Oracle® Identity Manager

Connector Guide for RSA ClearTrust

Release 9.0.4

E10440-03

July 2009

Oracle Identity Manager Connector Guide for RSA ClearTrust, Release 9.0.4

E10440-03

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

3 Configuring the Connector

4 Testing and Troubleshooting

5 Known Issues

A Attribute Mappings Between Oracle Identity Manager and RSA ClearTrust

Index

Preface

Oracle Identity Manager Connector Guide for RSA ClearTrust provides information about integrating Oracle Identity Manager with RSA ClearTrust.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for RSA ClearTrust.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Concepts*
- *Oracle Identity Manager Installation and Configuration Guide for BEA WebLogic Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*
- *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 API Usage Guide*
- *Oracle Identity Manager Audit Report Developer's Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Integration Guide for Crystal Reports*
- *Oracle Identity Manager Tools Reference*
- *Oracle Identity Manager Reference*

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

- *Oracle Identity Manager Connector Concepts Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack documentation library, 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.

Convention	Meaning
`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 RSA ClearTrust?

This chapter provides an overview of the updates made to the software and documentation for the RSA ClearTrust connector in release 9.0.4.2 of the Oracle Identity Manager connector pack.

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

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

- Software Updates Up To Release 9.0.4.1
- Software Updates in Release 9.0.4.2

Software Updates Up To Release 9.0.4.1

The following software updates have been made up to release 9.0.4.1 of the connector:

- Enhancement in the Multilanguage Support Feature
- Support for Oracle Application Server

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 1-4.

Support for Oracle Application Server

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the connector also supported Oracle Containers for J2EE (Oracle Application Server).

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Using the Connector Installer
- Changes in the Directory Structure of the Connector Files on the Installation Media
- Resolved Issues in Release

Using the Connector Installer

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

See Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later section for more information.

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

There are some changes in the directory structure of the testing utility files in release 9.0.4.2. These changes have been made in the following sections:

- Files and Directories That Comprise the Connector
- Step 2: Copying the Connector Files and External Code Files

Resolved Issues in Release

The following issues are resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7360876	Inadequate logging in RSA ClearTrust connector.	Adequate logging provided throughout the provisioning and reconciliation tasks. This issue has been resolved.
5632390	WPTG_TBT:SYS:INTXT:Q&A56272:CONFUSING TEXT IN RSA-CLEARTRUST.PROPERTIES:OIM902	Appropriate user text messages are provided. This issue has been resolved.
5453420	Child tables and options for combo box have not been localized.	This issue has been resolved.
5228349	Provisioning ClearTrust to Xellerate user task name is not appropriate.	This issue has been resolved.

Documentation-Specific Updates

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.2:

- Instructions in "Step 4: Importing the Connector XML Files" on page 2-5 have been revised.
- Instructions in the following sections have been revised:
  - Configuring Trusted Source Reconciliation on page 3-1
  - Configuring Trusted Source Reconciliation on page 3-1
- Instructions in the "Running Connector Tests" on page 4-1 have been revised.
- Instructions in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-8 have been added.
- In the "Multilanguage Support" section, Arabic has been added to the list of languages that the connector supports.

1 About the Connector

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

This chapter contains the following sections:

- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Multilanguage Support
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

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

At some places in this guide, RSA ClearTrust has been referred to as the *target system.*

Reconciliation Module

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

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

Reconciled Resource Object Fields

The following target system fields are reconciled:

- UserID
- FirstName
- LastName
- EmailID

- StartDate
- EndDate
- PasswordExpDate
- IsPublic
- IsUserlocked
- PropertyName
- PropertyValue
- GroupName

You can customize the following reconciliation fields by setting the `UseReconFieldMap` attribute to `true` and adding their values in the `Lookup.CTReconciliation.FieldMap` lookup:

> **Note:** The `userId` and `lastName` fields are mandatory fields and, therefore, they must exist in the lookup.

- userId
- lastName
- islock
- firstName
- email
- startDate
- endDate
- pwdExpDate
- isPublic
- properties
- groups

Reconciled Xellerate User Fields

The following target system fields are reconciled only if trusted source reconciliation is implemented:

- UserID
- FirstName
- LastName
- Email
- Organization
- User Type
- Employee Type

Provisioning Module

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

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

For this target system, the following fields are provisioned:

- User ID
- Password
- Password Expiration Date
- First Name
- Last Name
- Email Address
- Start Date
- End Date
- Lock User
- Is Public
- User Group Name
- Property Value
- Property Name
- Property Value (Date)
- Property Value (Boolean)

Supported Functionality

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

Process Task	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a provisioned user
Disable User	Provisioning	Disables an existing user
Enable User	Provisioning	Enables a disabled user
Update User	Provisioning	Updates an existing user
Set Password	Provisioning	Sets a password when a user is first created in RSA ClearTrust
Change Password	Provisioning	Updates a user's password

Process Task	Type	Description
Assign User to a Group	Provisioning	Assigns a user to a group in RSA ClearTrust To map an RSA ClearTrust group to Oracle Identity Manager: 1. Open the Oracle Identity Manager Design Console. 2. Expand the **Xellerate Administration** folder, and double-click **Lookup Definition.** The Lookup Definition page is displayed. 3. On the Lookup Definition page, query for the **CTGroups** record. 4. Click **Add.** A blank row is displayed on the Lookup Code Information tab. 5. In the **Code** Key and **Decode** fields, enter the name of the RSA ClearTrust group. Then, enter `en` in the Language field and `us` in the **Country** field. 6. Click **Save** on the Oracle Identity Manager toolbar. 7. Repeat Steps 4 through 6 to map additional RSA ClearTrust groups to Oracle Identity Manager.
Remove User from a Group	Provisioning	Removes a user from a group
Assign a Default Group to the User	Provisioning	Assigns a default group to a user
Update User Property	Provisioning	Assigns or removes a property value If the RSA ClearTrust property type is `Date,` then the corresponding value for the property can be set only by using the Property Value (Date) field in the RSA ClearTrust User Properties form. If the RSA ClearTrust property type is `Boolean,` then the corresponding value for the property can be set only by using the Property Value (Boolean) check box in the ClearTrust User Properties form. To set the value of any other type of property, use the Property Value field.
Trusted Reconciliation for Login	Reconciliation	Creates Xellerate Login accounts with respect to reconciled logins from RSA ClearTrust
Create User	Reconciliation	Reconciles user accounts from RSA ClearTrust
Update User Property	Reconciliation	Reconciles user properties from RSA ClearTrust
Assign User to a Group	Reconciliation	Reconciles user-group association from RSA ClearTrust

Multilanguage Support

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified

- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

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

Files and Directories That Comprise the Connector

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

```
Web Access Control/RSA ClearTrust
```

These files and directories are listed in the Table 1–1.

Table 1–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`lib/xliClearTrust.jar`	This JAR file contains the Java classes that are required for provisioning.
`lib/xliClearTrustRecon.jar`	This JAR file contains the Java classes that are required to reconcile users from RSA ClearTrust.
Files in the `resources` directory	Each of these resource bundles 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.
`tests/config/config.properties`	This file contains the properties that are used to connect to the RSA ClearTrust server.

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

File in the Installation Media Directory	Description
`tests/lib/xliClearTrustTest.jar`	This JAR file contains the test classes that can be used to test the functionality of the connector.
`xml/RSAClearTrustResourceObject.xml`	These XML files contain definitions for the following components of the RSA ClearTrust connector: ■ IT resource type ■ Process form ■ Process task and adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation scheduled task and its attributes ■ The adapter that is required to enable the AutoSave feature in the RSA ClearTrust provisioning process form
`xml/RSAClearTrustXLResourceObject.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.

File in the Installation Media Directory	Description
`lib/xliClearTrust.jar`	This JAR file contains the Java classes that are required for provisioning.
`lib/xliClearTrustRecon.jar`	This JAR file contains the Java classes that are required to reconcile users from RSA ClearTrust.
Files in the `resources` directory	Each of these resource bundles 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.
`tests/config/config.properties`	This file contains the properties that are used to connect to the RSA ClearTrust server.
`tests/lib/xliClearTrustTest.jar`	This JAR file contains the test classes that can be used to test the functionality of the connector.
`xml/RSAClearTrustResourceObject.xml`	These XML files contain definitions for the following components of the RSA ClearTrust connector: ■ IT resource type ■ Process form ■ Process task and adapters (along with their mappings) ■ Login resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation scheduled task and its attributes ■ The adapter that is required to enable the AutoSave feature in the RSA ClearTrust provisioning process form
`xml/RSAClearTrustXLResourceObject.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 `tests` directory are used only to run tests on the connector.

The "Step 2: Copying the Connector Files and External Code Files" section on page 2-1 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use the following method to determine the release number of the connector:

1. Extract the contents of the `xliClearTrust.jar` file. This file is in the following directory on the installation media:

   ```
   Web Access Control/RSA ClearTrust
   ```

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

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

2 Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files and External Code Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Importing the Connector XML Files

Depending on the release of Oracle Identity Manager that you use, perform the procedure:

Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

Step 1: Verifying Deployment Requirements

The following table lists the installation requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	RSA ClearTrust 5.5 or 5.5.2

External code	The following files from the directory in which RSA ClearTrust is installed:
	`ct_admin_api.jar`
	`ct_runtime_api.jar`
	`cleartrust.jar`

Target system user account	RSA ClearTrust administrator account You provide the credentials of this user account while performing the procedure in "Defining IT Resources" on page 2-6.

Step 2: Copying the Connector Files and External Code Files

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

Note: For the connector files, 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:

```
Web Access Control/RSA ClearTrust
```

Refer to "Files and Directories That Comprise the Connector" on page 1-5 for more information about these files.

Connector File/External Code File	Destination Directory
`lib/xliClearTrust.jar`	*`OIM_HOME`*`/xellerate/JavaTasks`
`lib/xliClearTrustRecon.jar`	`OIM_HOME/xellerate/ScheduleTask`
Files in the `resources` directory on the installation media	*`OIM_HOME`*`/xellerate/connectorResources`
Files and directories in the `tests` directory on the installation media	*`OIM_HOME`*`/xellerate/tests`
Files in the `xml` directory on the installation media	*`OIM_HOME`*`/xellerate/XLIntegrations/ClearTrust/xml`

The following files from the *`ClearTrust_installation_dir`*`/lib` directory:
`ct_admin_api.jar`
`ct_runtime_api.jar`
`cleartrust.jar`
	`OIM_HOME``/ThirdParty`

The following files in the *`ClearTrust_installation_dir`*`/lib/` directory:
`ct_admin_api.jar`
`ct_runtime_api.jar`
	`OIM_HOME``/xellerate/ext`

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

Step 3: Configuring the Oracle Identity Manager Server

This section discusses the following topics:

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.

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in "Step 2: Copying the Connector Files and External Code Files" on page 2-1, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

   `OIM_HOME``/xellerate/config/xlConfig.xml`

Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **BEA WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.ADAPTERS.CTINTEGRATION=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.ADAPTERS.CTINTEGRATION=INFO
     ```

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

  `WebLogic_home``/user_projects/domains/`*`domain_name`*`/`*`server_name`*`/`*`server_name`*`.log`

- **IBM WebSphere Application Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.ADAPTERS.CTINTEGRATION=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.ADAPTERS.CTINTEGRATION=INFO
     ```

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

```
WebSphere_home/AppServer/logs/server_name/startServer.log
```

- **JBoss Application Server**

  To enable logging:

  1. In the `JBoss_home/server/default/conf/log4j.xml` file, locate or add the following lines:

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

     <category name="ADAPTERS.CTINTEGRATION">
        <priority value="log_level"/>
     </category>
     ```

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

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

     <category name="ADAPTERS.CTINTEGRATION">
        <priority value="INFO"/>
     </category>
     ```

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

  ```
  JBoss_home/server/default/log/server.log
  ```

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.ADAPTERS.CTINTEGRATION=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.ADAPTERS.CTINTEGRATION=INFO
     ```

  After you enable logging, the 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

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

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `RSAClearTrustResourceObject.xml` file, which is in the *`OIM_HOME`*`/xellerate/XLIntegrations/ClearTrust/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 `ClearTrust` IT resource is displayed.
8. Specify values for the parameters of the `ClearTrust` IT resource. Refer to the table in "Defining IT Resources" 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 `ClearTrust` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

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

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.
13. Perform the same procedure to import the remaining connector XML files. These files are in the *`OIM_HOME`*`/xellerate/XLIntegrations/ClearTrust/xml` directory.

After you import the connector XML files, proceed to the next chapter.

Defining IT Resources

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

Parameter	Description
`CTAdminUserId`	Name of the RSA ClearTrust administrator This is a required parameter.
`CTAdminPassword`	Password of the RSA ClearTrust administrator This is a required parameter.

Parameter	Description
MachineName or IPAddress	Host name or IP address of the computer on which the RSA ClearTrust Entitlements Server is running. This is a required parameter.
Port	Port number on which the RSA ClearTrust Entitlements Server is running This is a required parameter. The default value is 5601.
SSLMode	SSL mode that is used to connect to the RSA ClearTrust server **Note:** Ensure that RSA ClearTrust is running in this mode. Otherwise, Oracle Identity Manager cannot connect to RSA ClearTrust. This is a required parameter. Note: It is recommended that you enable SSL to secure communication with the target system.
TimeOut	Timeout value for the connection that is established between Oracle Identity Manager and RSA ClearTrust This is a required parameter.
Default User Group	Default user group in RSA ClearTrust This is a required parameter.
CaFileLocation	Location of the CA certificate This parameter is used only with mutual authentication.
CaPassword	Password for the CA certificate This parameter is used only with mutual authentication.
KsFileLocation	Location of the keystore file This parameter is used only with mutual authentication.
KsPassword	Password of the keystore file This parameter is used only with mutual authentication.
KeyAlias	Key name that is to be used with the keystore file This parameter is used only with mutual authentication.
PrivatePassword	Password for the private key in the keystore file This parameter is used only with mutual authentication.
TimeStamp	This parameter is reserved for future use.
CTAdmin Group	Group to which the RSA ClearTrust administrative user belongs
CTAdmin Role	Role of the RSA ClearTrust administrative user
Target Locale: Country	Country code Default value: US **Note:** You must specify the value in uppercase.
Target Locale: Language	Language code Default value: en **Note:** You must specify the value in lowercase.

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

Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

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

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the procedure described in the following section. See "Running the Connector Installer" section for more information.

Running the Connector Installer

To run the Connector Installer:

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

   ```
   OIM_HOME/xellerate/ConnectorDefaultDirectory
   ```

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

   ```
   OIM_HOME/xellerate/ConnectorDefaultDirectory
   ```

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **RSA ClearTrust *RELEASE_NUMBER***.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see "Configuring Trusted Source Reconciliation" on page 3-1 for more information.

   c. Compilation of adapters

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

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

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

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

      Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-3 for information about running the `PurgeCache` utility.

      There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

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

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

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

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

Installing the Connector in an Oracle Identity Manager Cluster

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

3

Configuring the Connector

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

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System

Configuring Reconciliation

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

- Configuring Trusted Source Reconciliation
- Configuring System Properties
- Configuring the Reconciliation Scheduled Tasks
- Enabling Reconciliation in Oracle Identity Manager Release 9.0.4

Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or a target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

> **Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `RSAClearTrustXLResourceObject.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

   > **Note:** Only one target system can be designated as a trusted source. If you import the `RSAClearTrustXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Set the `TrustedSource` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

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

After you import the XML file for trusted source reconciliation, you must set the value of the `Trusted Source Recon - Resource Object name` reconciliation scheduled task attribute to `Xellerate User`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

Configuring System Properties

To configure system properties:

1. Open the Oracle Identity Manager Design Console.
2. Navigate to the System Configuration page.
3. Check if there is an entry for "Default date format." If this entry is not there, then perform Step 4.
4. Add a new entry in the Server category:
   - Name: `Default date format`
   - Keyword: `XL.DefaultDateFormat`
   - Value: `yyyy/MM/dd hh:mm:ss z`
5. Click **Save**.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in "Step 4: Importing the Connector XML Files" on page 2-5, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

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 task are displayed.
5. Enter a number in the **Max Retries** field. Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, set 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 `ClearTrust Reconciliation Task` scheduled task. Refer to the following table for information about the values to be specified.

Attribute	Description	Sample Value
`Server`	Name of the IT Resource	`ClearTrust`
`Target System CT Recon - Resource Object name`	Name of the target system parent resource object	`ClearTrust`
`Trusted Source Recon - Resource Object name`	Name of the trusted source resource object	Default value: `false` Specify trusted source resource object if you want to configure trusted source reconciliation.
`Paging Range`	Paging range to extract user accounts from the target system	`10`
`TrialRecNum`	Use this parameter if you only want to check connectivity with the target and reconcile a few records to ensure that reconciliation with the relevant target is working. Specify the number of records that you want to reconcile as the value of this parameter.	3

Attribute	Description	Sample Value
`UseReconFieldMap`	If this attribute is set to `true,` the Client Customize reconciliation is activated and only the fields in the `Attribute Name: CTReconciliationFields` lookup are reconciled. Otherwise, all the available fields are reconciled.	`True`
`CTReconciliationFields`	Name of the lookup definition that stores the reconciliation field data used in customized reconciliation	`Lookup.CTReconciliation.FieldMap`
`Trusted Source Recon - Resource Object name`	Name of the trusted source resource object	Default value: `Xellerate User` Specify `false` (in lowercase) if you do not want to configure trusted source reconciliation
`Date Format`	Format in which date values sent from the target system are to be saved during reconciliation The value that you specify must be the same as the value specified in the "Configuring System Properties" section on page 3-2.	`yyyy/MM/dd hh:mm:ss z`

> **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.

Enabling Reconciliation in Oracle Identity Manager Release 9.0.4

If you are using Oracle Identity Manager release 9.0.4, then you must perform the following procedure to enable reconciliation:

> **See Also:** *Oracle Identity Manager Design Console Guide*

1. Open the Process Definition form for the `ClearTrust` User. This form is in the Process Management folder.
2. Click the **Reconciliation Field Mappings** tab.
3. For each field that is of the IT resource type:
   a. Double-click the field to open the Edit Reconciliation Field Mapping window for that field.
   b. Deselect **Key Field for Reconciliation Matching**.

Configuring Provisioning

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

Note: You must perform this procedure if you want to use the provisioning features of Oracle Identity Manager for this target system.

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

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

- `CTUpdateUserProperty`
- `CTUpdateGroup`
- `CTStringTask`
- `CTModifyUser`
- `CTDeleteUser`
- `CTDeleteGroup`
- `CTCreateUser`
- `CTAssign Default Group`
- `CTAddGroup`
- `CTPrepopStartDate`
- `CTPrepopString`
- `CTPrepopDateAddOneYear`
- `CTEmailValidation`
- `CTAdd Default Group to User`
- `CTEndOrPwdExpDateValidatio`

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

To compile adapters by using the Adapter Manager form:

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

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

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

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`OIM_HOME`*`/xellerate/Adapter` directory to the

same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

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

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

To view detailed information about an adapter:

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

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 RSA ClearTrust.

You may want to configure the connector for multiple installations of RSA ClearTrust. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of RSA ClearTrust. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of RSA ClearTrust.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of RSA ClearTrust.

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

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

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

   The IT Resources form is in the Resource Management folder. An 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.

2. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you need to modify only the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

   You can designate either a single or multiple installations of RSA ClearTrust as the trusted source.

3. 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 RSA ClearTrust installation to which you want to provision the user.

4 Testing and Troubleshooting

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

- Running Connector Tests
- Troubleshooting

Running Connector Tests

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

To use the testing utility:

1. Modify the CLASSPATH environment variable to include the following:

```
OIM_HOME/xellerate/JavaTasks/xliClearTrust.jar
OIM_HOME/xellerate/XLIntegrations/ClearTrust/tests/lib/xliClearTrustTest.jar
OIM_HOME/xellerate/ext/ct_admin_api.jar
OIM_HOME/xellerate/ext/ct_runtime_api.jar
OIM_HOME/xellerate/ext/log4j-1.2.8.jar
OIM_HOME/xellerate/lib/xlLogger.jar
OIM_HOME/xellerate/lib/xlUtils.jar
OIM_HOME/xellerate/lib/xlVO.jar
```

2. Use the information in the following table to modify the default attributes given in the config.properties file. This file is in the *OIM_HOME*/xellerate/XLIntegrations/ClearTrust/tests/config/config.properties directory.

Attribute Name	Description	Default/Sample Value
machinename	Host name or IP address of the computer on which the RSA ClearTrust Entitlements Server is running	192.168.50.50
port	Port at which the RSA ClearTrust Entitlements Server is listening	5601
sslmode	Secure Sockets Layer (SSL) mode that the Entitlements Server is using: CLEAR, SSL_ANON, or SSL_AUTH	CLEAR
timeout	Timeout interval (in milliseconds) for connecting to the RSA ClearTrust Entitlements Server	10000 ms

Attribute Name	Description	Default/Sample Value
admingroup	Name of the default RSA ClearTrust Administrative group	*Default Administrative Group*
adminrole	Name of the default RSA ClearTrust Administrative role	*Default Administrative Role*
action	Action that is to be tested when Oracle Identity Manager connects to RSA ClearTrust The action can be connect, createuser, modifyattributes, getattributes, or deleteuser.	createuser
userid	User ID You must ensure that the ID does not exist in the RSA ClearTrust database.	c4
password	User's password	password
firstname	User's first name	Jane
lastname	User's last name	Doe
email	User's e-mail address	jane.doe@examplewidgets.com
startdate	User's date of hire All dates should be in the following format: YYYY-MM-DD	2004-02-28
enddate	User's account termination date	2005-02-28
password expirationdate	Date on which the user's password expires	2005-02-28
islock	Specifies whether or not the user is locked in RSA ClearTrust If the action attribute is set to connect, then this attribute does not apply.	false
loggerfile	Name and location of the log file	logs/Test_CTConnect.log
loggerlevel	Level of logging that is required The level can be one of the log levels discussed in the "Enabling Logging" section on page 2-3.	DEBUG

3. Enter a command similar to the following to run the CTConnectTest Java class file:

   ```
   java com.thortech.xl.integration.ct.tests.CTConnectTest
   config_with_full_path.properties ctadmin ctpassword
   ```

   For example:

   ```
   java com.thortech.xl.integration.ct.tests.CTConnectTest
   OIM_HOME/xellerate/XLIntegrations/ClearTrust/tests/config/config.properties
   admin admin
   ```

4. To verify that the designated action (for example, creating a user in RSA ClearTrust) is successful, check the log file specified in the config.properties file.

The following is sample output displayed in the log file:

```
29 Mar 2004 15:32:19 INFO Constructor: logs/Test_CTConnect.log DEBUG
29 Mar 2004 15:33:08 INFO Constructor: logs/Test_CTConnect.log DEBUG
29 Mar 2004 15:33:32 INFO Constructor: logs/Test_CTConnect.log DEBUG
29 Mar 2004 15:33:32 INFO CT_CONNECTION_SUCCESS
29 Mar 2004 15:36:46 INFO Constructor: logs/Test_CTConnect.log DEBUG
29 Mar 2004 15:36:46 INFO CT_CONNECTION_SUCCESS
29 Mar 2004 15:36:46 INFO CT_USERCREATION_SUCCESS
29 Mar 2004 15:36:46 INFO CT_CLOSECONNECTION_SUCCESS
```

Troubleshooting

The following table lists solutions to some commonly encountered errors associated with the connector.

Problem	Solution
Oracle Identity Manager cannot establish a connection with RSA ClearTrust.	■ Ensure that the RSA ClearTrust Entitlements Server is running. ■ Check the port on which the RSA ClearTrust Entitlements Server is running. Ensure that the same port number is specified in the `Port` parameter. ■ Validate the administrator's user ID, password, group, and role by using the Oracle Identity Manager Administrative and User Console. ■ Ensure that the SSL mode in which the Entitlements Server is running is the same as the SSL mode that is specified in the `SSLMode` parameter of the RSA ClearTrust IT resource. ■ Ensure that all required RSA ClearTrust JAR files are present in the *`OIM_HOME`*`\Xellerate\ext` directory.
Oracle Identity Manager cannot modify a user ID.	The user ID must be unique in RSA ClearTrust. Ensure that no other user has the same distinguished name.
An incompatible version is found for some classes.	Ensure that Oracle Identity Manager is using JDK 1.4.2 or later.
Oracle Identity Manager cannot provision a user with RSA ClearTrust. In addition, the following error message is displayed: `Data validation failed.`	■ Ensure that the AutoSave feature of the RSA ClearTrust provisioning process is enabled. ■ Ensure that the `CTPrepopServerInfo` adapter is compiled and assigned to the custom process form. ■ Ensure that the run-time and return variables of the connector are mapped properly.
Oracle Identity Manager cannot assign a default group to the user who has been provisioned with RSA ClearTrust. In addition, the following error message is displayed: `ct user group object not found fail`	Ensure that the default group specified in the RSA ClearTrust IT resource matches the group created in RSA ClearTrust.

5 Known Issues

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

- The connector supports provisioning against only one RSA ClearTrust server.
- The connector supports only users of RSA ClearTrust, not administrators. You must use RSA ClearTrust to create and manage administrators.
- 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 RSA ClearTrust

The following table discusses attribute mappings between Oracle Identity Manager and RSA ClearTrust.

Oracle Identity Manager Attribute	RSA ClearTrust Attribute	Description
User Id	User ID	User ID
Password	Password	Password
Password Expiration Date	Password Expires	Date and time the user's password expires
First Name	First Name	First name
Last Name	Last Name	Last name
Email Address	E-mail	E-mail address
Start Date	Account Starts	Date and time when the user's account must become active
End Date	Account Expires	Date and time when the user's account must expire
Lock User	Lock Out	Flag that indicates whether or not the user is locked out
Is Public	Visibility	Flag that specifies whether the user account is visible to all administrators or only to administrators of this administrative group
User Group Name	User Group	Group
Property Name	Property Name	Name of the property
Property Value		Property value Depending on the data type of the selected property, the value can be a string or integer.
Property Value (Date)		Property value as date
Property Value (Boolean)		Property value as Boolean

Index