Oracle® Identity Manager

Connector Guide for Siebel Enterprise Applications

Release 9.0.3

B32372-01

February 2007

ORACLE®

Oracle Identity Manager Connector Guide for Siebel Enterprise Applications, Release 9.0.3

B32372-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Venkatasubramaniam Iyer, Vijaykarthik Sathiyamurthy, Lyju Vadassery

Contents

3 Testing and Troubleshooting

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 library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation 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 Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 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.
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 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 9.0.3 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 release

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.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the "Multilanguage Support" section on page 1-2.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server

- BEA WebLogic

- IBM WebSphere

This release of the connector also supports Oracle Containers for J2EE (OC4J).

Documentation-Specific Updates

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

- In the "Reconciled Xellerate User Fields" section on page 1-4, the following fields have been removed from the list of reconciled fields:
  - Password
  - Xellerate

- In the "Enabling Logging" section on page 2-4, instructions for each of the application servers that are supported by this release of the connector have been added. In the "Running Test Cases" section on page 3-1, Step 3 describing how to enable logging has been removed.

- In the "Defining IT Resources" section on page 2-6, the value of the GatewayServerPort IT resource parameter has been changed from 2320 to 2321.

- In the "Step 6: Compiling Adapters" section on page 2-10, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.

- In the "Defining IT Resources" section on page 2-6, the sample values of the Language and ObjectManager parameters have been modified.

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. 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

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Traditional Chinese

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

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
- FirstName
- LastName
- Organization
- Xellerate Type
- 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 directory on the installation media:

```
Enterprise Applications\Siebel Enterprise Applications
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
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 `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector.
	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.
`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 troubleshooting utility.
`xml\SiebelEmpResourceObject.xml`	This XML file contains definitions for the following connector components: ■ 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.

> **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

To determine the release number of a connector that you have deployed:

1. Extract the contents of the `xlSiebel.jar` file. For a connector that has been deployed, this file is in the following directory:

   OIM_home\xellerate\JavaTasks

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.

See Also: *Oracle Identity Manager Design Console Guide*

2

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 topics:

- 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: 1. Create a user account. 2. Assign this user account the ERM Employee View responsibility. You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-6.

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 directory on the installation media:
>
> `Enterprise Applications\Siebel Enterprise Applications`
>
> 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
`lib\xlSiebel.jar`	*OIM_home*`\xellerate\JavaTasks`
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`
If you are using Siebel 7.5, then copy the following files from the *Siebel7.5_installation_directory*`\siebsrvr\CLASSES` directory: `SiebelJI.jar` `SiebelJI_Common.jar` `SiebelJI_enu.jar`	*OIM_home*`\xellerate\JavaTasks`
If you are using Siebel 7.8, then copy the following files from the *Siebel7.8_installation_directory*`\siebsrvr\CLASSES` directory: `Siebel.jar` `SiebelJI_enu.jar`	

> **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

■ Enabling Logging

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.

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.

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 informational messages that highlight the progress of the application at 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 still 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:

- **For JBoss Application Server**

  To enable logging:

  1. In the *JBoss_home*\server\default\conf\log4j.xml file, locate the following lines:

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

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

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

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

  JBoss_home\server\default\log\server.log

- **For IBM WebSphere:**

  To enable logging:

1. Add the following line in the
    OIM_home\xellerate\config\log.properties file:

    log4j.logger.XELLERATE=*log_level*

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

    For example:

    log4j.logger.XELLERATE=INFO

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

WebSphere_home\AppServer\logs*server_name*\startServer.log

- **For BEA WebLogic**

    To enable logging:

    1. Add the following line in the
        OIM_home\xellerate\config\log.properties file:

        log4j.logger.XELLERATE=*log_level*

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

        For example:

        log4j.logger.XELLERATE=INFO

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

    WebLogic_home\user_projects\domains*domain_name**server_name**server_name*.log

- **For OC4J**

    To enable logging:

    1. Add the following line in the
        OIM_home\xellerate\config\log.properties file:

        log4j.logger.XELLERATE=*log_level*

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

        For example:

        log4j.logger.XELLERATE=INFO

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

    OC4J_home\opmn\logs\default_group~home~default_group~1.log

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\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 table in the "Defining IT Resources" section on page 2-6 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 2-8.

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
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 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 time stamp 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 `SiebelEmpXLResourceObject.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 `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**.

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 2-9 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 2-10.

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 True for trusted source reconciliation. It is set to False 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 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 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.

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 2-12.

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 2-8 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.

3

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\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 Siebel Enterprise Applications
	Refer to the "Defining IT Resources" section on page 2-6 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. 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.

4. 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.pro
   perties 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.pro
   perties 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.pro
   perties TroubleShootingUtility D
   ```

   - Enter the following command to reconcile user information:

   ```
   java TroubleShootingUtilityLdap -java -DTproperties=
   OIM_home\xellerate\Siebel\Troubleshoot\troubleshoot.properties
   -Dlog4j.configuration=file:\OIM_home\xellerate\Siebel\Troubleshoot\log.prop
   erties 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	■ 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. **Returned Error Message:** User already exists **Returned Error Code:** SIEBEL.EMPLOYEE_ALREADY_EXIST	A user with the assigned ID already exists in Siebel Enterprise Applications.

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.EMPLOYEE_DOES_NOT_EXIST	The specified user does not exist in Siebel Enterprise Applications.

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	

4

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, a 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 language 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.

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.

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	Multivalue attribute for position
Responsibility	Name	Multivalue attribute for responsibility

Index