Oracle® Identity Manager

Connector Guide for Sun Java System Directory

Release 9.0.4

E10175-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for Sun Java System Directory, Release 9.0.4

E10175-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Vijaykarthik Sathiyamurthy, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for Sun Java System Directory provides information about integrating Oracle Identity Manager with Sun Java System Directory.

Note: Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for Sun Java System Directory.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

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

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`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 Sun Java System Directory?

This chapter provides an overview of the updates made to the software and documentation for the Sun Java System Directory connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 release

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

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

Software Updates

This section discusses the following updates made to this release of the connector software:

Enabling Provisioning of Users in Organizations and Organizational Units

Functionality for enabling provisioning of users in organizations and organizational units is discussed in the following sections:

- Enabling Provisioning of Users in Organizations and Organizational Units on page 3-10

Provisioning of Organizational Units, Groups, and Roles

Functionality for provisioning of organizational units, groups, and roles is discussed in the following section:

- Provisioning Organizational Units, Groups, and Roles on page 3-11

  The `ldapOrgUnitObjectClass` and `ldapGroupObjectClass` attributes have been added to the list of Oracle Identity Manager attribute names.

Reconciliation of Organizations, Organizational Units, Groups, and Roles

In this release of the connector, while configuring the lookup fields reconciliation scheduled task, you can specify the entity for which you want to configure reconciliation: groups, roles, or organizations and organizational units. The "Lookup Fields Reconciliation Scheduled Task" section on page 3-6, describes the attributes that you use to specify the entity to be configured for reconciliation.

Partial Reconciliation

The `CustomizedReconQuery` parameter has been added to the IT resource definition. You can use this parameter to customize the query that the reconciliation module uses to determine the records to be retrieved from the target system. The `CustomizedReconQuery` parameter is explained in the following sections:

- Defining IT Resources on page 2-6
- Partial Reconciliation on page 3-1
- Testing Partial Reconciliation on page 4-2

Batched Reconciliation

In this release of the connector, the `StartRecord`, `BatchSize`, and `NumberofBatches` attributes have been added to the reconciliation scheduled task definition. By specifying values for these attributes, you can reconcile user records in batches. The scheduled task attributes are discussed in the following sections:

- User Reconciliation Scheduled Task on page 3-7
- Batched Reconciliation on page 3-3
- Testing Batched Reconciliation on page 4-3

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-3, you can configure the generation of log information that is specific to the target system.

Changes in the Supported Target Systems List

In the "Step 1: Verifying Deployment Requirements" section on page 2-1, the information on supported target system host platform has been modified. This release of the connector is not dependent on any target system host platform.

Stopping Reconciliation

This release of the connector supports the stopping of reconciliation. This feature is discussed in the following section:

- Stopping Reconciliation on page 3-8

Documentation-Specific Updates

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

- In the "Reconciled Xellerate User Fields" section on page 1-2, the Password field has been removed from the list of fields that are reconciled during trusted source reconciliation.
- Instructions in the "Determining the Release Number of the Connector" section on page 1-6 have been revised.

- Some of the content from Chapter 2 of the earlier release of this guide has been moved to Chapter 3.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for Sun Java System Directory is used to integrate Oracle Identity Manager with Sun Java System Directory.

> **Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

> **Note:** At some places in this guide, Sun Java System Directory has been referred to as the *target system.*

Reconciliation Module

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

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

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the fields for groups, roles, organizations, and organizational units.

User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

Reconciled Resource Object Fields

The following target system fields are reconciled:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Timezone
- Communication Language
- Title
- Organizational Unit
- Group
- Role

Reconciled Xellerate User Fields

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

- User ID
- First Name
- Last Name
- Employee Type
- Timezone
- User Type
- Organization
- Email

Provisioning Module

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

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

For this target system, the following fields are provisioned:

- User ID
- First Name
- Last Name
- Middle Name
- Department
- Location
- Telephone
- Email
- Communication Language
- Title
- Organizational Unit
- Group
- Role

Supported Functionality

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

Function	Type	Description
Create User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Enable User	Provisioning	Enables a user
Disable User	Provisioning	Disables a user
Move User	Provisioning	Moves a user from one container to another
Password Updated	Provisioning	Updates the password of a user
First Name Updated	Provisioning	Updates the first name of a user
Last Name Updated	Provisioning	Updates the last name of a user
Department Updated	Provisioning	Updates the department of a user
Email ID Updated	Provisioning	Updates the e-mail address of a user
Location Updated	Provisioning	Updates the location of a user
Middle Name Updated	Provisioning	Updates the middle name of a user
Communication Language Updated	Provisioning	Updates the communication language preference of a user
Telephone Updated	Provisioning	Updates the telephone number of a user
Title Updated	Provisioning	Updates the title of the user

Function	Type	Description
Organization DN Updated	Provisioning	Updates the organization DN of a user
Add User to Group	Provisioning	Adds a user to a group
Remove User from Group	Provisioning	Removes a user from a group
Add User to Role	Provisioning	Adds a user to a role
Remove User from Role	Provisioning	Removes a user from a role
Create OU	Provisioning	Creates an organizational unit
Change OU Name	Provisioning	Changes OU name
Delete OU	Provisioning	Deletes organizational unit
Move OU	Provisioning	Moves organization sub unit to another parent organizational unit
Create iPlanet Group	Provisioning	Creates an iPlanet group
Delete iPlanet Group	Provisioning	Deletes an iPlanet group
New Group Name Updated	Provisioning	Changes the group name
Create iPlanet Role	Provisioning	Creates iPlanet role
Delete iPlanet Role	Provisioning	Deletes iPlanet role
New Role Name Updated	Provisioning	Changes the role name
Reconciliation Delete Received	Reconciliation	Deletes a user from Oracle Identity Manager if the user is deleted from Sun Java System Directory
Reconciliation Insert Received	Reconciliation	Inserts a user in Oracle Identity Manager
Reconciliation Update Received	Reconciliation	Updates user attributes, such as the first name and last name, in Oracle Identity Manager
Create User	Reconciliation	Creates a user in Oracle Identity Manager
Delete User	Reconciliation	Deletes a user is Oracle Identity Manager
Enable User	Reconciliation	Enables a user in Oracle Identity Manager
Disable User	Reconciliation	Disables a user in Oracle Identity Manager
Move User	Reconciliation	Moves a user from one container to another in Oracle Identity Manager
Add User to Group	Reconciliation	Adds a user to a group in Oracle Identity Manager
Remove User from Group	Reconciliation	Removes a user from a group in Oracle Identity Manager
Assign Role to User	Reconciliation	Assigns a role to a user in Oracle Identity Manager
Remove Assigned Role from User	Reconciliation	Removes a role from a user in Oracle Identity Manager

See Also: Appendix A, "Attribute Mappings Between Oracle Identity Manager and Sun Java System Directory"

Multilanguage Support

The connector supports the following languages:

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

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

Files and Directories That Comprise the Connector

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

`Directory Servers/Sun Java System Directory Server`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib/xliIPlanet.jar`	This JAR file contains the class files required for provisioning and reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
`troubleshooting/TroubleShootingUtilityIPlanet.class`	This is the standalone class that interacts with the target system. This is the class that has the code required to run the test cases.
`troubleshooting/log.properties`	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
`troubleshooting/TroubleShootIPlanet.properties`	This file contains the connection details that are required to connect to the target system and user details. It also contains details about the commands to be run.

File in the Installation Media Directory	Description
xml/iPlanetResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Custom process form ■ Process task and rule-generator adapters (along with their mappings) ■ Resource object ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
xml/iPlanetXLResourceObject.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

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

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

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector before you deploy it:

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

   Directory Servers/Sun Java System Directory Server/lib

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

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

Note: If you maintain a copy of the xliIPlanet.jar file after deployment, then you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files and External Code Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Importing the Connector XML File
- Step 5: Configuring SSL

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	Sun ONE Directory Server 5.2
Target system user account	Sun Java System Directory user account to which the Read, Write, Add, Delete, and Search permissions have been assigned You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-6. If you try to perform an operation for which the required permission has not been assigned to the user account, then the "Insufficient Privileges" message is displayed.

Step 2: Copying the Connector Files and External Code Files

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

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

`Directory Servers/Sun Java System Directory Server`

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

Files in the Installation Media Directory	Destination Directory
`lib/xliIPlanet.jar`	*OIM_home*`/xellerate/JavaTasks`
Files in the `resources` directory	*OIM_home*`/xellerate/connectorResources`
Files in the `troubleshooting` directory	*OIM_home*`/xellerate/troubleshooting`
Files in the `xml` directory	*OIM_home*`/xellerate/iPlanet/xml`

To copy the external code files into the required directories:

1. Log on the Sun Web site at

   `http://java.sun.com/products/jndi/downloads/index.html`
2. Click the **Download JNDI 1.2.1 & More** button.
3. From the table on the page that is displayed, select the **LDAP Service Provider 1.2.4** check box and download the `ldap-1_2_4.zip` file.
4. Extract the `ldap.jar` and `ldapbp.jar` files from the `ldap-1_2_4.zip` file.
5. Copy the `ldap.jar` and `ldapbp.jar` files into the *OIM_home*`/xellerate/JavaTasks` directory on the Oracle Identity Manager server.

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

Step 3: Configuring the Oracle Identity Manager Server

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

Configuring the Oracle Identity Manager server involves the following procedures:

Note: In a clustered environment, you must perform this step on each node of the cluster.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache

- Enabling Logging

Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

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

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

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

   Note: You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:

   `OIM_home``/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

   `OIM_home``/xellerate/config/xlConfig.xml`

Enabling Logging

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

- `ALL`

This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SJSDS=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.XL_INTG.SJSDS=INFO
     ```

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

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

- **IBM WebSphere**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.SJSDS=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.XL_INTG.SJSDS=INFO
```

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

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

- **JBoss Application Server**

  To enable logging:

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

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

<category name="XL_INTG.SJSDS">
   <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="XL_INTG.SJSDS">
   <priority value="INFO"/>
</category>
```

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

  JBoss_home/server/default/log/server.log

- **OC4J**

  To enable logging:

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

```
log4j.logger.XELLERATE=log_level
log4j.logger.XL_INTG.SJSDS=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.XL_INTG.SJSDS=INFO
```

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

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

Step 4: Importing the Connector XML File

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

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `iPlanetResourceObject.xml` file, which is in the *`OIM_home`*`/xellerate/iPlanet/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next.** The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `iPlanet User` IT resource is displayed.
8. Specify values for the parameters of the `iPlanet User` IT resource. Refer to the table in the "Defining IT Resources" section on page 2-6 information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the `LDAP Server` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

11. Click **View Selections.**

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

After you import the connector XML file, proceed to the "Step 5: Configuring SSL" section on page 2-7.

Defining IT Resources

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

Parameter	Description
`Admin Id`	DN value of the user who has administrator rights on Sun Java System Directory The default value is `uid=admin,ou=administrators,ou=topologymanagement,o=netscaperootAdmin`
`Admin Password`	Password of the user who has administrator rights on Sun Java System Directory
`Server Address`	IP address of the target Sun Java System Directory server

Parameter	Description
Port	Port number to connect to the target Sun Java System Directory server The default value is 389. This parameter is mentioned in the "Step 5: Configuring SSL" section on page 2-7.
Root DN	Base DN where all the user operations are to be carried out The value can be o=xyz
SSL	Specifies whether or not an SSL connection is used for communication between Oracle Identity Manager and the target Sun Java System Directory server The value can be true or false. This parameter is mentioned in the "Step 5: Configuring SSL" section on page 2-7. **Note:** It is recommended that you enable SSL to secure communication with the target system.
Last Recon TimeStamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. Do not change the default value of this parameter.
Prov Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning The default value of this parameter is AttrName.Prov.Map.iPlanet
Recon Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for reconciliation The default value of this parameter is AttrName.Recon.Map.iPlanet
Use XL Org Structure	If set to true, then the Oracle Identity Manager Organization structure is used during provisioning and reconciliation. If set to false, then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation.
CustomizedReconQuery	Query condition on which reconciliation must be based If you specify a query condition for this parameter, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then do not specify a value for this parameter. The query can be composed with the AND (&) and OR (|) logical operators. Sample value: givenname=John For more information about this parameter, refer to the "Partial Reconciliation" section on page 3-1.

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

Step 5: Configuring SSL

Note: This is an optional step of the deployment procedure.

To enable SSL communication between Oracle Identity Manager and Sun Java System Directory:

1. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager) `cacerts` keystore as follows:

   ```
   keytool -import -alias alias_name -file
   certificate_file_name_with_complete_path -keystore
   java_home/jre/lib/security/cacerts
   ```

   Here, *java_home* is the directory in which JDK is installed.

2. Restart the Oracle Identity Manager server.
3. In the `iPlanet User` IT Resource:
   - Set the `SSL` parameter value to `true`.
   - Set the `Port` parameter value to the SSL port number. Typically, this number is 636.

3

Configuring the Connector

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

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

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

Configuring Reconciliation

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

- Partial Reconciliation
- Batched Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

Partial Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying values for the `CustomizedReconQuery` and `Last Recon TimeStamp` IT resource parameters while performing the procedure described in the "Defining IT Resources" section on page 2-6.

The following table lists the Sun Java System Directory attributes, and the corresponding Oracle Identity Manager attributes, that you can use to build the query

condition. You specify this query condition as the value of the `CustomizedReconQuery` parameter.

Sun Java System Directory Attribute	Oracle Identity Manager Attribute
uid	User ID
givenname	First Name
sn	Last Name
mail	Email
preferredlanguage	Communication Language
initials	Middle Name
departmentnumber	Department
l	Location
title	Title

The following are sample query conditions:

- `givenname=John&sn=Doe`

  With this query condition, records of users whose first name is `John` and last name is `Doe` are reconciled.

- `givenname=John&sn=Doe|departmentnumber=033`

  With this query condition, records of users who meet either of the following conditions are reconciled:

  – The user's first name is `John` and last name is `Doe`.

  – The user belongs to the department that has the number `033`.

If you do not specify values for the `CustomizedReconQuery` parameter, then all the records in the target system are compared with existing Oracle Identity Manager records during reconciliation.

Along with the `CustomizedReconQuery` parameter, if you also specify a value for the `Last Recon TimeStamp` parameter, then only the records that meet *both* of the following criteria are reconciled:

- Records that meet the matching criteria specified by the `CustomizedReconQuery` parameter
- Records that are added or updated after the time-stamp value specified by the `Last Recon TimeStamp` parameter

> **Note:** As mentioned in the "Defining IT Resources" section on page 2-6, the value of the `Last Recon TimeStamp` parameter is automatically updated by Oracle Identity Manager at the end of every reconciliation run. It is recommended that you do not change the value of this parameter.

The following are guidelines to be followed while specifying a value for the `CustomizedReconQuery` parameter:

- For the Sun Java System Directory attributes, you must use the same case (uppercase or lowercase) as given in the table shown earlier in this section. This is because the attribute names are case-sensitive.
- You must not include unnecessary blank spaces between operators and values in the query condition.

  A query condition with spaces separating values and operators would yield different results as compared to a query condition that does not contain spaces between values and operators. For example, the output of the following query conditions would be different:

  ```
  givenname=John&sn=Doe
  ```

  ```
  givenname= John&sn= Doe
  ```

  In the second query condition, the reconciliation engine would look for first name and last name values that contain a space at the start.
- You must not include special characters other than the equal sign (=), ampersand (&), and vertical bar (|) in the query condition.

  Note: An exception is thrown if you include special characters other than the equal sign (=), ampersand (&), and vertical bar (|).

As mentioned earlier in this section, you specify values for the `CustomizedReconQuery` and `Last Recon TimeStamp` parameters while performing the procedure described in the "Defining IT Resources" section on page 2-6.

See Also: The "Testing Partial Reconciliation" section on page 4-2 for information about testing partial reconciliation

Batched 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 batched reconciliation to avoid such problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `StartRecord`: Use this attribute to specify the record number from which batched reconciliation must begin.
- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify `All Available` as the value of this attribute.

  Note: If you specify `All Available` as the value of this attribute, then the values of the `StartRecord` and `BatchSize` attributes are ignored.

You specify values for these attributes by following the instructions described in the "User Reconciliation Scheduled Task" section on page 3-7.

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed. The log file provides the following information about batched reconciliation:

- Serial numbers of the batches that have been successfully reconciled
- User IDs associated with the records with each batch that has been successfully reconciled
- If the batched reconciliation run fails, then the serial number of the batch that has failed

> **See Also:** The "Testing Batched Reconciliation" section on page 4-3 for information about testing partial reconciliation

Configuring 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 both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

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

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `iPlanetXLResourceObject.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 `iPlanetXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

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

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `iPlanetXLResourceObject.xml` file, which is in the *`OIM_home`*`/xellerate/iPlanet/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.

6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the `TrustedSource` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-5.

Configuring the Reconciliation Scheduled Tasks

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

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-6 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you configure both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-9.

Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `iPlanet Group Lookup Reconciliation` reconciliation scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- 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.

Attribute	Description	Default/Sample Value

`LookupCodeName`	Name of the lookup definition to which values are to be reconciled	The value can be any one of the following:
		■ For groups:
		`Lookup.IPNT.UserGroup`
		■ For roles:
		`Lookup.IPNT.Role`
		■ For organizations and organizational units:
		`Lookup.IPNT.Organization`

`ITResourceName`	Name of the IT resource for setting up a connection with Sun Java System Directory	`iPlanet User`
`SearchContext`	Search context to be used for searching for users	`DC=mycompany,DC=com,o=PXED-DEV`

`ObjectClass`	Name of the group object class	The value can be any one of the following:
		■ For group lookup reconciliation:
		`groupOfUniqueNames`
		■ For role lookup reconciliation:
		`ldapsubentry`
		■ For organization lookup reconciliation:
		`organization`
		■ For organizational unit lookup reconciliation:
		`organizationalunit`

Attribute	Description	Default/Sample Value
CodeKeyLTrimStr	String value for left-trimming the value obtained from the search If there is nothing to be trimmed, then specify the value [NONE].	cn= or uid=
CodeKeyRTrimStr	String value for right-trimming the value obtained from the search If there is nothing to be trimmed, then specify the value [NONE].	,DC=mycompany,DC=com, o=PXED-DEV
ReconMode	Specify REFRESH to completely refresh the existing lookup definition. Specify UPDATE to update the lookup definition with new or modified values.	REFRESH or UPDATE (specified in uppercase)
AttrType	Attribute type of group, role, or organization	The value can be any one of the following: ■ For group and role lookup reconciliation: cn ■ For organization lookup reconciliation: o ■ For organizational unit lookup reconciliation: ou

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

User Reconciliation Scheduled Task You must specify values for the following attributes of the iPlanet User Recon Task scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- 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.

Attribute	Description	Default/Sample Value
ITResourceName	Name of the IT resource for setting up a connection with Sun Java System Directory	iPlanet User
ResourceObjectName	Name of the resource object in which users are reconciled	iPlanet User

Attribute	Description	Default/Sample Value
XLDeleteUsersAllowed	If this attribute is set to True, then the Delete reconciliation event is started when the scheduled task is run. Users who are deleted from the target system are removed from Oracle Identity Manager. This requires all the users on the target system to be compared with all the users in Oracle Identity Manager. If this attribute is set to False, then users deleted from the target system are not deleted from Oracle Identity Manager. **Note:** Setting the value of this attribute to True causes an increase in the time required to complete reconciliation.	True
UserContainer	DN value from where the users are reconciled from the target system to Oracle Identity Manager	ou=user
TrustedSource	Specifies whether or not trusted source reconciliation must be enabled for this connector The value can be True or False.	False
Xellerate Type	Default Xellerate Type value for the Xellerate User	End-User Administrator
Organization	Default organization for the Xellerate User	Xellerate Users
Role	Default role for the Xellerate User	Consultant
StartRecord	This attribute is used for batched reconciliation. It specifies the record number from which batched reconciliation must begin. **See Also:** The "Batched Reconciliation" section on page 3-3	1
BatchSize	This attribute is used for batched reconciliation. It specifies the number of records that must be included in each batch. **See Also:** The "Batched Reconciliation" section on page 3-3	3
NumberOfBatches	This attribute is used for batched reconciliation. It specifies the total number of batches that must be reconciled. **See Also:** The "Batched Reconciliation" section on page 3-3	Default value that reconciles all the records: All Available Sample value: 50
IsIPlanetTarget	This attribute is meant for use in a future release of the connector.	True **Note:** This is the default value. You must not change this value.

After you specify values for these scheduled task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

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 4 of the procedure to configure reconciliation scheduled tasks.

2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Enabling Provisioning of Users in Organizations and Organizational Units
- Provisioning Organizational Units, Groups, and Roles

Compiling Adapters

Note: You must perform the procedure described in this section if you want to use the provisioning features of the connector.

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

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

- Update iPlanet Role Details
- iPlanet PP String
- iPlanet Create OU
- iPlanet Delete OU
- iPlanet Move OU
- iPlanet Create Role
- iPlanet Delete Role
- iPlanet Add User to Group
- iPlanet Create Group
- iPlanet Remove User From Group
- iPlanet Create User
- iPlanet Change Org Name
- iPlanet Delete User
- iPlanet Remove Role from user
- iPlanet Delete Group
- Update iPlanet Group Details

- Chk Process Parent Org
- iPlanet Add Role to User
- iPlanet Move User
- iPlanet Modify User

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

To compile adapters by using the Adapter Manager form:

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

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

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

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *`OIM_home`*`/xellerate/Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

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

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

To view detailed information about an adapter:

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

Enabling Provisioning of Users in Organizations and Organizational Units

Note: This section describes an optional procedure. You need not perform this procedure if you do not want to enable provisioning of users in organizations.

In the `AttrName.Prov.Map.iPlanet` lookup definition, the following are default settings for enabling provisioning of users in organizational units:

- `ldapOrgDNPrefix=ou`
- `ldapOrgUnitObjectClass=OrganizationalUnit`

If you want to enable the provisioning of users in organizations, then change these settings as follows:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about modifying lookup definitions

- `ldapOrgDNPrefix=o`
- `ldapOrgUnitObjectClass=organization`

Provisioning Organizational Units, Groups, and Roles

To provision an organizational unit:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Organizations**.
3. Click **Create**.
4. Specify a name and the type for the organization that you want to create, and then click **Create Organization**.
5. Select **Resource Profile** from the list.
6. Click **Provision New Resource**.
7. Select the organizational unit option.
8. Click **Continue**, and then click **Continue** again.
9. From the IT server lookup field, select the resource object corresponding to the required IT resource.
10. Click **Continue**, and then click **Continue** again on the Verification page.

To provision a group or role:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Expand **Organizations**.
3. Click **Manage**.
4. Search for the organizational unit under which you want to provision the group or role.
5. Select **Resource Profile** from the list.
6. Click **Provision New Resource**.
7. On this page, the option that must select depends on what you want to create:
   - Select the group option if you want to create a group.
   - Select the role option if you want to create a group.
8. Click **Continue**, and then click **Continue** again on the Verification page.
9. Enter a name for the group or role.
10. From the IT server lookup field, select the IT resource.
11. Click **Continue**, and then click **Continue** again on the Verification page.

Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of Sun Java System Directory.

You may want to configure the connector for multiple installations of Sun Java System Directory. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of Sun Java System Directory. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Sun Java System Directory.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Sun Java System Directory.

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

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

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

   The Resource Objects form is in the Resource Management folder. The `iPlanet User` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

   The IT Resources form is in the Resource Management folder. The `iPlanet User` IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

   The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

   - `UD_IPNT_USR` (main form)
   - `UD_IPNT_ROL` (child form for multivalued attributes)
   - `UD_IPNT_GRP` (child form for multivalued attributes)

   You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The `iPlanet User` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

   While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

   - From the **Object Name** lookup field, select the resource object that you create in Step 1.

- From the **Table Name** lookup field, select the process form that you create in Step 3.
- While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:
   - `ITResourceName`
   - `ResourceObjectName`
   - `TrustedSource`

   Set the `TrustedSource` attribute to `True` for the Sun Java System Directory installation that you want to designate as a trusted source.
6. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the Sun Java System Directory installation to which you want to provision the user.

4

Testing and Troubleshooting

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

- Running Test Cases
- Troubleshooting Connector Problems

Running Test Cases

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. Specify values for the parameters in the `TroubleShootIPlanet.properties` file.

   This file is in the *`OIM_home`*`/xellerate/troubleshooting` directory. The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Sun Java System Directory Server connection parameters	Connection parameters required to connect to the target system Refer to the "Defining IT Resources" section on page 2-6 for information about the values that you must provide.
Create User information	Parameters required to create a user
Modify User information	Parameters required to modify a user
Delete User information	DN of the user to be deleted

2. Add the following to the `CLASSPATH` environment variable:

   ```
   OIM_home/xellerate/JavaTasks/xliIPlanet.jar
   OIM_home/xellerate/lib/xlLogger.jar
   OIM_home/xellerate/ext/log4j-1.2.8.jar
   OIM_home/xellerate/lib/xlUtils.jar
   ```

3. Create an ASCII-format copy of the `TroubleShootIPlanet.properties` file as follows:

Note: You must perform this procedure every time you make a change in the contents of the `TroubleShootIPlanet.properties` file.

a. In a command window, change to the following directory:

   OIM_home`/xellerate/troubleshooting`

b. Enter the following command:

   ```
   native2ascii TroubleShootIPlanet.properties global.properties
   ```

   The `global.properties` is created when you run the `native2ascii` command. The contents of this file are an ASCII-format copy of the contents of the `TroubleShootIPlanet.properties` file.

4. Perform the following tests:

   - Create a user as follows:

     ```
     java -DpropertyFile=./global.properties
     -Dlog4j.configuration=./log.properties TroubleShootingUtilityIPlanet
     createUser
     ```

   - Modify a user as follows:

     ```
     java -DpropertyFile=./global.properties
     -Dlog4j.configuration=./log.properties TroubleShootingUtilityIPlanet
     modifyUser
     ```

   - Delete a user as follows:

     ```
     java -DpropertyFile=./global.properties
     -Dlog4j.configuration=./log.properties TroubleShootingUtilityIPlanet
     deleteUser
     ```

Testing Partial Reconciliation

The following are sample query conditions that you can use to test partial reconciliation. You specify these query conditions as values of the `CustomizedReconQuery` parameter.

- Query conditions that contain user attributes
  - Value assigned to the `CustomizedReconQuery` parameter:

    `uid=jodoe|uid=jadoe`

    Outcome: Records of users with user ID `jodoe` or `jadoe` are reconciled.
  - Value assigned to the `CustomizedReconQuery` parameter:

    `givenname=John|mail=john@acmewidgets.com`

    Outcome: Records of users with first name `John` or e-mail address `john@acmewidgets.com` are reconciled.
- Query conditions and time stamp values
  - Value assigned to the `CustomizedReconQuery` parameter: None

    Value of the `Last Recon TimeStamp` parameter: `20070118062126Z`

Outcome: Users with records that are added or updated after the time stamp value are reconciled.

– Value assigned to the `CustomizedReconQuery` parameter: `uid=JOHN`

  Value of the `Last Recon TimeStamp` parameter: `20070118062126Z`

  Outcome: Users with user ID `John` and records that are added or updated after the time stamp value are reconciled.

Testing Batched Reconciliation

You can test batched reconciliation by specifying values for the following user reconciliation scheduled task attributes:

- If you set the value of `StartRecord` to `1`, `BatchSize` to `0`, and `NumberOfBatches` to `All Available`, then all the users are reconciled.
- If you set the value of `StartRecord` to `1`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then the users starting from record 1 are reconciled in 50 batches, with 5 records in each batch.
- If you set the value of `StartRecord` to `200`, `BatchSize` to `5`, and `NumberOfBatches` to `50`, then the users starting from record 200 are reconciled in 50 batches, with 5 records in each batch.

Depending on the application server that you use, log information is written to one of the following file:

- For JBoss Application Server:

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

- For IBM WebSphere:

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

- For BEA WebLogic:

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

- For OC4J:

  OC4J_home`/opmn/logs/default_group~home~default_group~1.log`

In the log file, you can view the batch numbers, the user IDs of the users that are reconciled, and whether or not the reconciliation was successful.

Troubleshooting Connector Problems

The following sections list solutions to some commonly encountered errors of the following types:

- Connection Errors
- Create User Errors
- Modify User Errors
- Delete User Errors
- Reconciliation Errors

Connection Errors

The following table describes solutions to commonly encountered Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to Sun Java System Directory. **Returned Error Message:** Connection error encountered **Returned Error Code:** INVALID_CONNECTION_ERROR	■ Ensure that Sun Java System Directory is running. ■ Ensure that Oracle Identity Manager is running (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Verify that the specified IP address, admin ID, and admin password are correct.
Target not available **Returned Error Message:** Target server not available **Returned Error Code** TARGET_UNAVAILABLE_ERROR	Ensure that the specified Sun Java System Directory server connection values are correct.
Authentication error **Returned Error Messages** Invalid or incorrect password **Returned Error Code** AUTHENTICATION_ERROR	Ensure that the password is correct in the user account credentials that you specify.

Create User Errors

The following table describes solutions to commonly encountered Create User errors.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** Required field information not provided **Returned Error Code:** INSUFFICIENT_INFORMATION_PROVIDED	■ Ensure that the IP address, admin ID, and admin password are correct. ■ Ensure that the following information is provided: User ID User password User container User first name User last name
Oracle Identity Manager cannot create a user. **Returned Error Message:** User already exists **Returned Error Code:** USER_ALREADY_EXIST	Check if a user with the specified ID already exists in Sun Java System Directory. Assign a new ID for this user, and try again.

Problem Description	Solution
Oracle Identity Manager cannot create a user. **Returned Error Message:** Naming exception encountered **Returned Error Code:** INVALID_NAMING_ERROR	■ Check if the specified Sun Java System Directory connection values are correct. ■ Check if an attribute value violates the schema definition.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Required information missing, could not create user **Returned Error Code:** USER_CREATION_FAILED	Check if an attribute value violates the schema definition.
The Create User operation failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** ATTRIBUTE_DOESNOT_EXIST	In the `AttrName.Prov.Map.iPlanet` lookup definition, check if the decode values are valid attribute names in the target system.
The Create User operation failed because an invalid value was being added. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** INVALID_ATTR_VALUE_ERROR	Check the values specified during user creation.

Modify User Errors

The following table describes the solution to commonly encountered Modify User errors.

Problem Description	Solution
Oracle Identity Manager cannot modify the attribute value of a user. **Returned Error Message:** Invalid attribute value or state **Returned Error Code:** INVALID_ATTR_MODIFY_ERROR	Check the specified user ID.

Problem Description	Solution
The Modify User operation failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** ATTRIBUTE_DOESNOT_EXIST	1. From the corresponding process task, get the value that is passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check in the `AttrName.Prov.Map.iPlanet` lookup definition if the decode value is a valid attribute name in the target.
The Modify User operation failed because an invalid value was being added. **Returned Error Message:** Invalid value specified for an attribute **Returned Error Code:** INVALID_ATTRIBUTE_VALUE_ERROR	Check the value specified.
The Modify User operation failed because of an attempt to add a value to an attribute that does not exist in the `AttrName.Recon.Map.iPlanet` lookup definition. **Returned Error Message:** One or more attribute mappings are missing **Returned Error Code:** ATTR_MAPPING_NOT_FOUND	1. From the corresponding process task, get the value that is passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check if an entry has been made in the `AttrName.Recon.Map.iPlanet` lookup definition.
The operation failed because a duplicate value was being added to an attribute. **Returned Error Message:** Duplicate value **Returned Error Code:** DUPLICATE_VALUE_ERROR	Check the value specified.
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Could not move user to different container **Returned Error Code:** USER_MOVE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a user to a security group. **Returned Error Message:** Group does not exist **Returned Error Code:** GROUP_DOES_NOT_EXIST	The specified user security group does not exist in Sun Java System Directory. Check the group name.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Duplicate value **Returned Error Code:** DUPLICATE_VALUE_ERROR	The user is already a member of the group.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Role does not exist **Returned Error Code:** ROLE_DOESNOT_EXIST	The specified role for the user in Oracle Identity Manager does not exist in Sun Java System Directory. Create the role in Sun Java System Directory.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Could not update user **Returned Error Code:** USER_UPDATE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a role to a user. **Returned Error Message:** Duplicate value **Returned Error Code:** DUPLICATE_VALUE_ERROR	The user has already been assigned this role.
Oracle Identity Manager cannot remove a role assigned to a user. **Returned Error Message:** Could not remove role from user **Returned Error Code:** USER_REMOVE_ROLE_FAILED	Generic error. Review the log for more details.

Delete User Errors

The following table describes the solution to a commonly encountered Delete User error.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist **Returned Error Code:** USER_DOESNOT_EXIST	The specified user does not exist in Sun Java System Directory.

Reconciliation Errors

The following table describes the solution to a commonly encountered reconciliation error.

Problem Description	Solution

Oracle Identity Manager cannot reconcile users from Sun Java System Directory.
Returned Error Message:
`javax.naming.NamingException: tcUtilLDAPOperations -> : NamingException : Unable to search LDAP`
Returned Error Code:
`LDAP: error code 11 - Administrative Limit Exceeded`
	Change the Sun Java System Directory configuration as follows:
	1. Open the Sun ONE Directory Server admin console.
	2. Select **Configuration, Performance,** and **Client Control.**
	3. Set the size limit to `unlimited`.
	4. Set the look-through limit to `unlimited`.
	5. Save the changes, and restart Sun Java System Directory.

5

Known Issues

The following are known issues related to this release of the connector:

- If you have configured Sun Java System Directory for nontrusted source reconciliation, then while manually creating a user account in Sun Java System Directory through Oracle Identity Manager, you must ensure that the user ID in the process form is the same as the Oracle Identity Manager user login. Otherwise, reconciliation of the following operations would fail because these operations require direct API calls to update the information:
  - Enable status of user
  - Disable status of user
  - Organization update
- The user search is based on the user ID only.
- During provisioning, you cannot use non-English characters for the password of the user. This is because Sun Java System Directory does not support non-ASCII characters in the Password field.
- During provisioning, you cannot use non-ASCII characters for the user ID or e-mail address of the user. This is because, by default, Sun Java System Directory does not permit the entry of non-ASCII characters in the User ID and E-mail fields. If you want to enable the entry of non-ASCII characters in these fields, then you must disable the 7-bit check plug-in as follows:
  1. Open Sun ONE Directory Server.
  2. Click the **Configuration** tab.
  3. Expand **Plugins.**
  4. Select **7-bit check.**
  5. Deselect the **Enable plug-in** check box.
  6. Click **Save.**
- Some Asian languages use multibyte character sets. Because the character limit for the fields in the target system is specified in bytes, the number of Asian-language characters that you can enter in a particular field is usually 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, then you would not be able to enter more than 25 characters in the same field.

A

Attribute Mappings Between Oracle Identity Manager and Sun Java System Directory

The following table discusses attribute mappings between Oracle Identity Manager and Sun Java System Directory.

Oracle Identity Manager Attribute	Sun Java System Directory Attribute	Description
User ID	uid	User's login ID
First Name	givenname	First name
Last Name	sn	Last name or surname
Organizational Unit	ou	Organization to which a user belongs
Email	mail	E-mail address
ldapUserDisableAttr	nsaccountlock	This attribute specifies whether or not the user's account is locked. If the value is `True`, then the account is locked. If the value is `False`, then the account is not locked.
ldapOrgDNPrefix	ou	Prefix of organization entry
ldapUserDNPrefix	uid	Prefix of user entry
ldapUserUniqueAttr	uid	Unique attribute of user
Middle Name	initials	Middle name
ldapUserObjectClass	inetorgperson	User is represented by the inetOrgPerson object class
GroupName	uniquemember	This is the multivalued attribute for the group object. Its value is a list of user IDs of all the users in the group.
RoleName	nsroledn	Customized object class for role
UserGroup	groupOfUniqueNames	Group represented object class
UserRole	customOrganizationalRole	Role represented object class
ldapUserDNPrefix	uid	User ID of an entry
ldapObjectClass	objectclass	Object classes are used to group information
ldapGroupDNPrefix	cn	Common name of an entry (for example, organization, user, role, or group)
Title	title	User's title
Location	l	City of office address

Oracle Identity Manager Attribute	Sun Java System Directory Attribute	Description
Telephone	telephoneNumber	Office telephone number
Department	departmentnumber	Department name
Communication Language	preferredlanguage	Preferred language for communication
ldapPassword	userpassword	Password
ldapTargetResourceTimeStampField	modifytimestamp	Time stamp of the last modification
ldapRoleDNPrefix	cn	Common name of an entry (for example, organization, user, role, or group)
ldapRoleMemberName	nsroledn	Members to whom the role has been assigned
ldapOrgDNPrefix	ou	Common name of an entry (for example, organization, user, role, or group)
ldapUserObjectClass	inetorgperson	Object class for the user
ldapRoleObjectClass	ldapsubentry	Object class of the role
ldapOrgPersonObject	OrganizationalPerson	Required object class for the user of any organization
ldapOrgUnitObjectClass	ldunit	Object class of organizational unit
ldapGroupObjectClass	group	Object class of group

Index

M

O

P

R

S

T

U

X