Oracle® Identity Manager

Connector Guide for RSA ClearTrust

Release 9.0.4

E10440-07

December 2010

ORACLE®

Oracle Identity Manager Connector Guide for RSA ClearTrust, Release 9.0.4

E10440-07

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

2 Deploying the Connector

3 Using the Connector

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with RSA ClearTrust.

Audience

This guide is intended for resource administrators and target system integration teams.

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.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://www.oracle.com/technology/documentation/oim1014.html

Documentation Updates

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

http://www.oracle.com/technology/documentation/oim1014.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 software and documentation for the RSA ClearTrust connector in release 9.0.4.12.

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.

Software Updates

The following sections discuss software updates:

- Software Updates Up To Release 9.0.4.1
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.11
- Software Updates in Release 9.0.4.12

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 Section 1.2, "Certified Languages."

Support for Oracle Application Server

Earlier releases of the connector supported the following application servers:

- JBoss Application Server

- Oracle 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

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 Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" 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
- Copying the Connector Files

Resolved Issues

The following are issues 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.

Software Updates in Release 9.0.4.3

The following is an issue resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
8538409	When you locked a user on the process form, the user was set to the Disabled state in Oracle Identity Manager and the Locked state on the target system.	This issue has been resolved. The Lock User and Unlock User functions are no longer linked with the Enable User and Disable User functions. Instead, the Enable User and Disable User functions are linked with the Account Expires attribute.

Software Updates in Release 9.0.4.11

The following are the software updates in release 9.0.4.11 of the connector:

- Support for New Target System
- Support for Synchronization of Group Lookup Field

Support for New Target System

From this release onward, the connector adds support for RSA Access Manager V6.1 as the target system.

This target system is mentioned in the "Step 1: Verifying Deployment Requirements" section.

Support for Synchronization of Group Lookup Field

From this release onward, the connector supports group lookup field synchronization. The Clear Trust Group Lookup Reconciliation Task scheduled task is used to automate reconciliation of group lookup data.

See the "Scheduled Task for Group Lookup Field Synchronization" section in the connector guide for more information.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.5.2, "Request-Based Provisioning" for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates Up To Release 9.0.4.3

Documentation-Specific Updates Up To Release 9.0.4.3

The following are documentation-specific updates up to release 9.0.4.3:

- Instructions in "Configuring Trusted Source Reconciliation" on page 2-9 have been revised.
- Instructions in the following sections have been revised:
  - Configuring Trusted Source Reconciliation on page 3-1
- Instructions in the "Running Connector Tests" on page 5-1 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.
- From the "Known Issues" chapter, two known issues have been removed.
- From this release onward:

  The minimum certified release of Oracle Identity Manager is release 9.1.0.1.

  The minimum certified release of JDK is release 1.4.2.

  See "Step 1: Verifying Deployment Requirements" for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.11

The following is a documentation-specific update in release 9.0.4.11:

The "User Reconciliation Scheduled Task" section has been added.

Documentation-Specific Updates in Release 9.0.4.12

There are no documentation-specific updates in release 9.0.4.12.

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 external, identity-aware applications. This guide discusses the connector that enables you to use RSA ClearTrust either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

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

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

> **Note:** It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

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*.

1.1 Certified Components

Table 1–1 lists the certified components for this connector.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through 9.0.3.2 ■ Oracle Identity Manager release 9.1.0.1 or later **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) BP02 **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1). The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at http://www.oracle.com/technetwork/documentation/oim1014-097544.html
Target systems	The target system can be one of the following: ■ RSA ClearTrust V5.5.*x* ■ RSA Access Manager V6.0.*x* and V6.1.*x*
External code	The following files from the directory in which RSA ClearTrust is installed: ct_admin_api.jar ct_runtime_api.jar
Target system user account	RSA ClearTrust administrator account You provide the credentials of this user account while performing the procedure in Section 2.2.2.2, "Configuring the IT Resource."
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.2, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)

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

See Also: One of the following guides for information about supported special characters supported by Oracle Identity Manager:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*:

  Oracle Identity Manager Globalization Guide

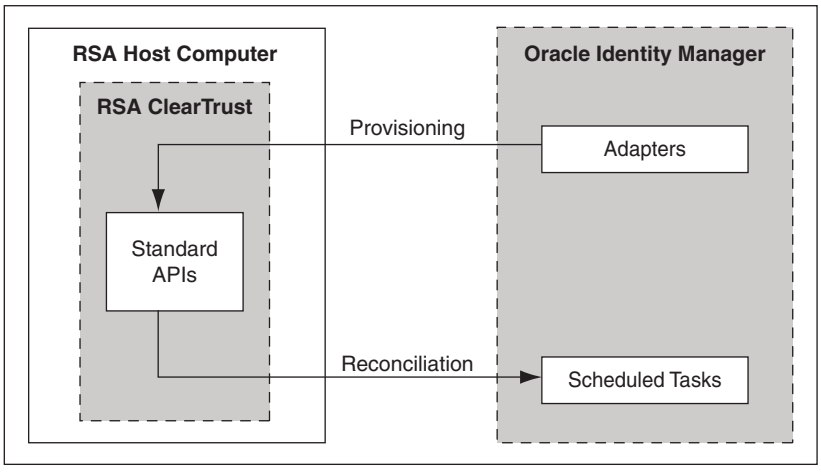
- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

1.3 Connector Architecture

The architecture of the connector is the blueprint for the functionality of the connector. Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



The connector can be configured to run in one of the following modes:

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

- Identity reconciliation

  In the identity reconciliation mode, RSA ClearTrust is used as the trusted source and users are directly created and modified on it.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager.

  Each record fetched from the target system is compared with existing OIM Users. If a match is found, then the update made to the record on the target system is applied to the OIM User record. If no match is found, then the target system record is used to create an OIM User.

- Account Management

  In the account management mode, RSA ClearTrust is used as a target resource. The connector enables target resource reconciliation and provisioning operations. Through provisioning operations performed on Oracle Identity Manager, user accounts are created and updated on the target system for OIM Users. During reconciliation from the target resource, the RSA ClearTrust connector fetches into Oracle Identity Manager data about user accounts that are created or modified on the target system. This data is used to add or modify resources allocated to OIM Users.

  During provisioning operations, adapters carry provisioning data submitted through the process form to the target system. APIs on the target system accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager. The next step depends on the mode of connector configuration.

1.4 Features of the connector

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure RSA ClearTrust as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3.4, "User Reconciliation Scheduled Task" for more information.

1.4.2 Specifying the Attributes That Must Be Used During Reconciliation

You can specify the subset of target system attributes that must be reconciled. See Section 3.3.3, "Specifying the Attributes That Must Be Used During Reconciliation" for more information.

1.4.3 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

1.4.4 Support for Paged Reconciliation

Paged reconciliation is the reconciliation of a specified set of target system records at a time, within a reconciliation run. Multiple pages of records are fetched to complete the reconciliation run. This feature helps reduce memory issues that might arise when there are a large number of records to be reconciled.

Paged reconciliation is implemented using the Paging Range attribute of the scheduled task. See Section 3.3.2, "Paged Reconciliation" for more information about paged reconciliation.

1.5 Lookup Definitions Used During Connector Operations

Lookup definitions used during connector operations can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Group lookup field to select the group to which the user must be assigned. When you deploy the connector, the CTGroups and Property Names lookup definitions are automatically created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the list of groups and properties on the target system into the CTGroups and Property Names lookup definitions in Oracle Identity Manager.

See Also: Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.CTReconciliation.Fieldmap	This lookup definition is used to store mappings of attributes that you add for reconciliation.	You can add entries in this lookup definition if you want to map new target system attributes for reconciliation. Section 3.3.3, "Specifying the Attributes That Must Be Used During Reconciliation" describes the procedure.

1.6 Connector Objects Used During Target Resource Reconciliation

This section discusses the following topics:

- Section 1.6.1, "User Attributes for Target Resource Reconciliation"
- Section 1.6.2, "Reconciliation Rules for Target Resource Reconciliation"
- Section 1.6.3, "Reconciliation Action Rules for Target Resource Reconciliation"

1.6.1 User Attributes for Target Resource Reconciliation

Table 1–3 lists the user attributes of the target system from which values are fetched during reconciliation. The ClearTrust Reconciliation Task scheduled task is used to reconcile user data.

Table 1–3 User Attributes for Target Resource Reconciliation

Resource Object Field	Target System Attribute	Description
UserID	User ID	User ID
FirstName	First Name	First Name
LastName	Last Name	Last Name
EmailID	E-mail	E-mail address
StartDate	Account Starts	Date and time when the user's account must become active
EndDate	Account Expires	Date and time when the user's account must expire
PasswordExpDate	Password Expires	Date and time the user's password expires
IsPublic	Visibility	Flag that specifies whether the user account is visible to all administrators or only to administrators of this administrative group
IsUserlocked	Lock Out	Flag that indicates whether or not the user account is locked
PropertyName	Property Name	Name of the property
PropertyValue	Property Value	Depending on the data type of the selected property, the value can be a string or integer.
GroupName	User Group	Group

1.6.2 Reconciliation Rules for Target Resource Reconciliation

See Also: For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following sections provide information about the reconciliation rules for this connector:

- Section 1.6.2.1, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.2.2, "Viewing Reconciliation Rules for Target Resource Reconciliation in the Design Console"

1.6.2.1 Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

Rule name: CT Recon Rule

Rule element: User Login Equals (userId)

In the rule element:

- User Login is one of the following:
  - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2:

    User ID attribute on the Xellerate User form
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

    User ID attribute on the OIM User form
- userId is the user ID field of the account on RSA ClearTrust.

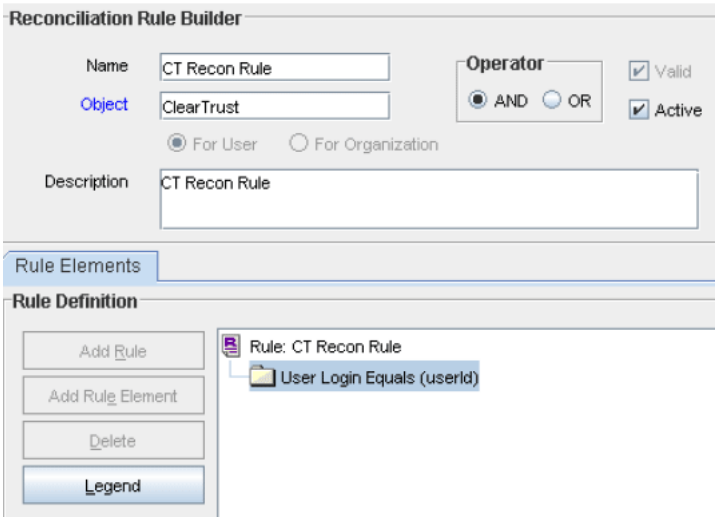
1.6.2.2 Viewing Reconciliation Rules for Target Resource Reconciliation in the Design Console

After you deploy the connector, you can view the reconciliation rule for reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open **CT Recon Rule**. Figure 1–2 shows this reconciliation rule.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.3 Reconciliation Action Rules for Target Resource Reconciliation

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

The following sections provide information about the reconciliation rules for this connector:

- Section 1.6.3.1, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.3.2, "Viewing Reconciliation Action Rules for Target Resource Reconciliation in the Design Console"

1.6.3.1 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–4 lists the action rules for target resource reconciliation.

Table 1–4 Action Rules for Target Resource Reconciliation

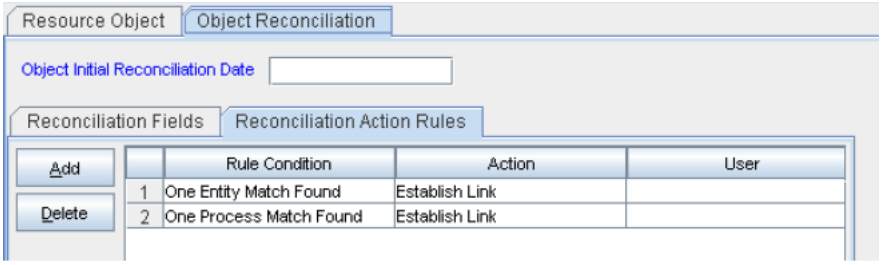
Rule Condition	Action
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.6.3.2 Viewing Reconciliation Action Rules for Target Resource Reconciliation in the Design Console

After you deploy the connector, you can view the reconciliation action rules for reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **ClearTrust** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rules for reconciliation.

Figure 1–3 Action Rules for Target Resource Reconciliation



1.7 Connector Objects Used During Trusted Source Reconciliation

This section discusses the following topics:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–5 provides information about user attribute mappings for trusted source reconciliation.

Table 1–5 User Attributes for Trusted Source Reconciliation

Field on the Xellerate User Resource Object	Target System Attribute	Description
UserID	User ID	User ID
FirstName	First Name	First name
LastName	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

Table 1–5 (Cont.) User Attributes for Trusted Source Reconciliation

Field on the Xellerate User Resource Object	Target System Attribute	Description
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 (Boolean)	If the RSA ClearTrust property type is Date, 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 Boolean, 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. To set the value of any other type of property, use the Property Value field.	Property value as date Property value as Boolean

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following sections provide information about the reconciliation rules for this connector:

- Section 1.7.2.1, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.2.2, "Viewing Reconciliation Rules for Trusted Source Reconciliation in the Design Console"

1.7.2.1 Reconciliation Rule for Trusted Source Reconciliation

The following is the process-matching rule:

Rule name: Trusted Source Recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2:

    User ID attribute on the Xellerate User form

  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

    User ID attribute on the OIM User form

- User ID is the user ID of the account on RSA ClearTrust.

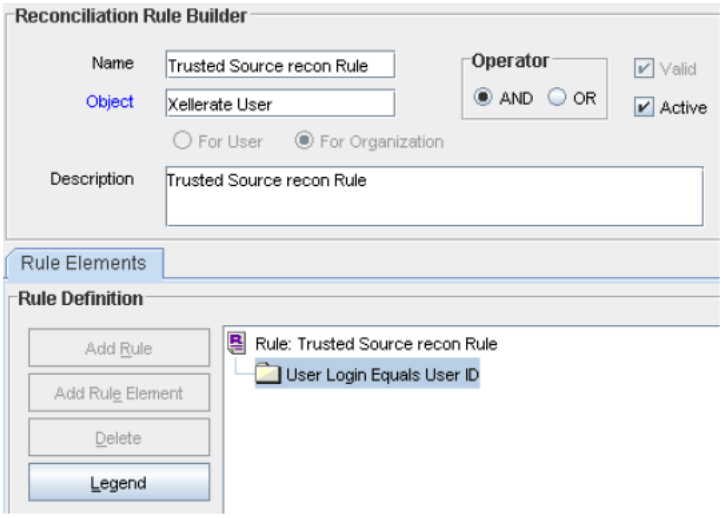
1.7.2.2 Viewing Reconciliation Rules for Trusted Source Reconciliation in the Design Console

After you deploy the connector, you can view the reconciliation rule for reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open **Trusted Source Recon Rule**. Figure 1–4 shows this reconciliation rule.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

The following sections provide information about the reconciliation rules for this connector:

- Section 1.7.3.1, "Reconciliation Action Rules for Trusted Source Reconciliation"
- Section 1.7.3.2, "Viewing Reconciliation Action Rules for Trusted Source Reconciliation in the Design Console"

1.7.3.1 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–6 lists the action rules for reconciliation.

Table 1–6 Action Rules for Trusted Source Reconciliation

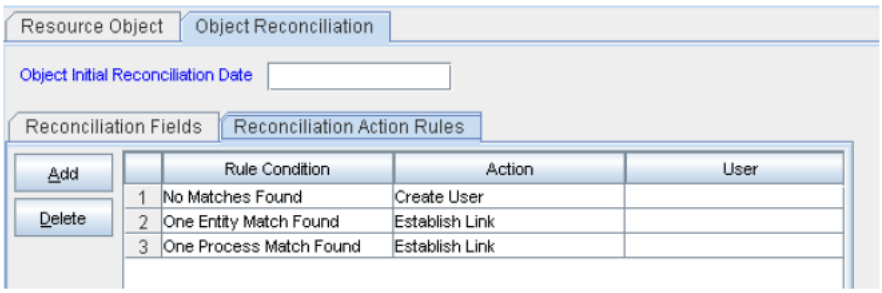
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.7.3.2 Viewing Reconciliation Action Rules for Trusted Source Reconciliation in the Design Console

After you deploy the connector, you can view the reconciliation action rules for reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the reconciliation action rules for reconciliation, then search for and open the **Xellerate User** resource object.
4. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for reconciliation.

Figure 1–5 Action Rules for Trusted Source Reconciliation



1.8 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

See Also: For conceptual information about provisioning, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

This section discusses the following topics:

- Section 1.8.1, "User Attributes for Provisioning"
- Section 1.8.2, "User Provisioning Functions"

1.8.1 User Attributes for Provisioning

Table 1–7 lists the process form fields for which you can specify or modify values during provisioning operations.

Table 1–7 User Attributes for Provisioning

Process Form Field	Target System Attribute	Adapter
UserID	User ID	User ID
FirstName	First Name	First name
LastName	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 visibleto 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 (Date) field	If the RSA ClearTrust property type is Date, then the value for the property can be set only by using the Property Value (Date) field on the RSA ClearTrust User Properties form.
Property Value (Boolean)	Property Value (Boolean) check box	If the RSA ClearTrust property type is Boolean, then the value for the property can be set only by using the Property Value (Boolean) check box on the RSA ClearTrust User Properties form.

Table 1–8 lists special characters that are supported in process form fields.

Table 1–8 Special Characters Supported in Process Form Fields

Name of the Character	Character
ampersand	&
asterisk	*
at sign	@
caret	^
comma	,
dollar sign	$
equal sign	=
exclamation point	!
hyphen	-
left brace	{
left bracket	[
number sign	#
percent sign	%
period	.
plus sign	+
question mark	?
right brace	}
right bracket	]
slash	/
single quotation	'
underscore	_

Note: The following special characters are *not* supported in process form fields:

- Double quotation mark (")
- Left parenthesis (()
- Right parenthesis ())

1.8.2 User Provisioning Functions

Table 1–9 lists the user provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

See Also: For generic information about process tasks and adapters, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

Table 1–9 User Provisioning Functions Supported by the Connector

Process Task	Description	Adapter
Create User	Creates a user	CTCreateUser
Delete User	Deletes a provisioned user	CTDeleteUser
Disable User	Disables an existing user by setting the Account Expires attribute to the current date	CTDisableUser
Enable User	Enables a disabled user by setting the Account Expires attribute to a date that is one year ahead of the current date	CTenableuser
Email Address Updated	Updates the e-mail address	CTModifyUser
Start Date Updated	Updates the start date	CTModifyUser
End Date Updated	Updates the end date	CTModifyUser
Change User Password	Updates the user's password	CTStringTask
First Name Updated	Updates the first name	CTModifyUser
Last Name Updated	Updates the last name	CTModifyUser
Lock User Updated	Updates the locked or unlocked status of the user	CTModifyUser
Change First Name	This adapter is used to copy a change in the first name from the user object form to the process form.	CTStringTask
Change Last Name	This adapter is used to copy a change in the last name from the user object form to the process form.	CTStringTask
Change User Password	This adapter is used to copy a change in the user's password from user object form to the process form.	CTStringTask
Change email	This adapter is used to copy a change in the e-mail address from the user object form to the process form.	CTStringTask
Password Expiration Date Updated	Updates the password expiration date	CTModifyUser
Assign User to Group	Add a user to a group in RSA ClearTrust	CTAddGroup
Delete User from Group	Deletes a user from a group	CTDeleteGroup
Update Group For A User	Removes a user from one group and adds the user to another group	CTUpdateGroup
Add Default Group	Adds a default group to a user	CTAssign Default Group
Add Property to User	Adds 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.	CTUpdateUserProperty
Delete Property to User	Deletes a property value	CTUpdateUserProperty

1.9 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures to perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure that you must perform to test the connector. In addition, this chapter provides instructions for identifying and resolving some commonly encountered errors.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- Section 2.1.1, "Files and Directories That Comprise the Connector"
- Section 2.1.2, "Determining the Release Number of the Connector"
- Section 2.1.3, "Using External Code Files"

2.1.1 Files and Directories That Comprise the Connector

The files and directories on the installation media are listed and described in Table 2–1.

Table 2–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
configuration/	RSACT_CI.xml
DataSets/ModifyResourceClearTrust.xml DataSets/ProvisionResourceClearTrust.xml	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/xliClearTrust.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/xliClearTrustRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

Table 2–1 (Cont.) Files and Directories on the Installation Media

File in the Installation Media Directory	Description
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
tests/config/config.properties	This file contains the properties that are used to connect to the target system for testing purposes.
tests/lib/xliClearTrustTest.jar	This JAR file contains test classes that are used for testing purposes.
xml/RSAClearTrustResourceObject.xml	This XML file contains the definitions of the objects that constitute the connector.
xml/RSAClearTrustXLResourceObject.xml	This file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode. Section 2.3.1, "Configuring Trusted Source Reconciliation" provides instructions.

2.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 or 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

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

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/xliClearTrust.jar

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.

2.1.3 Using External Code Files

Copy the ct_admin_api.jar and ct_runtime_api.jar files from the *CLEARTRUST_INSTALLATION_DIR*/lib directory to the following directories:

- On Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, copy the files to the *OIM_HOME*/xellerate/ThirdParty and *OIM_HOME*/xellerate/ext directories.
- On Oracle Identity Manager release 11.1.1, copy the files to the *OIM_HOME*/server/ThirdParty and *OIM_HOME*/server/ext directories.

2.2 Installation

Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Releases 9.0.1 Through 9.0.3.2"
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

2.2.1 Installing the Connector on Oracle Identity Manager Releases 9.0.1 Through 9.0.3.2

Installing the connector on Oracle Identity Manager releases 9.0.1 through 9.0.3.2 involves performing the following procedures:

- Section 2.2.1.1, "Copying the Connector Files"
- Section 2.2.1.2, "Compiling Adapters"

2.2.1.1 Copying the Connector Files

Table 2–2 lists the files to be copied and the directories to which you must copy them.

Note: The directory paths given in the first column of this table correspond to the location of the connector files on the installation media. See Section 2.1.1, "Files and Directories That Comprise the Connector" for more information about these files.

While installing Oracle Identity Manager in a cluster, 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.

Table 2–2 Connector Files to Be Copied

File in the Installation Media Directory	Destination Directory
lib/xliClearTrust.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xliClearTrustRecon.jar	*OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources **Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
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

2.2.1.2 Compiling Adapters

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: Section 1.8.2, "User Provisioning Functions" 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. In an Oracle Identity Manager cluster, 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.

2.2.2 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

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.*x* or release 11.1.1 involves performing the following procedures:

- Section 2.2.2.1, "Running the Connector Installer"
- Section 2.2.2.2, "Configuring the IT Resource"

2.2.2.1 Running the Connector Installer

To run the Connector Installer:

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

   Note: In an Oracle Identity Manager cluster, perform this step on each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/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 the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, 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 in Step 1.

   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 XML files (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 2.3.1, "Configuring Trusted Source Reconciliation."

   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 Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" 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

Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

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 Section 2.1.1, "Files and Directories That Comprise the Connector."

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, 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 Section 2.1.1, "Files and Directories That Comprise the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.2.2 Configuring the IT Resource

You must specify values for the parameters of the ClearTrust IT resource as follows:

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration section, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `ClearTrust` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–3 describes each parameter.

Table 2–3 IT Resource Parameters

Parameter	Description
CTAdminUserId	Enter the name of the RSA ClearTrust administrator. This is a required parameter.
CTAdminPassword	Enter the password of the RSA ClearTrust administrator. This is a required parameter.

Table 2–3 (Cont.) IT Resource Parameters

Parameter	Description
MachineName or IPAddress	Enter the host name or IP address of the computer on which the RSA ClearTrust Entitlements Server is running. This is a required parameter.
Port	Enter the port number at which the RSA ClearTrust Entitlements Server is listening. This is a required parameter. The default value is `5601`.
SSLMode	Specify whether SSL mode is used to connect to the RSA ClearTrust server. This is a required parameter. You can specify `yes`, `no`, or `SSL_ANON` as the value of this parameter. `SSL_ANON` stands for anonymous SSL, which means that neither the client nor the server needs to present a certificate when establishing a connection. **Note:** It is recommended that you enable SSL to secure communication with the target system.
TimeOut	Specify a timeout value for the connection that is established between Oracle Identity Manager and RSA ClearTrust. This is a required parameter.
Default User Group	Enter the name of the default user group in RSA ClearTrust. This is a required parameter.
CaFileLocation	Enter the location of the CA certificate. This parameter is used only with mutual authentication.
CaPassword	Enter the password for the CA certificate. This parameter is used only with mutual authentication.
KsFileLocation	Enter the location of the keystore file. This parameter is used only with mutual authentication.
KsPassword	Enter the password of the keystore file. This parameter is used only with mutual authentication.
KeyAlias	Enter the key name that is to be used with the keystore file. This parameter is used only with mutual authentication.
PrivatePassword	Enter the password for the private key in the keystore file. This parameter is used only with mutual authentication.
TimeStamp	For the first target resource reconciliation run, this parameter does not hold any value. For subsequent rounds of reconciliation, the time at which the previous reconciliation run was completed is stored in this parameter. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for information about using this parameter to switch from incremental to full reconciliation.
CTAdmin Group	Enter the name of the group to which the RSA ClearTrust administrative user belongs.
CTAdmin Role	Enter the role of the RSA ClearTrust administrative user.
Target Locale: Country	Enter the country code. Default value: `US` **Note:** You must specify the value in uppercase.
Target Locale: Language	Enter the language code. Default value: `en` **Note:** You must specify the value in lowercase.

8. To save the values, click **Update**.

2.3 Postinstallation

This section discusses the following topics:

- Section 2.3.1, "Configuring Trusted Source Reconciliation"
- Section 2.3.2, "Changing to the Required Input Locale"
- Section 2.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.4, "Enabling Logging"
- Section 2.3.5, "Configuring the Oracle Identity Manager System Property for the Date Format"
- Section 2.3.6, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.3.1 Configuring Trusted Source Reconciliation

Note: This section describes an optional procedure. Perform the procedure only if you want to configure the connector for trusted source reconciliation.

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

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. Ensure that the value of the Trusted Source Recon - Resource Object name attribute of the ClearTrust Reconciliation Task scheduled task is Xellerate User. See

Section 3.3.4, "User Reconciliation Scheduled Task" for information about this scheduled task.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 or 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the RSAClearTrustXLResourceObject.xml file, which is in the xml directory on the installation media.
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 specify values for the attributes of the ClearTrust Reconciliation Task scheduled task. This procedure is described in Section 3.4, "Configuring Scheduled Tasks."

2.3.2 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.

2.3.3 Clearing Content Related to Connector Resource Bundles from the Server Cache

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:
   - If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/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:

   For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*:

   OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

   For Oracle Identity Manager release 11.1.1:

   OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

   Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

   For example, the following commands purge Metadata entries from the server cache:

   ```
   PurgeCache.bat MetaData
   ```

   ```
   PurgeCache.sh MetaData
   ```

   - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*:

     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. This exception is different from the one mentioned in Step 1.

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

     OIM_HOME/xellerate/config/xlconfig.xml

   - For Oracle Identity Manager release 11.1.1:

     On Microsoft Windows: `PurgeCache.bat All`

     On UNIX: `PurgeCache.sh All`

     When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.3.4 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform instructions in one of the following sections:

- Section 2.3.4.1, "Enabling Logging on Oracle Identity Manager Releases 9.0.1 through 9.0.3.2 and 9.1.0.x"
- Section 2.3.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.4.1 Enabling Logging on Oracle Identity Manager Releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

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 might 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:

- **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, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <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, 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, log information is written to the following file:

ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

- **Oracle 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, log information is displayed on the server console.

2.3.4.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

Note: In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–4.

Table 2–4 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='rsa-ct-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ADAPTERS.CTINTEGRATION" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="rsa-ct-handler"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–4 lists the supported message type and level combinations.

      Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

      The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='rsa-ct-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ADAPTERS.CTINTEGRATION" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="rsa-ct-handler"/>
     <handler name="console-handler"/>
   </logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the `NOTIFICATION:1` level are recorded in the specified file.

2. Save and close the file.
3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace *FILENAME* with the location and name of the file to which you want to redirect the output.
4. Restart the application server.

2.3.5 Configuring the Oracle Identity Manager System Property for the Date Format

To configure the Oracle Identity Manager system property for the date format:

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 present, then perform the remaining steps of this procedure.
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**.

2.3.6 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple RSA ClearTrust accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.3.6.1, "Copying Predefined Request Datasets"
- Section 2.3.6.2, "Importing Request Datasets into MDS"
- Section 2.3.6.3, "Enabling the Auto Save Form Feature"
- Section 2.3.6.4, "Running the PurgeCache Utility"

2.3.6.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following are the predefined request datasets available in the DataSets directory on the installation media:

- ModifyResourceClearTrust.xml
- ProvisionResourceClearTrust.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\ClearTrust

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.3.6.2 Importing Request Datasets into MDS

All request datasets must be imported into MDS, which can be done by using the MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

   Note: While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.3.6.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\ClearTrust directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     `weblogicImportMetadata.bat`

   - On UNIX

     `weblogicImportMetadata.sh`

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

/custom/connector/*RESOURCE_NAME*

2.3.6.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **CT Users** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.6.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

3

Using the Connector

This chapter is divided into the following sections:

- Section 3.1, "Performing First-Time Reconciliation"
- Section 3.2, "Scheduled Task for Lookup Field Synchronization"
- Section 3.3, "Configuring Reconciliation"
- Section 3.4, "Configuring Scheduled Tasks"
- Section 3.5, "Performing Provisioning Operations"
- Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing user records from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing user records:

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled tasks provided for this operation.

   See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform user reconciliation by running the scheduled task for user reconciliation.

See Section 3.3.4, "User Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, the TimeStamp parameter of the IT resource is automatically set to the time stamp at which the reconciliation run began.

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The Clear Trust Group Lookup Reconciliation Task scheduled task is used for lookup field synchronization. You must specify values for the attributes of this scheduled tasks. Table 3–1 describes the attributes of these scheduled tasks. Section 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 3–1 Attributes of the Scheduled Task for Lookup Field Synchronization

Attribute	Description
`LookupCodeName`	Name of the lookup definition with which values are to be synchronized You can enter either `CTGroups` or `Property Names` as the value of this attribute. See Section 1.5.1, "Lookup Definitions Synchronized with the Target System" for information about these lookup definitions. Default value: `CTGroups`
`Server`	Name of the IT Resource `CT IT Resource`
`ReconMode`	Enter `REFRESH` to completely refresh the existing lookup. Existing values in the lookup definition are deleted and then new values are added. Enter `UPDATE` if you want to update the lookup definition with new values. Existing values in the lookup definition are left untouched. Default value: `REFRESH`

3.3 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:

3.3.1 Full Reconciliation vs. Incremental Reconciliation

The TimeStamp parameter of the IT resource store the time stamp at which a reconciliation run begins. During the next reconciliation run, the scheduled task fetches only target system records that are added or modified after the time stamp stored in the TimeStamp parameter. This is incremental reconciliation.

If you delete the value of the TimeStamp parameter, then full reconciliation is performed when the scheduled task is run. In full reconciliation, all existing target system records are fetched into Oracle Identity Manager.

You can switch from incremental to full reconciliation at any time by deleting the value of the TimeStamp parameter. At the end of the reconciliation run, the TimeStamp parameter again stores the time stamp at which the reconciliation run began. In this way, incremental reconciliation is performed during the next reconciliation run.

3.3.2 Paged Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure paged reconciliation to avoid these problems.

To configure paged reconciliation, you must specify a value for the Paging Range attribute of the user reconciliation scheduled task while performing the procedure described in Section 3.3.4, "User Reconciliation Scheduled Task."

3.3.3 Specifying the Attributes That Must Be Used During Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to specify a subset of the available target system attribute mappings for reconciliation.

If you want to specify the subset of target system attributes that must be reconciled:

1. In the Design Console, open the Lookup.CTReconciliation.FieldMap lookup definition.
2. For attributes that must be reconciled from the target system, retain or add entries in the lookup definition.

   For each target system attribute that you want to add, enter the name of the attribute in both the Code Key and Decode columns. The following table shows the default entries in this lookup definition:

Code Key	Decode
userId	userId **Note:** Do not remove this row from the lookup definition.
lastName	lastName **Note:** Do not remove this row from the lookup definition.
endDate	endDate

3. Save and close the lookup definition.
4. Open the ClearTrust Reconciliation Task scheduled task.
5. Set `true` as the value of the UseReconFieldMap atribute.
6. Ensure that the CTReconciliationFields attribute is set to Lookup.CTReconciliation.FieldMap.

> **Note:** If you create and use a different lookup definition for storing these attribute names, then set the value of that lookup definition as the value of the CTReconciliationFields attribute.

7. Save and close the scheduled task.

From each subsequent run of the ClearTrust Reconciliation Task scheduled task, only attributes specified in the Lookup.CTReconciliation.FieldMap are reconciled.

3.3.4 User Reconciliation Scheduled Task

The ClearTrust Reconciliation Task scheduled task is used for reconciling user data. Table 3–1 describes the attributes of this scheduled task.

Table 3–2 Attributes of the ClearTrust Reconciliation Task Scheduled Task

Attribute	Description
`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: `Xellerate User` Specify `false` (in lowercase) if you do not 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`

Table 3–2 (Cont.) Attributes of the ClearTrust Reconciliation Task Scheduled Task

Attribute	Description
UseReconFieldMap	If this attribute is set to true, then only user attributes mapped in the lookup definition specified by the CTReconciliationFields attribute are fetched from the target system for reconciliation. The CTReconciliationFields attribute is described later in this table. If the UseReconFieldMap attribute is set to false, then all the attributes for which there are reconciliation field mappings in the resource object are fetched for reconciliation. Default value: false
CTReconciliationFields	Name of the lookup definition that stores the reconciliation field data used in customized reconciliation Lookup.CTReconciliation.FieldMap
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 Section 2.3.5, "Configuring the Oracle Identity Manager System Property for the Date Format." yyyy/MM/dd hh:mm:ss z

3.4 Configuring Scheduled Tasks

Table 3–3 lists the scheduled tasks that form part of the connector.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Clear Trust Group Lookup Reconciliation Task	This scheduled task is used to synchronize the values of the group lookup field between Oracle Identity Manager and the target system. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
ClearTrust Reconciliation Task	This scheduled task is used for user reconciliation. See Section 3.3.4, "User Reconciliation Scheduled Task" for information about this scheduled task.

To configure these scheduled tasks, perform the procedure described in one of the following sections depending on the Oracle Identity Manager release that you are using:

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Releases 9.0.1 Through 9.0.3.2"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x and 11.1.1"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Releases 9.0.1 Through 9.0.3.2

To configure a scheduled task Oracle Identity Manager releases 9.0.1 through 9.0.3.2:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder, and then select **Task Scheduler**.
3. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
4. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the FAILED status to the task.

5. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
6. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
7. 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.
8. Provide values for the attributes of the scheduled task.
9. 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.

Stopping Reconciliation

Suppose the user reconciliation scheduled task for the connector is running and user records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 3 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box.
3. Click **Save**.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x and 11.1.1

This section describes the procedure to configure scheduled tasks on Oracle Identity Manager release 9.1.0.*x* and 11.1.1. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
     b. In the search results table, click the edit icon in the Edit column for the scheduled task.
     c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.
   - If you are using Oracle Identity Manager release 11.1.1, then:

a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task. To do so:

a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

– **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

– **Max Retries:** Enter an integer value in this 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. The default value is 1.

– **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

– **Frequency:** Specify the frequency at which you want the task to run.

b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

– **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

– **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task. To do so:

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- Attributes of the scheduled task are discussed in Section 3.3.4, "User Reconciliation Scheduled Task."

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

     Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

   - If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

     Note: The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

Stopping Reconciliation

If you want to stop a scheduled task while it is running, open the scheduled task in the Design Console and then select the **Stop Execution** check box.

3.5 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

See Also: For conceptual information about the types of provisioning, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning"
- Section 3.5.2, "Request-Based Provisioning"

3.5.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager releases 9.0.1 through 9.0.3.2 or 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

b. On the Resource Profile page, click **Provision New Resource**.

- If you are using Oracle Identity Manager release 11.1.1, then:

  a. On the user details page, click the **Resources** tab.

  b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **ClearTrust** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for ClearTrust User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 5: Provide Process Data for ClearTrust Property Updation Details page, if required, search for and select a group for the user on the target system and then click **Continue**. If you do not want to specify a group, then directly click **Continue**.
9. On the Step 5: Provide Process Data for ClearTrust User Group Membership Details page, if required, search for and select a group for the user on the target system and then click **Continue**. If you do not want to specify a group, then directly click **Continue**.
10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
11. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

    - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:

      a. Close the window displaying the "Provisioning has been initiated" message.

      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

Note: The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

Note: The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 3.5.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.5.2.2, "Approver's Role in Request-Based Provisioning"

3.5.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account..

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **Clear Trust**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

Note: It is assumed that you have performed the procedure described in Section 2.3.6, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **CT Users** process definition.
   c. Deselect the **Auto Save Form** check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **ClearTrust** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.

b. Search for and open the **CT User** process definition.

c. Select the **Auto Save Form** check box.

d. Click the Save icon.

3. If you want to enable end users to raise requests for themselves, then:

a. Expand **Resource Management**, and then double-click **Resource Objects**.

b. Search for and open the **ClearTrust** resource object.

c. Select the **Self Request Allowed** check box.

d. Click the Save icon.

4

Extending the Functionality of the Connector

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

- Section 4.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding New Attributes for Trusted Source Reconciliation"

4.1 Adding New Attributes for Target Resource Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add new attributes for target resource reconciliation.

You must ensure the new attributes that you add for reconciliation contain data in string-format only. Binary attributes must not be introduced into Oracle Identity Manager natively.

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

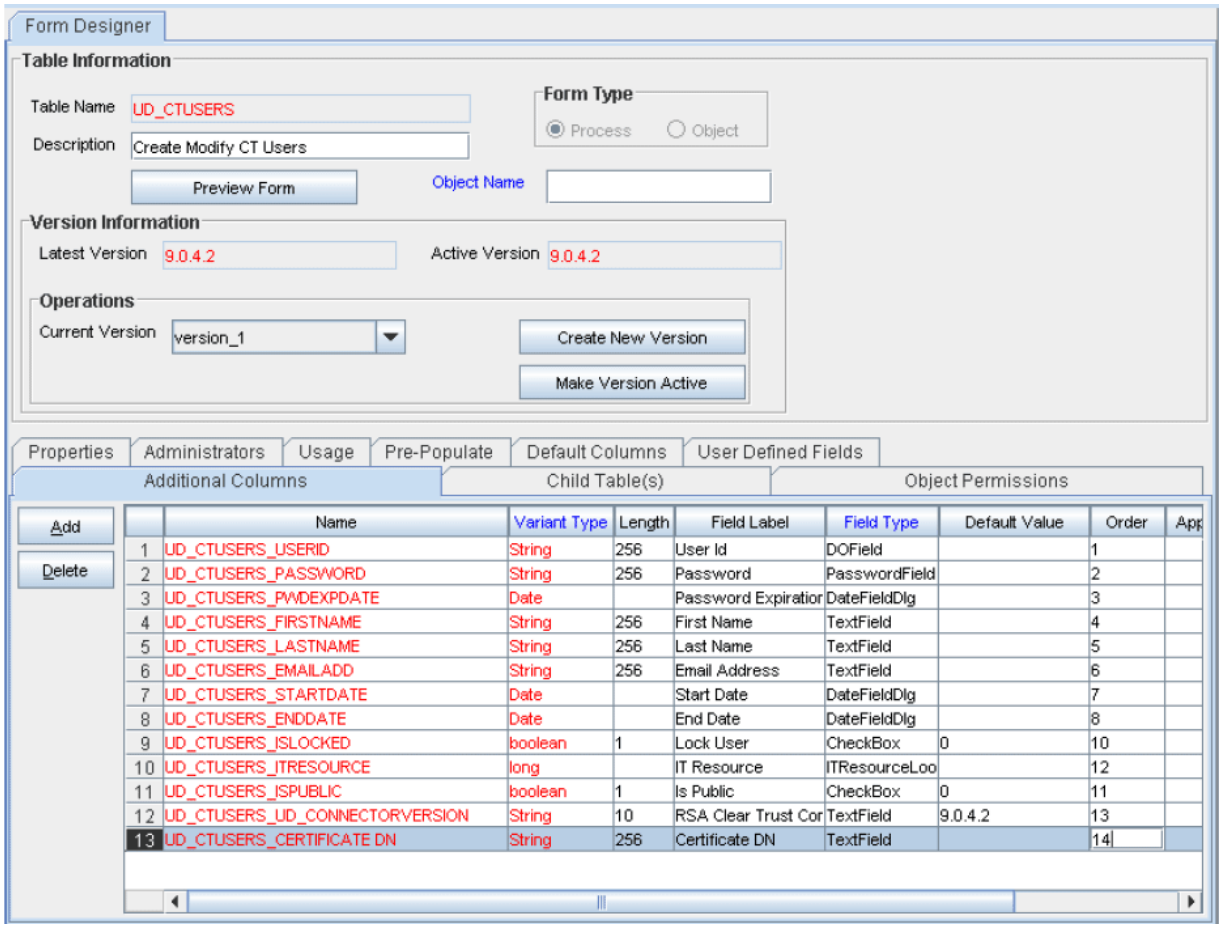
To add a new attribute for target resource reconciliation, perform the following procedure:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the **CT Users** process form.
   d. Click **Create New Version**.
   e. In the **Label** field, enter the version name. For example, `version_1`.
   f. Click the **Save** icon.
   g. Select the current version created in Step e from the **Current Version** list.
   h. Click **Add** to create an attribute and provide the values for that attribute.

      For example, if you are adding the Certificate DN attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	Certificate DN
Variant Type	String
Length	100
Field Label	Certificate DN
Field Type	TextField
Order	20

The following screenshot shows this form:



i. Click the **Save** icon.

j. Click **Make Version Active**.

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

   a. Expand **Resource Management.**

   b. Double-click **Resource Objects**.

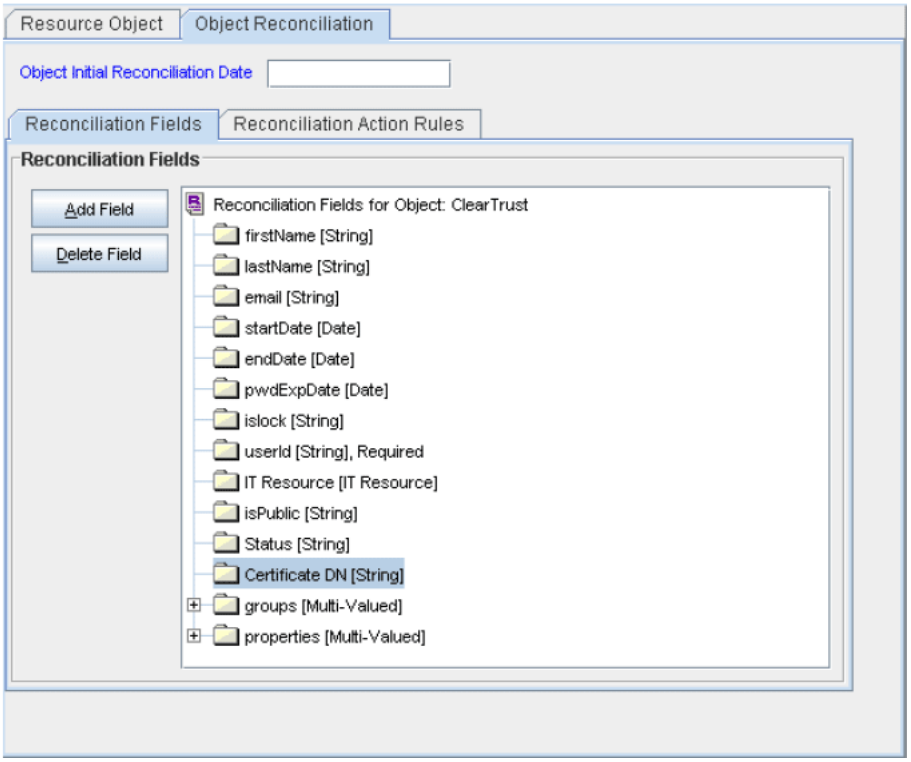
   c. Search for and open the **ClearTrust** resource object.

   d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

Field Name: `Certificate DN`

Field Type: `String`

The following screenshot shows this form:



e. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

f. Click the **Save** icon.

4. Create a reconciliation field mapping for the new attribute in the process definition form as follows:

a. Expand **Process Management.**

b. Double-click **Process Definition**.

c. Search for and open the **CT Users** process definition.

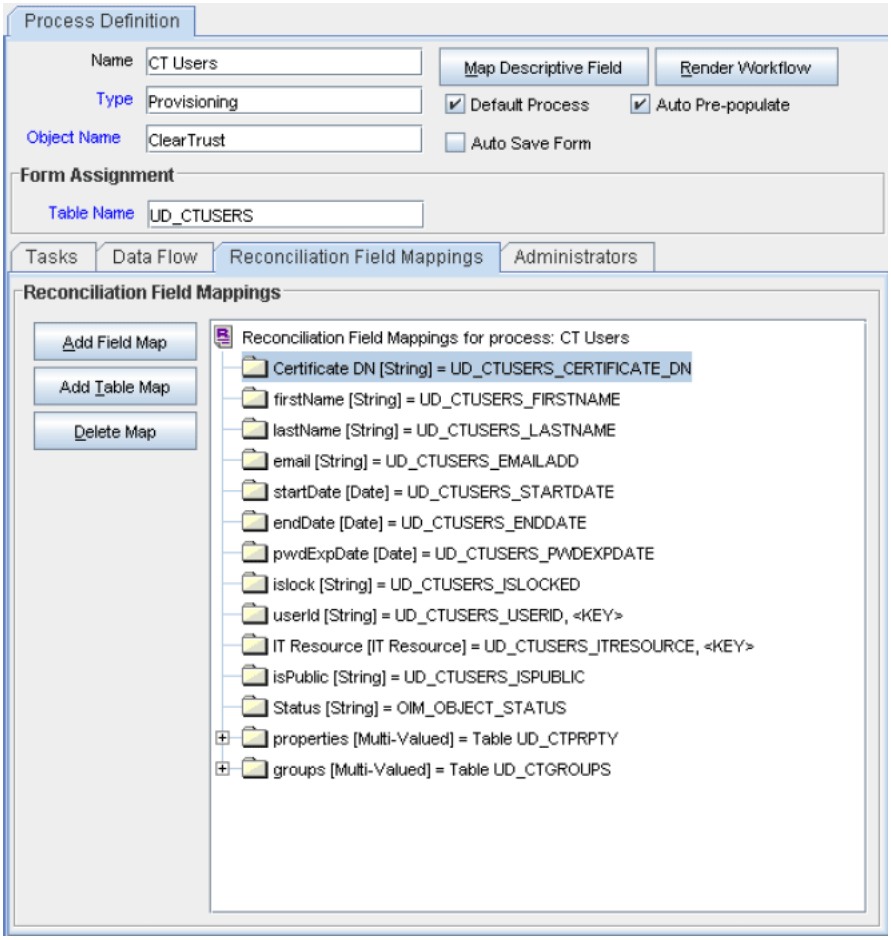
d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: `Certificate DN`

Field Type: `String`

Process Data Field: `Certificate DN`

The following screenshot shows this form:



e. Click the **Save** icon.

5. Create an entry for the attribute in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

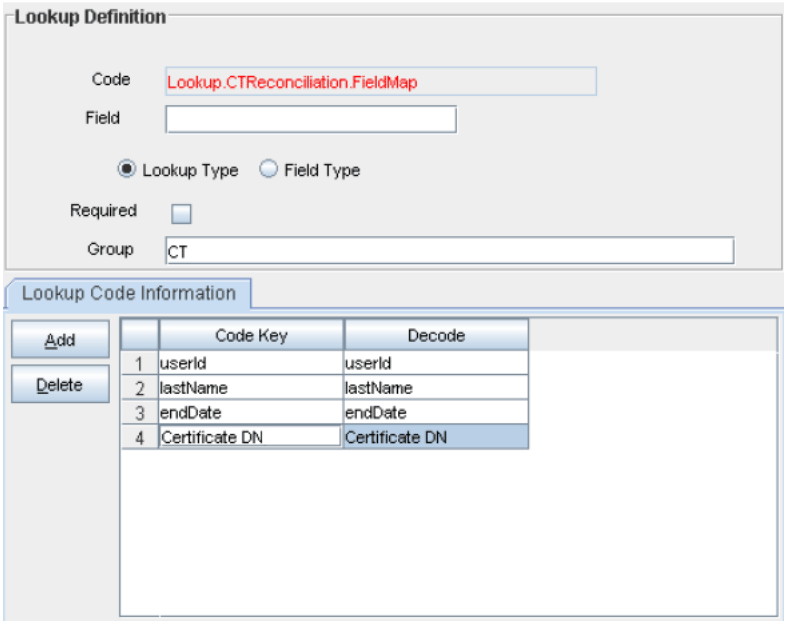
   b. Double-click **Lookup Definition**.

   c. Search for and open the **Lookup.CTReconciliation.FieldMap** lookup definition.

   d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

   For example, enter `organization` in the **Code Key** field and then enter `o` in the **Decode** field.

   The following screenshot shows this form:



e. Click the **Save** icon.

4.2 Adding New Attributes for Trusted Source Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add new attributes for trusted source reconciliation.

You must ensure that the new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Section 1.7.1, "User Attributes for Trusted Source Reconciliation" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for trusted resource reconciliation.

To add a new attribute for trusted source reconciliation:

See Also: One of the following guides for detailed instructions on performing the steps in this section:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

  Oracle Identity Manager Design Console Guide

- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the Users process form as follows:
   a. Expand **Administration**.

b. Double-click **User Defined Field Definition.**

c. Search for and open the **Users** process form.

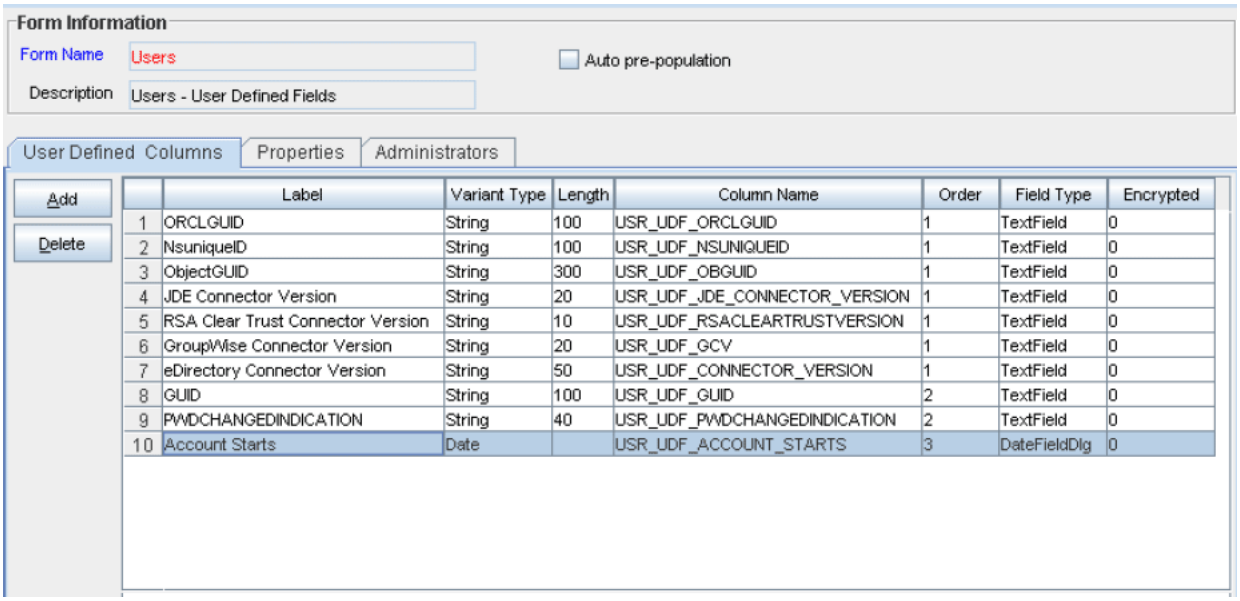
d. Click **Add**.

e. In the User Defined Fields dialog box, enter the details of the attribute.

For example, if you are adding the Account Starts attribute, then enter the following details in the User Defined Fields dialog box:

- In the **Label** field, enter `Account Starts`.
- From the Data Type list, select **Date**.
- From the Field Type list, select **DateField with Dialog**.
- In the **Column Name** field, enter `USR_UDF_ACCOUNT_STARTS`.

The following screenshot shows this form:



	Label	Variant Type	Length	Column Name	Order	Field Type	Encrypted
1	ORCLGUID	String	100	USR_UDF_ORCLGUID	1	TextField	0
2	NsuniqueID	String	100	USR_UDF_NSUNIQUEID	1	TextField	0
3	ObjectGUID	String	300	USR_UDF_OBGUID	1	TextField	0
4	JDE Connector Version	String	20	USR_UDF_JDE_CONNECTOR_VERSION	1	TextField	0
5	RSA Clear Trust Connector Version	String	10	USR_UDF_RSACLEARTRUSTVERSION	1	TextField	0
6	GroupWise Connector Version	String	20	USR_UDF_GCV	1	TextField	0
7	eDirectory Connector Version	String	50	USR_UDF_CONNECTOR_VERSION	1	TextField	0
8	GUID	String	100	USR_UDF_GUID	2	TextField	0
9	PWDCHANGEDINDICATION	String	40	USR_UDF_PWDCHANGEDINDICATION	2	TextField	0
10	Account Starts	Date		USR_UDF_ACCOUNT_STARTS	3	DateFieldDlg	0

f. Click **Save**.

3. Add the new attribute to the list of reconciliation fields in the resource object as follows:

a. Expand **Resource Management**.

b. Double-click **Resource Objects.**

c. Search for and open the **Xellerate User** resource object.

d. On the Object Reconciliation tab, click **Add Field**.

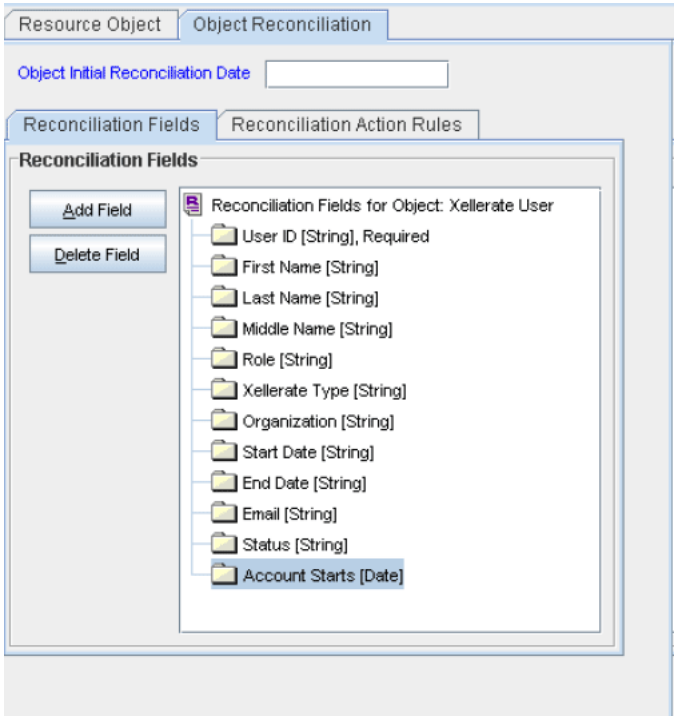
e. Enter the details of the attribute.

For example, enter `Account Starts` in the **Field Name** field and select **Date** from the Field Type list.

f. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

g. Click **Save**.

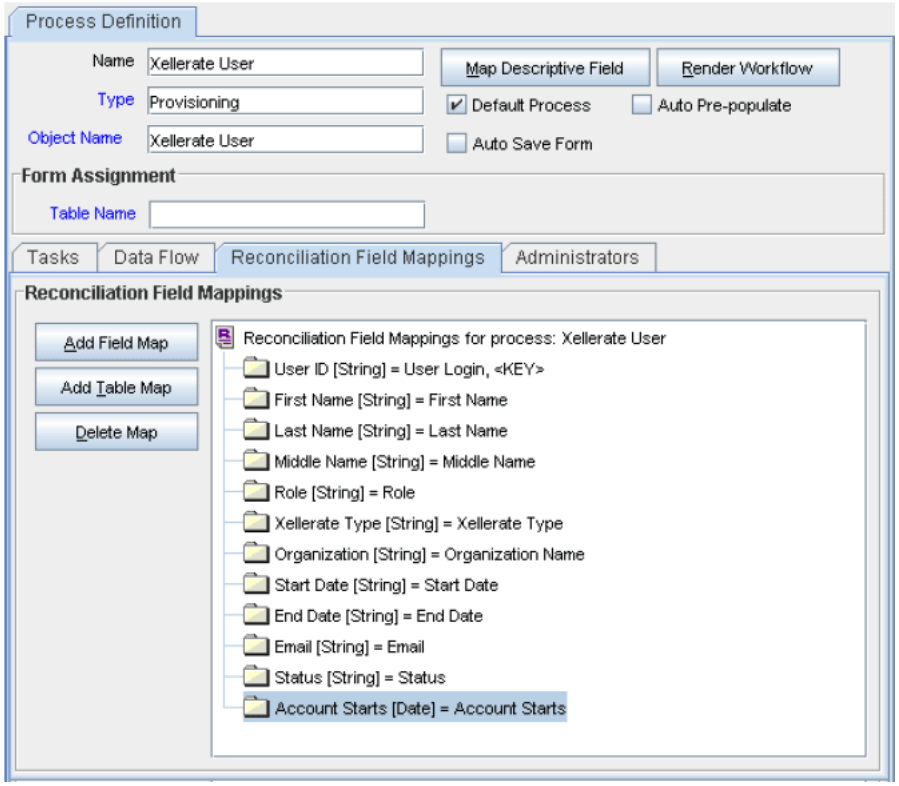
The following screenshot shows the Account Starts field added to the resource object:



4. Create a reconciliation field mapping for the new attribute in the process definition as follows:
   a. Expand **Process Management**.
   b. Double-click **Process Definition**.
   c. Search for and open the **Xellerate User** process definition.
   d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**.
   e. In the Field Name field, select the value for the attribute that you want to add.

      For example, select `Account Starts=Account Starts`.

      The following screenshot shows this form:



f. Click **Save**.

5. Create an entry for the attribute in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

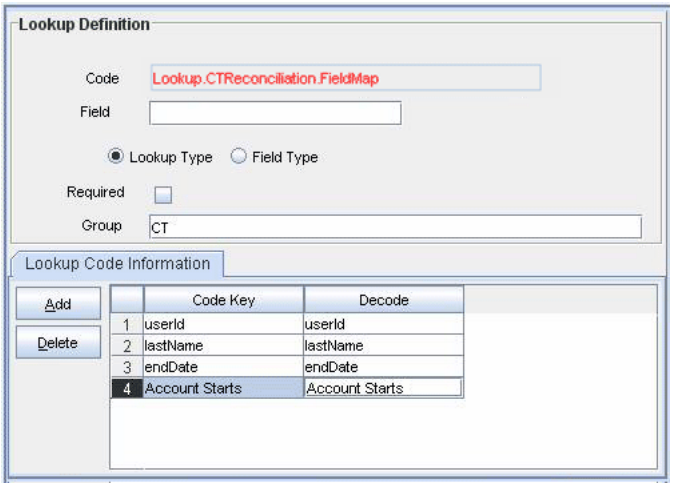
   b. Double-click **Lookup Definition.**

   c. Search for and open the **Lookup.CTReconciliation.FieldMap** lookup definition.

   d. Click **Add** and enter the Code Key and Decode values for the attribute. The Code Key value must be the name of the attribute on the target system, which you determined at the start of this procedure. The Decode value is the name that you provide for the reconciliation field in Step 3.e.

      For example, enter `Account Starts` in the **Code Key** field and then enter `Account Starts` in the **Decode** field.

      The following screenshot shows this form:


Lookup Definition
Code
Lookup.CTReconciliation.FieldMap
Field
Lookup Type
Field Type
Required
Group
CT
Lookup Code Information
Add
Delete
Code Key
Decode
1 userId userId
2 lastName lastName
3 endDate endDate
4 Account Starts Account Starts

e. Click **Save**.

5

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:

5.1 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. Copy the contents of the tests directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/ClearTrust/tests/config directory.
2. Modify the `CLASSPATH` environment variable to include the following:
   - For Oracle Identity Manager releases 9.0.1 through 9.0.3.2 and 9.1.0.*x*:

     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

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/JavaTasks/xliClearTrust.jar
     OIM_HOME/server/XLIntegrations/ClearTrust/tests/lib/xliClearTrustTest.jar
     OIM_HOME/server/ThirdParty/ct_admin_api.jar
     OIM_HOME/server/ThirdParty/ct_runtime_api.jar
     OIM_HOME/server/ext/log4j-1.2.8.jar
     OIM_HOME/server/lib/xlLogger.jar
     OIM_HOME/server/lib/xlUtils.jar
     OIM_HOME/server/lib/xlVO.jar
     OIM_HOME/server/client/oimclient.jar

3. Use the information in the following table to modify the default attributes given in the `config.properties` file. This file is in the `XLIntegrations/ClearTrust/tests/config` directory in the Oracle Identity Manager home 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	SL_ANON
timeout	Timeout interval (in milliseconds) for connecting to the RSA ClearTrust Entitlements Server	10000
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 2-12.	DEBUG

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

```
java com.thortech.xl.integration.ct.tests.CTConnectTest
FULL_PATH_OF_CONFIG.PROPERTIES_FILE ctadmin ctpassword
```

For example:

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

5. 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
```

5.2 Troubleshooting

Table 5–1 lists solutions to some commonly encountered errors associated with the connector.

Table 5–1 Commonly Encountered Errors

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 ext directory on the Oracle Identity Manager host computer.
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.

Table 5–1 (Cont.) Commonly Encountered Errors

Problem	Solution
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.

6

Known Issues

The following is a known issue associated with this release of the connector:

- **Bug 7207232**

  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.

Index

R

S

T

V

X