

Oracle® Identity Manager

Connector Guide for RSA ClearTrust

Release 9.0.1

B31133-01

June 2006

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

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

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

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

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
 1 About the Connector	
Supported Functionality	1-1
Reconciliation Module	1-3
Provisioning Module	1-3
Files and Directories That Comprise the Connector	1-4
 2 Deploying the Connector	
Step 1: Verifying Deployment Requirements	2-1
Step 2: Configuring the Oracle Identity Manager Server	2-1
Adding a Log Module	2-2
Step 3: Copying the Connector Files and External Code	2-2
Step 4: Importing the Connector XML Files	2-2
Defining IT Resources	2-3
Step 5: Configuring Reconciliation	2-4
Adding Prerequisites for Reconciliation	2-5
Configuring System Properties	2-5
Configuring Trusted Source Reconciliation Oracle Identity Manager Entities	2-5
Defining Scheduled Tasks	2-5
Step 6: Compiling Adapters	2-7
 3 Testing the Connector	
Running Connector Tests	3-1
Troubleshooting	3-3
 4 Known Issues	
 Index	

Preface

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

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. 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 Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

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](#)
- [Reconciliation Module](#)
- [Files and Directories That Comprise 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 in RSA ClearTrust with the input values provided
Delete User	Provisioning	Deletes a provisioned user in RSA ClearTrust
Disable User	Provisioning	Disables an existing user in RSA ClearTrust
Enable User	Provisioning	Enables a disabled user in RSA ClearTrust
Update User	Provisioning	updates an existing user in RSA ClearTrust with the input values provided
Set Password	Provisioning	Sets a password when a user is first created in RSA ClearTrust
Change Password	Provisioning	Updates a user's password in RSA ClearTrust

Process Task	Type	Description
Assign User to a Group	Provisioning	<p>Assigns a user to a group in RSA ClearTrust</p> <p>To map an RSA ClearTrust group to Oracle Identity Manager:</p> <ol style="list-style-type: none"> 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 in RSA ClearTrust
Assign a Default Group to the User	Provisioning	Assigns a default group to a user in RSA ClearTrust
Update User Property	Provisioning	<p>Assigns or removes a property value</p> <p>If the RSA ClearTrust property type is <code>Date</code>, then the corresponding value for the property can only be set by using the Property Value (Date) field in the RSA ClearTrust User Properties form. If the ClearTrust property type is <code>Boolean</code>, then the corresponding value for the property can only be set by using the Property Value (Boolean) check box in the ClearTrust User Properties form.</p> <p>To set the value of any other type of property, use the Property Value field.</p>
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

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 of the RSA ClearTrust connector are provisioned.

Name	Data Type
User ID	String

Name	Data Type
Password	String
Password Expiration Date	Date
First Name	String
Last Name	String
Email Address	String
Start Date	Date
End Date	Date
Lock User	Boolean
Is Public	Boolean
User Group Name	String
Property Value	String
Property Name	String
Property Value (Date)	Date
Property Value (Boolean)	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 3.0.0.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	<p>These XML files contain the following components of the RSA ClearTrust connector:</p> <ul style="list-style-type: none">■ 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	<p>This XML file contains the code for the adapter that is required to enable the AutoSave feature on the RSA ClearTrust provisioning process form.</p>
xml\XLIClearTrustScheduleTask_DM.xml	<p>This XML file contains the code for the reconciliation scheduled task and its attributes.</p>
lib\xliClearTrust.jar	<p>This JAR file contains the Java classes that are required for provisioning.</p>
test\config\config.properties	<p>This file contains the properties that are used to connect to the RSA ClearTrust server.</p>

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 docs\html	These are PDF and HTML versions of 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 3: Copying the Connector Files and External Code"](#) section on page 2-2 provides instructions to copy these files into the required directories.

Deploying the Connector

Deploying the connector involves the following steps:

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

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 system	RSA ClearTrust 5.5 or 5.52
Target system host platform	Any one of the following operating systems: <ul style="list-style-type: none">■ Microsoft Windows 2000■ Microsoft Windows 2003■ Solaris 8■ Solaris 9
External code	<p>The following files from the directory in which RSA ClearTrust is installed:</p> <ul style="list-style-type: none">■ <code>ct_admin_api.jar</code>■ <code>ct_runtime_api.jar</code>■ <code>cleartrust.jar</code> <p>Refer to the "Step 3: Copying the Connector Files and External Code" section on page 2-2 for information about copying these files to the required directories.</p>

Step 2: Configuring the Oracle Identity Manager Server

This section discusses the following:

Adding a Log Module

In the `xellerate_home/config/log.properties` file, add an entry similar to the following for a new log module:

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

The following are the log levels that you can use:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

Step 3: Copying the Connector Files and External Code

The following table lists the files to be copied and the locations where you must copy them.

File in the Installation Media Directory	Destination Directory
The following files from the Web Access Control\RSA ClearTrust\RSA ClearTrust Rev 3.0.0\xml directory:	
■ XLIClearTrust_DM.xml	<code>xellerate_home/xellerate/XLIntegrations/</code>
■ XLIClearTrustEntityAdp_DM.xml	
■ XLICTAutoSaveAdapter_DM.xml	
■ XLIClearTrustScheduleTask_DM.xml	
The following files from the <code>ClearTrust_installation_dir/lib</code> directory:	
■ <code>ct_admin_api.jar</code>	<code>xellerate_home/ThirdParty</code>
■ <code>ct_runtime_api.jar</code>	
■ <code>cleartrust.jar</code>	
<code>ClearTrust_installation_dir/lib/xlicle</code>	<code>xellerate_home/xellerate/JavaTasks</code>
<code>arTrust.jar</code>	<code>xellerate_home/xellerate/ScheduleTask</code>
The following files from the Web Access Control\RSA ClearTrust\RSA ClearTrust Rev 3.0.0\test directory:	
<code>config\config.properties</code>	<code>xellerate_home/xellerate/test</code>
<code>lib\xlicleartrusttest.jar</code>	
<code>docs\B31133_01.pdf</code>	<code>xellerate_home/xellerate/docs</code>
<code>docs\html</code>	

Step 4: Importing the Connector XML Files

You must import the following 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 `xellerate_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 2-3 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. You must remove these nodes. To do this, right-click each such node and then select **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 `xellerate_home/xellerate/XLIntegrations/ClearTrust/xml` directory.

Defining IT Resources

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

Parameter Name	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	Name or IP address of the computer on which the RSA ClearTrust entitlement server is running. This is the same computer to which Oracle Identity Manager connects. This is a required parameter.
Port	Port number on which the RSA ClearTrust entitlement server is running This is a required parameter.
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.
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

After you specify values for these IT resource parameters, go 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](#)
- [Defining Scheduled Tasks](#)

Adding Prerequisites for Reconciliation

This section describes the following steps involved in configuring the Oracle Identity Manager server:

- [Configuring System Properties](#)
- [Configuring Trusted Source Reconciliation Oracle Identity Manager Entities](#)

Configuring System Properties

1. Open the Oracle Identity Manager Design Console.
2. Navigate to the System Configuration page.
3. Add a new entry in the Server category:

Name: Default date format

Keyword: XL.DefaultDateFormat

Value: MMM dd, yyyy 'at' hh:mm:ss z
4. Click **Save**.

Configuring Trusted Source Reconciliation Oracle Identity Manager Entities

This procedure involves the following steps:

1. Open the Resource Object form, and search for the Xellerate User. On the Object Reconciliation tab, add the required reconciliation fields. You must add the reconciliation fields that would be needed to provide input for mandatory fields in the Xellerate User form. For example, fields like User Login and First Name. Although the Password field is mandatory, you can ignore it. There must be mappings to all mandatory fields of the User Defined process form.
2. Open the Process Definition form, and search for the Xellerate User. On the Reconciliation Field Mappings tab, add the required reconciliation field mappings. All the mandatory fields of the user defined process form should be mapped.
3. Open the Reconciliation Rules form, and create a new rule for the Xellerate User resource object, with a rule element.
4. After creating the rule, select the **Active** check box.

Defining Scheduled Tasks

Configuring reconciliation involves creating scheduled tasks for lookup fields and user reconciliations. To create a scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.

5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the ERROR status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
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 Name	Description	Sample Value
Server	Name of the IT Resource	ClearTrustITResource
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	In case the user does not want to do a complete scheduled reconciliation and quickly want to check connectivity with the target and reconcile few records to ensure that reconciliation with the relevant target is working, this parameter could be used. The number of records, to be reconciled (ONLY) could be mentioned here.	3
UseReconFieldMap	This attribute is for the Client Customize reconciliation activity. The Client Customize reconciliation is activated and the fields in the Attribute Name: CTRconciliationFields lookup are reconciled if this attribute is set to true. Otherwise, all the available fields are reconciled.	True
CTRconciliationFields	This lookup definition stores the reconciliation fields data that is used in customized reconciliation.	Lookup.CTRconciliation.FieldMap

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

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

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

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

To compile adapters by using the Adapter Manager form:

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

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

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 adapters that you specify.

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 multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

Note: In earlier releases of this guide, the connector was referred to as the *integration*.

This chapter contains the following sections:

- [Running Connector Tests](#)
- [Troubleshooting](#)

Running Connector Tests

This section discusses test cases that you can perform by using the troubleshooting utility.

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

Before you can use the troubleshooting utility, you must set the required values in the `config.properties` file. This file is in the `xellerate_home/xellerate/XLIntegrations/ClearTrust/tests/config/config.properties` directory.

After you specify the required values in the `config.properties` file, perform the following steps to run the test cases:

1. Modify the classpath file to include the following:

```
xellerate_home/Xellerate/XLIntegrations/ClearTrust/lib/xliClearTrust.jar
xellerate_home/Xellerate/XLIntegrations/ClearTrust/tests/lib/xliClearTrustTest.jar
xellerate_home/Xellerate/ext/ct_admin_api.jar
xellerate_home/Xellerate/ext/ct_runtime_api.jar
xellerate_home/Xellerate/ext/log4j-1.2.8.jar
xellerate_home/Xellerate/lib/xl.jar
xellerate_home/Xellerate/XLIntegrations/ClearTrust/tests
```

2. Use the following table to modify the default attributes of the `config.properties` file. This file is in the `xellerate_home/Xellerate/XLIntegrations/ClearTrust/tests/config` directory.

Attribute Name	Description	Default Value
machinename	The name or IP address of the computer on which the RSA ClearTrust Entitlements server is running	192.168.50.50
port	The number of the port on which the RSA ClearTrust Entitlements server is listening	5601
sslmode	The Secure Sockets Layer (SSL) mode that the Entitlements server is using (CLEAR, SSL_ANON, or SSL_AUTH)	CLEAR
timeout	The timeout interval (in milliseconds) for connecting to the RSA ClearTrust Entitlements server	10000 ms
admingroup	The name of the default RSA ClearTrust Administrative group	<i>Default Administrative Group</i>
adminrole	The name of the default RSA ClearTrust Administrative role	<i>Default Administrative Role</i>
action	The 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	The User ID Ensure that the ID does not exist in the RSA ClearTrust database.	c4
password	The user's password	welcome1
firstname	The user's first name	Jane
lastname	The user's last name	Doe
email	The user's e-mail address	jane.doe@acmewidgets.com
startdate	The user's date of hire All dates should be in the following format: YYYY-MM-DD	2004-02-28
enddate	The user's account termination date	2005-02-28
password expirationdate	The date on which the user's password expires	2005-02-28
islock	This Boolean attribute represents 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	The location and name of the log file	logs/Test_CTConnect.log
loggerlevel	The level of logging that is required The level of logging can be DEBUG, INFO, WARN, or FATAL.	DEBUG

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

```
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 the 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 issues associated with the connector.

Problem	Solution
Oracle Identity Manager cannot establish a connection with RSA ClearTrust.	<ul style="list-style-type: none"> ■ Ensure that the RSA ClearTrust Entitlements server is running. ■ Check the port on which the RSA ClearTrust Entitlements server is running. Verify 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. ■ Verify 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. ■ Check that all required RSA ClearTrust JAR files are present in the <code>xellerate_home/Xellerate/ext</code> directory. ■ Verify that the <code>jnet.jar</code>, <code>jsse.jar</code>, <code>jcrt.jar</code>, and <code>jcel_4.jar</code> files are present in the <code>xellerate_home/java/jre/lib/ext</code> directory.
Oracle Identity Manager cannot modify a user's distinguished name.	The distinguished name must be unique in RSA ClearTrust. Verify 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 file correctly.
An incompatible version is found for some classes.	Ensure that Oracle Identity Manager is using JDK 1.4.2, and not JDK 1.3.

Problem	Solution
<p>Oracle Identity Manager cannot provision a user with RSA ClearTrust. In addition, the following error message is displayed:</p> <p>Data validation failed.</p>	<ul style="list-style-type: none"> ■ Ensure that the AutoSave feature of the RSA ClearTrust provisioning process is enabled. ■ Verify that the CTPrepopServerInfo adapter is compiled and assigned to the custom process form. ■ Check the run-time and return variables of the connector to ensure that they are mapped properly.
<p>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:</p> <p>CT_USERGROUP_OBJECT NOTFOUND_FAIL</p>	<p>Ensure that the default group specified in the RSA ClearTrust IT Resource matches the group created in RSA ClearTrust.</p>

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.

Index

A

Adapter Factory form, 2-8
Adapter Manager form, 2-7

C

configuring Oracle Identity Manager server, 2-1
configuring reconciliation, 2-4
connector files and directories
 copying, 2-2
 description, 1-4
 destination directories, 2-2
 installation media file, 1-4
connector testing, 3-1
connector XML files
 See XML files

D

defining scheduled tasks, 2-4
deployment
 requirements, 2-1

E

errors, 3-3

F

files and directories of the connector
 See connector files and directories
functionality supported, 1-1
functions available, 1-1

I

importing connector XML files, 2-2
issues, 4-1

L

limitations, 4-1

O

Oracle Identity Manager Administrative and User

 Console, 2-3
Oracle Identity Manager server configuration, 2-1

P

problems, 3-3
process tasks, 1-1
provisioning
 fields, 1-3
 functions, 1-1
 module, 1-3

R

reconciliation
 configuring, 2-4
 module, 1-3
reconciliation functions, 1-1
requirements for deploying, 2-1

S

supported target systems, 2-1
supported versions
 Oracle Identity Manager, 2-1

T

testing the connector, 3-1
troubleshooting, 3-3

X

XML files
 importing, 2-2

