

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](#)

Running Test Cases

You can use the troubleshooting 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 troubleshooting utility:

1. Specify the required values in the `global.properties` file.

This file is in the `OIM_home\xellerate\Siebel1.0.0\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 Siebel Enterprise Applications Refer to the " Defining IT Resources " section on page 2-4 for information about the values that you must provide.
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.

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

```
OIM_home\xellerate\lib\xlUtils.jar
OIM_home\xellerate\JavaTasks\xlSiebel.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\JavaTasks` directory

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

For Siebel 7.8, the following files from the *OIM_home\xellerate\JavaTasks* directory

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

3. In the `log.properties` file in the same directory:
 - a. In the following parameter, set the path of the directory in which you want to create the log files:

```
log4j.appender.logfile.File=log_file_path
```

Here, *log_file_path* is the path of the directory in which you want to create the log file.

- b. Specify any one of the following log levels:

```
- DEBUG  
- INFO  
- WARN  
- ERROR  
- FATAL
```

For example, if the log level for `DEBUG` is to be enabled, then you must add the following entry file:

```
log4j.rootLogger=DEBUG, stdout, logfile
```

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\sapcua\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\Siebel1.0.0\Troubleshoot\troubleshoot.prop  
erties-Dlog4j.configuration=file:\OIM_home\xellerate\Siebel1.0.0\Troublesho  
ot\log.properties TroubleshootingUtility C
```

- Enter the following command to modify a user:

```
java
-DTproperties=OIM_home\xellerate\Siebel1.0.0\Troubleshoot\troubleshoot.prop
erties-Dlog4j.configuration=file:\OIM_home\xellerate\Siebel1.0.0\Troublesho
ot\log.properties TroubleShootingUtility M
```

- Enter the following command to delete a user:

```
java
-DTproperties=OIM_home\xellerate\Siebel1.0.0\Troubleshoot\troubleshoot.prop
erties-Dlog4j.configuration=file:\OIM_home\xellerate\Siebel1.0.0\Troublesho
ot\log.properties TroubleShootingUtility D
```

- Enter the following command to reconcile user information:

```
java TroubleShootingUtilityLdap -java -DTproperties=
OIM_home\xellerate\Siebel1.0.0\Troubleshoot\troubleshoot.properties
-Dlog4j.configuration=file:\OIM_home\xellerate\Siebel1.0.0\Troubleshoot\log
.properties TroubleShootingUtility R
```

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](#)

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 Siebel Enterprise Applications. Returned Error Message: SIEBEL connection exception	<ul style="list-style-type: none"> ■ Ensure that Siebel Enterprise Applications 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.

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.	A user with the assigned ID already exists in Siebel Enterprise Applications.
Returned Error Message: User already exists	
Returned Error Code: SIEBEL.EMPLOYEE_ALREADY_EXIST	

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.	The specified user does not exist in Siebel Enterprise Applications.
Returned Error Message: User does not exist in target system	
Returned Error Code: SIEBEL.EMPLOYEE_DOES_NOT_EXIST	

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.	Review the log for more details.
Returned Error Message: User does not exist in target system	
Returned Error Code: SIEBEL.EMPLOYEE_DOES_NOT_EXIST	

Known Issues

The following are known issues associated with this release of the connector:

- During provisioning, the Set/Reset Password function cannot be run because there is no JDB_API support.
- During provisioning, the primary position assigned to a user in Siebel Enterprise Applications cannot be removed through Oracle Identity Manager.
- During reconciliation, an user's password cannot be fetched because there is no JDB_API support.
- During reconciliation, the value of the (GMT+13:00) Nuku'alofa time zone cannot be inserted into the database.
- The Lock/Unlock and Disable/Enable functions cannot be run because Siebel Enterprise Applications does not support these functions.
- 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 were using the Japanese locale and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

Attribute Mappings Between Oracle Identity Manager and Siebel Enterprise Applications

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

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
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

Index

A

- activating employee accounts, 2-12
- Adapter Factory form, 2-9
- Adapter Manager form, 2-9
- adapters, compiling, 2-8
- additional files, 2-1, 2-2
- Administrative and User Console, 2-4, 2-6
- attributes
 - lookup fields reconciliation scheduled task, 2-7
 - user reconciliation scheduled task, 2-7
- attributes mappings, A-1

C

- changing input locale, 2-2, 2-3
- clearing server cache, 2-3
- compiling adapters, 2-8
- configuring
 - connector for multiple installations of the target system, 2-11
 - Oracle Identity Manager server, 2-2
 - reconciliation, 2-5
 - target system, 2-9
- connection errors, 3-3
- connector files and directories
 - copying, 2-2
 - description, 1-4
 - destination directories, 2-2
 - installation media file, 1-4, 2-2
- connector release number, determining, 1-5
- connector testing, 3-1
- connector XML files
 - See XML files
- Create User errors, 3-3
- creating scheduled tasks, 2-5, 2-6

D

- deactivating employee accounts, 2-12
- defining
 - IT resources, 2-4
 - scheduled tasks, 2-5, 2-6
- Delete User errors, 3-4
- deployment requirements, 2-1
- Design Console, 1-6, 2-6

- determining release number of connector, 1-5

E

- Edit User errors, 3-4
- employee accounts
 - activating, 2-12
 - deactivating, 2-12
- encryption, configuring target system for, 2-9
- errors
 - connection, 3-3
 - Create User, 3-3
 - Delete User, 3-4
 - Edit User, 3-4
- external code files, 2-1, 2-2

F

- files
 - additional, 2-1, 2-2
 - external code, 2-1, 2-2
 - See also XML files
- files and directories of the connector
 - See connector files and directories
- functionality supported, 1-1
- functions available, 1-1

G

- globalization features, 1-2

I

- importing connector XML files, 2-4
- input locale changing, 2-2
- input locale, changing, 2-3
- issues, 4-1
- IT resources
 - defining, 2-4
 - parameters, 2-4
 - SIEBEL IT Resource, 2-4, 2-7
 - types, SIEBEL IT Resource
 - Definition, 2-4

L

limitations, 4-1
lookup fields reconciliation, 1-2
lookup fields reconciliation scheduled task, 2-7

M

mapping between attributes of target system and
 Oracle Identity Manager, A-1
multilanguage support, 1-2

O

Oracle Identity Manager Administrative and User
 Console, 2-4, 2-6
Oracle Identity Manager Design Console, 1-6, 2-6
Oracle Identity Manager server, configuring, 2-2

P

parameters of IT resources, 2-4
problems, 3-3
process tasks, 1-1
provisioning
 fields, 1-4
 functions, 1-1
 module, 1-4

R

reconciliation
 configuring, 2-5
 functions, 1-1
 lookup fields, 1-2
 module, 1-2
 trusted source, 2-6
 trusted source mode, 1-4
 user, 1-3
release number of connector, determining, 1-5
requirements for deploying, 2-1
RSA encryption
 configuring Siebel Enterprise Applications
 for, 2-9
 configuring Siebel Web Server Extension for, 2-10
 enabling, 2-10

S

scheduled tasks
 attributes, 2-7
 defining, 2-5, 2-6
 lookup fields reconciliation, 2-7
 user reconciliation, 2-7
server cache, clearing, 2-3
Siebel Internet Session API, 2-9
Siebel Software Configuration Wizard, 2-10
SISNAPI, 2-9
supported
 functionality, 1-1
 languages, 1-2

releases of Oracle Identity Manager, 2-1
target systems, 2-1

T

target system, multiple installations, 2-11
target systems
 configuration, 2-9
 supported, 2-1
test cases, 3-1
testing the connector, 3-1
troubleshooting, 3-3
troubleshooting utility, 3-1
trusted source reconciliation, 1-4, 2-6

U

user attribute mappings, A-1
user reconciliation, 1-3
user reconciliation scheduled task, 2-7

X

XML files
 copying, 2-2
 description, 1-4
 for trusted source reconciliation, 1-4
 importing, 2-4