Oracle® Identity Manager

Connector Guide for RSA ClearTrust

Release 9.0.2

B32169-01

September 2006

ORACLE®

Oracle Identity Manager Connector Guide for RSA ClearTrust, Release 9.0.2

B32169-01

Contents

3   Testing and Troubleshooting

4   Known Issues

Index

Preface

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

> **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 RSA ClearTrust.

Documentation Accessibility

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

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

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

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.2 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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 RSA ClearTrust?

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

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

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

Incorporation of Multilanguage Support

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

- The installation media directory includes resource bundle files for the languages supported by the connector. These resource bundle files are described in the "Files and Directories That Comprise the Connector" section on page 1-4.

- The "Step 2: Copying the Connector Files and External Code" section on page 2-1 specifies the destination directory into which you must copy the resource bundle files during the deployment procedure.

- The "Step 3: Configuring the Oracle Identity Manager Server" section on page 2-2 describes the procedure to change to the required input locale and to clear content related to connector resource bundles from the server cache.

- Two new IT resource parameters have been added to carry country code and language code information to the target system. These parameters are described in the "Defining IT Resources" section on page 2-5.

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

Determining the Release Number of the Connector

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

Additions to the IT Resource Definition

The following IT resource parameters have been added in the "Defining IT Resources" section on page 2-5:

- `Trusted Source Recon - Resource Object name`

- `Date Format`

Documentation-Specific Updates

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

- Oracle Identity Manager uses an RSA ClearTrust user account to connect to and exchange data with RSA ClearTrust. The "Step 1: Verifying Deployment Requirements" section on page 2-1 provides information about the minimum rights that must be assigned to this user account.

- Instructions to copy the connector JAR files and adapter files to all the nodes of a clustered environment have been added in the following sections:

  - Step 2: Copying the Connector Files and External Code on page 2-1

  - Step 3: Configuring the Oracle Identity Manager Server on page 2-2

  - Step 6: Compiling Adapters on page 2-9

- Instructions and pointers to information about configuring trusted source reconciliation have been moved to the "Configuring Trusted Source Reconciliation" section on page 2-7.

- Instructions to enable reconciliation in Oracle Identity Manager release 9.0.1 have been added in the "Enabling Reconciliation in Oracle Identity Manager Release 9.0.1" section on page 2-9.

- Instructions to use Oracle Identity Manager for linking multiple installations of RSA ClearTrust are given in the "Configuring the Connector for Multiple Installations of the Target System" on page 2-10.

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 RSA ClearTrust is used to integrate Oracle Identity Manager with RSA ClearTrust.

> **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
- 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.

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

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

- French

- Japanese

Reconciliation Module

The reconciliation module extracts the following elements from the target system to construct reconciliation event records:

- 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 putting 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

Provisioning Module

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)

Files and Directories That Comprise the Connector

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

```
Web Access Control\RSA ClearTrust\RSA ClearTrust Rev 3.1.0.zip
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
xml\XLIClearTrust_DM.xml xml\XLIClearTrustEntityAdp_DM.xml	These XML files contain definitions for the following components of the RSA ClearTrust connector: - IT resource type - Custom process form - Process task and adapters (along with their mappings) - Login resource object - Provisioning process - Pre-populate rules
xml\XLICTAutoSaveAdapter_DM.xml	This XML file contains the code for the adapter that is required to enable the AutoSave feature in the RSA ClearTrust provisioning process form.
xml\XLIClearTrustScheduleTask_DM.xml	This XML file contains the code for the reconciliation scheduled task and its attributes.
lib\xliClearTrust.jar	This JAR file contains the Java classes that are required for provisioning.
Files in the resources directory	Each of these files contains locale-specific information that is used by the connector.
test\config\config.properties	This file contains the properties that are used to connect to the RSA ClearTrust server.

File in the Installation Media Directory	Description
test\lib\xlicleartrusttest.jar	This JAR file contains the test classes that can be used to test the functionality of the connector.
docs\B31133_01.pdf	This guide, which provides instructions to deploy the connector.

> **Note:** The files in the test directory are used only to run tests on the connector.

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

Determining the Release Number of the Connector

To determine the release number of the connector:

1. Extract the contents of the xliClearTrust.jar file. This file is in the lib directory inside the installation media directory.

2. Open the manifest.mf file in a text editor, which is one of the files bundled inside the 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

- Step 3: Configuring the Oracle Identity Manager Server

- Step 4: Importing the Connector XML Files

- Step 5: Configuring Reconciliation

- Step 6: Compiling Adapters

If you want to configure the connector for multiple installations of RSA ClearTrust, then perform the following procedure:

- Configuring the Connector for Multiple Installations of the Target System

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 or later
Target systems	RSA ClearTrust 5.5 or 5.52

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 the "Defining IT Resources" section on page 2-5.

Step 2: Copying the Connector Files and External Code

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

> **Note:** Some of the directory paths given in the first column of this table correspond to the location of the connector files in the following ZIP file on the installation media:
>
> ```
> Web Access Control\RSA ClearTrust\RSA ClearTrust Rev 3.1.0.zip
> ```
>
> Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

File	Destination Directory
Files in the `xml` directory on the installation media	`OIM_home\xellerate\XLIntegrations`
`lib\xliClearTrust.jar`	`OIM_home\xellerate\JavaTasks` `OIM_home\xellerate\ScheduleTask`
Files in the `resources` directory on the installation media	`OIM_home\xellerate\connectorResources`
Files in the `test` directory on the installation media	`OIM_home\xellerate\test`
`docs\B31133_01.pdf`	`OIM_home\xellerate\docs\ClearTrust`

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 `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.

- Adding a Log Module
- Changing to the Required Input Locale

■ [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)

Adding a Log Module

To add a log module, in the *OIM_home*\config\log.properties file, add an entry similar to the following for a new log module:

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

You can specify any one of the following log levels:

■   DEBUG

■   INFO

■   WARN

■   ERROR

■   FATAL

Changing to the Required Input Locale

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

To set the required input locale:

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

1. Open Control Panel.

2. Double-click **Regional Options**.

3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle file in the *OIM_home*\xellerate\connectorResources directory or make a change in an existing resource bundle file, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *OIM_home*\xellerate\bin directory.

2. Enter one of the following commands:

> **Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:
>
> *OIM_home*\xellerate\bin*batch_file_name*

■   On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

■ On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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

OIM_home\xellerate\config\xlConfig.xml

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

Step 4: Importing the Connector XML Files

You must import the connector XML files into Oracle Identity Manager in the following sequence:

1. `XLIClearTrust_DM.xml`

2. `XLIClearTrustEntityAdp_DM.xml`

3. `XLICTAutoSaveAdapter_DM.xml`

4. `XLIClearTrustScheduleTask_DM.xml`

> **Caution:** If you do not import the connector XML files in the specified order, then the connector may not work.

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 locating files is displayed.

4. Locate and open the `XLIClearTrust_DM.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 the "Defining IT Resources" section on page 2-5 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 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.

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 "Step 5: Configuring Reconciliation" section on page 2-6.

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.
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.
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.

Parameter	Description
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.

Step 5: Configuring Reconciliation

This section discusses the following topics:

- Adding Prerequisites for Reconciliation

- Creating Scheduled Tasks

- Enabling Reconciliation in Oracle Identity Manager Release 9.0.1

Adding Prerequisites for Reconciliation

This section describes the following prerequisite steps for configuring reconciliation:

- Configuring System Properties

- Configuring Trusted Source Reconciliation

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 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 configure trusted source reconciliation for this connector 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.

This procedure involves the following steps:

1. In the Oracle Identity Manager Design Console, open the Resource Object form.

2. Search for the Xellerate User.

3. On the Object Reconciliation tab, add reconciliation fields as required. Add all those reconciliation fields that would be needed to provide input for the mandatory fields in the Xellerate User form, such as User Login and First Name. However, you can ignore the Password field, although it is a mandatory field.

4. Open the Process Definition form.

5. Search for the Xellerate User.

6. On the Reconciliation Field Mappings tab, add the required reconciliation field mappings. All the mandatory fields of the User Defined process form must be mapped.

7. Open the Reconciliation Rules form.

8. Create a rule for the Xellerate User object, with a rule element as required. The Reconciliation Rules form is in the Development Tools folder.

9. After you create the rule, select the **Active** check box.

Creating Scheduled Tasks

To create the scheduled task:

1. Open the Oracle Identity Manager Design Console.

2. Expand the **Xellerate Administration** folder.

3. Select **Task Scheduler.**

4. Click **Find**. The details of the predefined scheduled task are displayed.

5. 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, 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 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 Oracle Identity Manager resource object	The default value is Xellerate User
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
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 2-6.	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 9.0.1

If you are using Oracle Identity Manager release 9.0.1, 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**.

Step 6: Compiling Adapters

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

- `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 you can use them to provision accounts on the target system.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.

2. To compile all the adapters that you import into the current database, select **Compile All**.

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

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

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.

4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_home*\xellerate\Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes. Then, restart each node.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.

2. Double-click the row header of the adapter, or right-click the adapter.

3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

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

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. 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 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 "Step 5: Configuring Reconciliation" section on page 2-6 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.

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 Connector Tests
- Troubleshooting

Running Connector Tests

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. Modify the CLASSPATH environment variable to include the following:

```
OIM_home\Xellerate\XLIntegrations\ClearTrust\lib\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\xl.jar
OIM_home\Xellerate\XLIntegrations\ClearTrust\tests
```

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 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 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	`welcome1`
firstname	User's first name	`Jane`
lastname	User's last name	`Doe`
email	User's e-mail address	`jane.doe@acmewidgets.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 `DEBUG`, `INFO`, `WARN`, or `FATAL`.	`DEBUG`

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

```
java CTConnectTest config.properties ctadmin ctpassword
```

For example:

```
java com.thortech.xl.integration.ct.tests.CTConnectTest
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's distinguished name.	The distinguished name must be unique in RSA ClearTrust. Ensure that no other user has the same distinguished name.
Related classes for RSA ClearTrust are not found.	Ensure that the RSA ClearTrust JAR files are added into the CLASSPATH environment variable correctly.
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_USERGROUP_OBJECT NOTFOUND_FAIL`	Ensure that the default group specified in the RSA ClearTrust IT resource matches the group created in RSA ClearTrust.

4

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 locale and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

Index

R

reconciliation
  configuring,   2-6
  enabling in Oracle Identity Manager Release
      9.0.1,   2-9
  functions,   1-1
  module,   1-3
  trusted source,   2-7
requirements for deploying,   2-1

S

scheduled tasks
  defining,   2-6
server cache, clearing,   2-3
supported
  languages,   1-2
  releases of Oracle Identity Manager,   2-1
  target systems,   2-1
supported versions
  Oracle Identity Manager,   2-1

T

target system, multiple installations,   2-10
target systems supported,   2-1
testing the connector,   3-1
troubleshooting,   3-3
trusted source reconciliation,   2-7

V

version number of connector, determining,   1-5

X

XML files
  importing,   2-4