Oracle® Identity Manager

Connector Guide for Sun Java System Directory

Release 9.0.4

E10446-04

July 2009

ORACLE®

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

E10446-04

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

3 Configuring the Connector

Preface

This guide provides information about Oracle Identity Manager Connector for Sun Java System Directory.

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.

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For 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/oim.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/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 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 9.0.4.4.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

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

- Software Updates in Release 9.0.4.1_6742889
- Software Updates in Release 9.0.4.1_6858468
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4

Software Updates in Release 9.0.4.1_6742889

The following are software updates in release 9.0.4.1_6742889:

- Resolved Issues
- Support for New Attributes and Object Classes for Reconciliation and Provisioning
- Support for Native Queries for Partial Reconciliation
- Support for Configuring Both Target Resource and Trusted Source Reconciliation
- Changes in the Directory Structure of the Connector Files on the Installation Media

Resolved Issues

The following are issues resolved in release 9.0.4.1_6742889:

Bug Number	Issue	Resolution
5353476	A limited subset of target system attributes was available for reconciliation.	You can now expand the subset of target system attributes for reconciliation.
6332970	Provisioning was limited to the default object class (`inetorgperson`) of Sun Java System Directory.	You can specify the mandatory and optional attributes of a custom object class that you want to use for provisioning operations.
6333007	A limited subset of target system attributes was available for trusted source reconciliation.	The subset of attributes has been expanded.
6521484	There was scope for improvement in the reconciliation of deleted user data.	Reconciliation of deleted user data has been optimized. To realize the full benefit of this change, you must upgrade the Oracle Identity Manager installation to Oracle Identity Manager release 9.0.3.0.8a or later (or the equivalent in the release 9.0.1, 9.0.3.1, and 9.1 tracks). Contact Oracle Global Support for further information on the equivalent Oracle Identity Manager patch.

Support for New Attributes and Object Classes for Reconciliation and Provisioning

You can add new attributes and object classes for reconciliation and provisioning. See the following sections for more information:

- Adding New Attributes for Group or Role Reconciliation
- Adding New Attributes for Provisioning
- Adding New Object Classes

Support for Native Queries for Partial Reconciliation

You can now use a native query for implementing partial reconciliation. In the earlier release, you could use only queries specified in a non-native format to implement partial reconciliation. To implement this feature, the `IsNativeQuery` attribute has been added to the scheduled task.

See "Partial Reconciliation" for more information.

Support for Configuring Both Target Resource and Trusted Source Reconciliation

You can now configure the connector for both target resource and trusted source reconciliation. The reconciliation scheduled task has been modified to implement this feature. To implement this feature, the `DualMode` attribute has been added to the scheduled task.

Note: The Dual Mode Reconciliation feature has been desupported from release 9.0.4.3 onward.

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

The `xliIPlanet.jar` file has been split into two files, `SJSDSProv.jar` and `SJSDSRecon.jar`. Corresponding changes have been made in the following sections:

- Files and Directories on the Installation Media
- Determining the Release Number of the Connector
- Copying the Connector Files

Software Updates in Release 9.0.4.1_6858468

The following are issues resolved in release 9.0.4.1_6858468:

Bug Number	Issue	Resolution
6858468	If you performed an Update User provisioning operation on a user who was created directly under the root context, then an error was encountered.	This issue has been resolved. You can now perform Update User provisioning operations on users who are created directly under the root context.
6488868	For connector operations, you had to use an administrator account on the target system with maximum privileges.	You can now create a target system account with specific privileges for connector operations. See "Creating a Target System User Account for Connector Operations" on page 2-2 for more information.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

Using the Connector Installer

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

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

Resolved Issues

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7262351	User details and group details are stored in separate object classes on the target system. For *each* target system user, a new connection to the target system was opened for fetching the user's group membership details during a reconciliation run. Performance was adversely affected if a large number of connections were opened.	This issue has been resolved. A single connection is used to fetch group membership details. This connection is kept open until the end of the reconciliation run.
7282425	A reconciliation search filter and sort query are run on the target system records during reconciliation. If the target system contained a large number of users, then the reconciliation process was very slow.	In earlier releases, target system records were sorted on the basis of the `modifytimestamp` attribute. You can now create a VLV index on the target system and select the attribute on the basis of which target system records must be sorted during reconciliation. See "Creating a VLV Index" on page 2-4 for information about the procedure to create VLV index.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

Support for New Target System Version

Sun ONE Directory Server 6.3 has been added to the list of certified target system versions. See "Verifying Deployment Requirements" for information about the full list of certified target system versions.

No Support for Dual Mode Reconciliation

In earlier releases, the connector supported dual mode reconciliation in which you ran both trusted source and target resource reconciliation on the target system. From this release onward, the connector does not support dual mode reconciliation.

Support for Adding New Attributes for Connector Operations

From this release onward, the following procedures are supported:

- Adding New Attributes for Trusted Source Reconciliation
- Adding New Multivalued Attributes for Target Resource Reconciliation
- Enabling Update of New Multivalued Attributes for Provisioning

Additions to the List of Fields Covered by Reconciliation

In the "Reconciled Resource Object Fields" section, the following fields have been added to the list of fields covered by target resource reconciliation:

- NsuniqueID
- Common Name
- Status

In the "Reconciled Xellerate User (OIM User) Fields" section, the `Status` field has been added to the list of fields covered by trusted source reconciliation.

Additions to the List of Fields Covered by Provisioning

In the "Provisioning Module" section, the `Common Name` field has been added to the list of fields covered by provisioning.

Resolved Issues

The following are issues resolved in release 9.0.4.3:

Bug Number	Issue	Resolution

7612234	The following is the format of the time-stamp filter applied to each target system record during reconciliation:
	`timestamp_record_updated >= last_reconciliation_run_timestamp`
	
	When this filter was applied, a record that was added or modified at the instant the reconciliation run ended was also reconciled. However, the application of the time-stamp filter caused the same record to be reconciled during the next reconciliation run.
		This issue has been resolved.
		The time-stamp filter cannot be changed to the following:
		`timestamp_record_updated > last_reconciliation_run_timestamp`
		
		As a workaround, one second is added to the time stamp recorded in the IT resource before the filter is applied during a reconciliation run. In other words, the filter is changed to the following:
		`timestamp_record_updated + 1 second >= last_reconciliation_run_timestamp`
		
		Application of this filter ensures that a record reconciled at the end of a reconciliation run is not reconciled during the next reconciliation run.

7557852	The following issue was observed if you created and then disabled a user on the target system before the user was reconciled into Oracle Identity Manager: After the reconciliation run, the OIM User was created with the Active status.	This issue has been resolved. If the user is Disabled on the target system, then the user is created with the Disabled status on Oracle Identity Manager. **Note:** The minimum release of Oracle Identity Manager that supports reconciliation of status data is release 9.0.3.2. This requirement is mentioned later in the guide.

7516594	Suppose you had two organizations with the same name and at different locations on the target system, for example:
	`ou=PeopleOrg,dc=support`
	`ou=PeopleOrg,ou=Engineering,dc=support`
	
	After lookup field reconciliation, the Code Key column was populated with the DN value and the Decode key was populated with the organization name.
	Because provisioning was based on the Decode key, the user was sometimes provisioned to the wrong organization.
		This issue has been resolved. Provisioning operations are performed in the specified organization even if there is more than one organization with the same name.

7478975 and 7676228	During reconciliation of deleted users, records of users who had been newly created or modified were also fetched into Oracle Identity Manager. The `IsIplanetTarget` attribute was redundant.	This issue has been resolved. New scheduled tasks have been introduced in this release. See "Configuring the Reconciliation Scheduled Tasks" for more information.

Bug Number	Issue	Resolution
7386568	During lookup reconciliation, roles names are reconciled in the same case (uppercase and lowercase) in which they are stored in the target system lookup field. When you assign a role to a user on the target system, the role name is converted to lowercase letters in the user record. When you reconcile this user into Oracle Identity Manager, the role name is stored in Oracle Identity Manager in the same case (uppercase and lowercase) in which it is stored on the target system. If the role assigned to a user was stored in a different case in the lookup definition, then the role details were not displayed along with the rest of the user details in Oracle Identity Manager.	This issue has been resolved. During lookup field reconciliation, names of all roles are converted to lowercase. With this update, roles assigned to users can be matched with the roles in the lookup definition and, therefore, role details can be displayed in Oracle Identity Manager. For information about a limitation related to this resolution, see Bug 8276871 in the "Known Issues" chapter.
7345488	Incremental reconciliation did not work if you set the `IsNativeQuery` attribute to `yes` and also specified a value for the `CustomizedReconQuery` parameter.	The `IsNativeQuery` attribute and `CustomizedReconQuery` parameter have been replaced by the `searchfilter` scheduled task attribute. See "User Reconciliation Scheduled Task" for more information.
6937079	Only a single time-stamp format was supported. The time stamp is used during reconciliation to identify newly added or modified target system records.	This issue has been resolved. You can now use the `TARGET_TIMESTAMP_SEARCHFORMAT` parameter in the `IPNT.Parameter` lookup definition to specify the time-stamp format. See "Setting Up Lookup Definitions in Oracle Identity Manager" for more information.
6792067	The target system allows you to change the user ID (UID) of a user. However, when reconciliation was performed after the user ID of a user was changed on the target system, a new account was created for the user in Oracle Identity Manager.	This issue has been resolved. The `nsuniqueid` field of the target system is now used as the key field for reconciliation matching. This field is populated by the target system during user creation.
7676205	The Prov Attribute Lookup Code and Attribute Lookup Code IT resource parameters did not have default values.	This issue has been resolved. The following default values have been assigned to these parameters: ■ For the Prov Attribute Lookup Code parameter: `AttrName.Prov.Map.iPlanetRecon` ■ For the Attribute Lookup Code parameter: `AttrName.Recon.Map.iPlanet`
7721222	When you disable a user on the target system: ■ The `cn=nsmanageddisablerole` role is assigned to the user. ■ The `nsaccountlock` flag of the user's record is set to `TRUE`. When you disabled a user on Oracle Identity Manager, only the `nsaccountlock` flag of the user's record was set to `TRUE`.	This issue has been resolved. When you disable a user on Oracle Identity Manager, the `cn=nsmanageddisablerole` role is assigned to the user and the `nsaccountlock` flag of the user's record is set to `TRUE`. For information about a limitation related to this resolution, see Bug 8294827 in the "Known Issues" chapter.

Bug Number	Issue	Resolution
7707148 and 7676263	Batched reconciliation did not work if you set the `BatchSize` attribute to `0`. The `StartRecord` attribute was redundant.	This issue has been resolved. If you set the `BatchSize` attribute to 0, then all target system records are fetched into Oracle Identity Manager at the same time. In other words, set the `BatchSize` attribute to 0 if you do not want to implement batched reconciliation. The `StartRecord` attribute has been removed.
7680631	During a provisioning operation, the e-mail address that you specified for the user was not propagated to the target system.	This issue has been resolved. During provisioning operations, the e-mail address is propagated to the target system along with the rest of the user data fields.
7676299	Two lookup definitions were mapped to the same group data table on the target system.	This issue has been resolved. One of the lookup definitions has been deleted.
7676283	Default roles and groups were assigned to users during provisioning operations.	This issue has been resolved. Default roles and groups are not assigned during provisioning operations.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- Support for High-Availability
- Support for Attribute Mapping for Groups and Roles
- Resolved Issues

Support for High-Availability

The high-availability feature for ITResource is now supported by the connector. This feature enables the connector to perform operations using the backup servers if the primary LDAP server fails or is unavailable.

Support for Attribute Mapping for Groups and Roles

The connector now supports attribute mapping for groups and roles. New attributes can be added for groups and roles, and they can be provisioned and reconciled.

Resolved Issues

The following are issues resolved in release 9.0.4.4:

Bug Number	Issue	Resolution
8287081	The connector did not support attribute mapping for Roles and Groups.	This issue has been resolved. The connector now supports attribute mapping for groups and roles. New attributes can be added for groups and roles, and they can be provisioned and reconciled.
8287058	The Organization Name in the Resource Object form for Groups and Roles field was a text field instead of a lookup field.	This issue has been resolved. The Organization Name in the Resource Object form for Groups and Roles is now modified to a look up field.

Documentation-Specific Updates

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

- Documentation-Specific Updates from Release 9.0.4 Through 9.0.4.2

Documentation-Specific Updates from Release 9.0.4 Through 9.0.4.2

- There are no known issues associated with this release of the connector. Points that were earlier listed in the "Known Issues" chapter have been moved to the "Guidelines to Be Applied While Using the Connector" section.
- Changes have been made in the "Configuring SSL" section.
- Instructions to create or modify the ACI for the user account have been added in the following sections:
  - Creating a Target System User Account for Connector Operations
  - Adding New Attributes for Group or Role Reconciliation
  - Adding New Attributes for Provisioning
  - Adding New Object Classes

Documentation-Specific Updates in Release 9.0.4.3

The following are documentation-specific updates in release 9.0.4.3:

- In the "Multilanguage Support" section, Arabic has been added to the list of supported languages.
- In the "Testing and Troubleshooting" chapter, the "Testing Partial Reconciliation" and "Testing Batched Reconciliation" sections have been removed.
- In the "Known Issues" chapter, known issues have been added.

Documentation-Specific Updates in Release 9.0.4.4

The following are documentation-specific updates in release 9.0.4.4:

- In the "Configuring the IT Resource" section, IT resource parameters have been added.
- In the "Importing the Connector XML File" section, IT resource parameters have been added.
- In the "Deploying the Connector" chapter, the "Configuring High Availability of the Target System" section has been added.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.
- In the "Specifying Values for the Scheduled Task Attributes" section, the "Group and Role Reconciliation Scheduled Task" section has been added.
- In the "Compiling Adapters" section, the adapter list has been updated.
- In the "Provisioning Organizational Units, Groups, and Roles" section, the lookup definition for provisioning Group and Role in organization unit has been added.
- In the "Configuring the Connector" chapter, the "Adding New Attributes for Group or Role Reconciliation" section has been added.
- In the "Adding New Multivalued Attributes for Target Resource Reconciliation" section, a Note has been added for provisioning multivalued attributes for Group and Role.
- In the "Known Issues" chapter, known issues have been removed.

1

About the Connector

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

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, Sun Java System Directory has been referred to as the *target system*.

1.1 Reconciliation Module

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

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

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

1.1.1 Lookup Fields Reconciliation

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

1.1.2 User Reconciliation

User reconciliation involves reconciling the fields discussed in this section.

1.1.2.1 Reconciled Resource Object Fields

The following target system fields are reconciled:

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

1.1.2.2 Reconciled Xellerate User (OIM User) Fields

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

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

1.2 Provisioning Module

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

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

For this target system, the following fields are provisioned:

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

1.3 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

Function	Type	Description
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
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
Group Name Updated	Provisioning	Changes the group name
Create iPlanet Role	Provisioning	Creates iPlanet role
Delete iPlanet Role	Provisioning	Deletes iPlanet role
Role Name Updated	Provisioning	Changes the role name
Common Name Updated	Provisioning	Changes the common name
User ID Updated	Provisioning	Changes the user ID
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"

1.4 Multilanguage Support

The connector supports the following languages:

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

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

1.5 Files and Directories on the Installation Media

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

Table 1–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
`configuration/SJSDS-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/SJSDSProv.jar`	This JAR file contains the class files required for provisioning. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/JavaTasks`
`lib/SJSDSRecon.jar`	This JAR file contains the class files required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/ScheduleTask`

Table 1–1 (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 deployment, these resource bundles are copied into the following directory: *OIM_HOME*`/xellerate/connectorResources` **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.
`test/troubleshoot/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.
`test/troubleshoot/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.
`test/troubleshoot/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.
`xml/iPlanetResourceObject.xml`	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ 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 (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

File in the Installation Media Directory	Description
`configuration/SJSDS-CI.xml`	This XML file contains configuration information that is used during connector installation.
`lib/SJSDSProv.jar`	This JAR file contains the class files required for provisioning. During connector deployment, this file is copied into the following directory: *OIM_HOME*`/xellerate/JavaTasks`

File in the Installation Media Directory	Description
lib/SJSDSRecon.jar	This JAR file contains the class files required for reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied into the following directory: *OIM_HOME*/xellerate/connectorResources **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.
test/troubleshoot/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.
test/troubleshoot/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.
test/troubleshoot/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.
xml/iPlanetResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ 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 (OIM 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.

1.6 Determining the Release Number of the Connector

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

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

   OIM_HOME/xellerate/JavaTasks/SJSDSProv.jar

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

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

2

Deploying the Connector

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Using External Code Files
- Configuring the Target System
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 9.0.3.2 or Later Release in the 9.0.3.x Series
- Configuring the Oracle Identity Manager Server
- Configuring SSL

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 9.0.3.2 or later
Target systems	Sun ONE Directory Server 5.2 Sun Java System Directory Server Enterprise Edition 6.3
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 configuring the IT resource. The procedure is described later in the guide. 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.

2.2 Using External Code Files

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

The `ldapbp.jar` file is used by the connector to enable LDAP-based search of user records on the target system. You must download this JAR file from the Sun Web site and copy it into the `ThirdParty` directory as follows:

1. Log on the Sun Web site at

   `http://java.sun.com/products/jndi/downloads/index.html`

2. Click **Download JNDI 1.2.1 & More**.
3. From the table on the page that is displayed, select and download the file containing the ldapbp.jar file.
4. Copy the ldapbp.jar file into the following directories:

   OIM_HOME`/xellerate/ThirdParty`

> **Note:** In an Oracle Identity Manager cluster, copy this JAR file into the `ThirdParty` directory on each node of the cluster.

2.3 Configuring the Target System

Configuring the target system involves performing the following steps:

- Creating a Target System User Account for Connector Operations
- Creating a VLV Index

2.3.1 Creating a Target System User Account for Connector Operations

Oracle Identity Manager requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account while performing the procedure described in "Configuring the IT Resource" on page 2-6.

To create this user account:

> **See Also:** Sun Java System Directory documentation for detailed information about performing this procedure

1. Log in to the Sun One Server Console by using administrator credentials.
2. Expand the host name folder.
3. Expand **Server Group**.
4. Select **Directory Server**, and then click **Open** on the right pane.
5. On the Directory tab, right-click the root context. You can also select the OU under the root context in which you want to create the user.

6. From the shortcut menu that is displayed, select **New** and then select **User**.
7. In the Create New User dialog box, enter information about the user account and then click **OK**.

   The newly created user account is displayed on the right pane.
8. To determine the entryDN value of the user account:
   a. Right-click the user account, and select **Edit with Generic Editor**.
   b. In the Generic Editor dialog box, copy the value that is displayed in the **entrydn** field. Record this value for future reference. You use the `entrydn` while assigning permissions to the user account. In addition, while configuring the IT resource, you specify the entrydn as the value of the `AdminId` IT resource parameter.

After creating the user account, you must assign the following permissions to the user account for each target system attribute that is used during reconciliation and provisioning:

- Read: View the value of the attribute.
- Write: Modify the value of the attribute.
- Add: Set a value for the attribute.
- Delete: Remove the value of the attribute.

To assign permissions to the user account:

1. On the Sun One Server Console, expand the host name folder.
2. Expand **Server Group**.
3. Select **Directory Server**, and then click **Open** on the right pane.
4. On the Directory tab, right-click the root context.
5. From the shortcut menu that is displayed, select **Edit with Generic Editor**.
6. Select **aci**.
7. In the Edit region, click **Add value**.
8. In the field that is displayed, copy the following:

```
(targetattr = "physicalDeliveryOfficeName || homePhone ||
preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
internationaliSDNNumber || owner || postalAddress || roomNumber || givenName ||
carLicense || userPKCS12 || searchGuide || userPassword ||
teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
userSMIMECertificate || displayName || destinationIndicator || telexNumber ||
employeeNumber || secretary || uid || userCertificate || st || sn ||
description || mail || labeledUri || businessCategory || homePostalAddress ||
x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou || nsAccountLock
|| seeAlso || registeredAddress || postalCode || photo || title || uniqueMember
|| street || pager || departmentNumber || dc || o || cn || l || initials ||
telephoneNumber || preferredLanguage || facsimileTelephoneNumber || x121Address
|| employeeType") (version 3.0;acl "ACI_NAME";allow
(read,write,delete,add)(userdn = "ldap:///ENTRYDN_VALUE");)
```

9. In the string that you copy:
   - Replace *ACI_NAME* with the name that you want to assign to the ACI, for example, `OIMUserACI`.

- Replace *ENTRYDN_VALUE* with the entrydn value that you record in Step 8.b, for example, `uid=OIMUser,ou=Org1,dc=corp,dc=oracle,dc=com`.

10. Click **OK**.
11. To view or modify the access permissions you have set for the user account:
    a. In the main Sun One Server Console window, right-click the root context.
    b. From the shortcut menu, click **Set Access Permissions**.
    c. In the Manage Access Control dialog box, select the ACI that you create for the user account and then click **Edit**.

       The ACI that you create for the user account is displayed.
    d. If required, make changes in the ACI and then click **OK**.

2.3.2 Creating a VLV Index

By creating a VLV index, you can improve the performance of reconciliation runs. To create a VLV index:

1. Log in to the Sun One Server Console by using administrator credentials.
2. Expand the host name folder.
3. Expand **Server Group**.
4. Select **Directory Server**, and then click **Open** on the right pane.
5. On the Directory tab, right-click the root context.
6. From the shortcut menu that is displayed, select **New** and then select **Other**.
7. In the New Object dialog box, select **vlvindex** and then click **OK**.
8. In the Generic Editor dialog box, select **Object class** and then click **Add value**.
9. In the Add Object Class dialog box, select **vlvsearch** and then click **OK**.
10. In the Generic Editor dialog box, click **Change**.
11. In the Naming Attribute column of the Change Naming Attribute dialog box, deselect the check box for the vlvsort attribute, select the check box for the cn attribute, and then click **OK**.
12. Specify values for the following attributes:
    - **vlvbase**: Enter the tree level where you want the index to be created.

      Sample value: `dc=corp,dc=example,dc=com`
    - **vlvfilter**: Enter the search filter for the index.

      Sample value: `(|(objectclass=*)(objectclass=ldapsubentry))`
    - **vlvscope**: This attribute specifies the scope of the search. Specify one of the following values:
      - Enter `0` for a base-level search.
      - Enter `1` stands for a one-level search.
      - Enter `2` for a sub-tree search.

      Sample value: `1`
    - **vlvsort**: This attribute specifies the sort order that the VLV ldapsearch command uses for the VLV index.

Sample value: `modifytimestamp`

13. Click **OK**.

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

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

Installing the connector on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.4.1 Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME`/xellerate/ConnectorDefaultDirectory`

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

   OIM_HOME`/xellerate/ConnectorDefaultDirectory`

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **Sun Java System Directory *RELEASE_NUMBER***.
5. Click **Load**.
6. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries
   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see "Configuring Trusted Source Reconciliation" on page 3-4.

c. Compilation of adapters

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

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

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

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

Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-11 for information about running the `PurgeCache` utility.

There are no prerequisites for some predefined connectors.

b. Configuring the IT resource for the connector

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

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

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

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

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See "Files and Directories on the Installation Media" on page 1-5 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

You must specify values for the parameters of the `iPlanet IT Resource` IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management.**

3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `iPlanet User` 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. The following table describes each parameter:

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=netscaperoot`
`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
`Port`	Port number to connect to the target Sun Java System Directory server The default value is `389`. This parameter is mentioned in the "Configuring SSL" section on page 2-16.
`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 "Configuring SSL" section on page 2-16. **Note:** It is recommended that you enable SSL to secure communication with the target system.
`Target Resource Reconciliation Time Stamp`	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a target resource reconciliation run ends. **Note:** You must not change the default value of this parameter.
`Trusted Source Reconciliation Time Stamp`	Starting with the first reconciliation run, this parameter stores the time-stamp value at which trusted source reconciliation run ends. **Note:** You must 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 of users 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 of users 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 Sun Java System Directory is used for reconciliation.

Parameter	Description
Group Reconciliation Time Stamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a group reconciliation run ends. **Note:** You must not change the default value of this parameter.
Role Reconciliation Time Stamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a role reconciliation run ends. **Note:** You must not change the default value of this parameter.
Prov Group Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning of Groups. The default value of this parameter is AtMap.iPlanetGroup.
Prov Role Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning of Roles. The default value of this parameter is AttrMap.iPlanetRole.

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

2.5 Installing the Connector on Oracle Identity Manager Release 9.0.3.2 or Later Release in the 9.0.3.x Series

Installing the connector on any Oracle Identity Manager release between release 9.0.3.2 or later releases in the 9.0.3.x series involves the following procedures:

- Copying the Connector Files
- Importing the Connector XML File

2.5.1 Copying the Connector Files

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

See Also: "Files and Directories on the Installation Media" on page 1-5 for more information about these files

Files in the Installation Media Directory	Destination Directory
lib/SJSDSProv.jar	*OIM_HOME*/xellerate/JavaTasks
lib/SJSDSRecon.jar	*OIM_HOME*/xellerate/ScheduleTasks
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the test directory	*OIM_HOME*/xellerate/SJSDS/test/troubleshoot
Files in the xml directory	*OIM_HOME*/xellerate/SJSDS/xml

Note: In a clustered environment, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

2.5.2 Importing the Connector XML File

As mentioned in the "Files and Directories on the Installation Media" 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 opening 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 following table for information about the values to be specified:

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=netscaperoot`
`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
`Port`	Port number to connect to the target Sun Java System Directory server The default value is `389`. This parameter is mentioned in the "Configuring SSL" section on page 2-16.
`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 "Configuring SSL" section on page 2-16. **Note:** It is recommended that you enable SSL to secure communication with the target system.
`Target Resource Reconciliation Time Stamp`	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a target resource reconciliation run ends. **Note:** You must not change the default value of this parameter.

Parameter	Description
Trusted Source Reconciliation Time Stamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which trusted source reconciliation run ends. **Note:** You must 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 Sun Java System Directory is used for reconciliation.
Group Reconciliation Time Stamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a group reconciliation run ends. **Note:** You must not change the default value of this parameter.
Role Reconciliation Time Stamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which a role reconciliation run ends. **Note:** You must not change the default value of this parameter.
Prov Group Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning of Groups. The default value of this parameter is AtMap.iPlanetGroup.
Prov Role Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning of Roles. The default value of this parameter is AttrMap.iPlanetRole.

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 Administrative and User Console Guide* for instructions.

11. Click **View Selections.**

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

2.6 Configuring the Oracle Identity Manager Server

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
- Setting Up Lookup Definitions in Oracle Identity Manager

2.6.1 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.

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-8, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

   Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

   `OIM_HOME``/xellerate/bin/`*`batch_file_name`*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

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

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

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

2.6.3 Enabling Logging

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **BEA WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.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, log information is displayed on the server console.

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

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

2.6.4 Setting Up Lookup Definitions in Oracle Identity Manager

The following lookup definition are created in Oracle Identity Manager when you deploy the connector:

- `Lookup.IPNT.CommLang`

  During a provisioning operation, you use this lookup definition to specify a communication language for the user.

- `IPNT.Parameter`

  The entries in this lookup definition are used during both reconciliation and provisioning.

You must enter or modify values in these lookup definitions before they can be used for connector operations.

To enter or modify value in the lookup definitions:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the **Lookup.IPNT.CommLang** lookup definition.
4. Enter Code Key and Decode values for each communication language that can be used for provisioning operations.

   You can enter any value. However, you must enter the same value in both the Code Key and Decode column, for example, `German`.
5. Click **Save**.
6. Search for and open the **IPNT.Parameter** lookup definition.

   Enter Decode values for the following Code Key entries:

   Note: It is recommended that you do not change Decode values of the remaining code Key entries.

   - TARGET_TIMESTAMP_SEARCHFORMAT

     Use this parameter to specify the time-stamp format used by the target system to store time stamps of events related to user data changes. During reconciliation, the connector uses the time stamp value of each event to determine whether the user data change should be fetched into Oracle Identity Manager for reconciliation.

     Default value: `yyyyMMddHHmmss.0'Z'`

   - SPECIALCHARACTERS

     Use this parameter to specify the special characters that must not be allowed in the User ID and Common Name fields during reconciliation and provisioning operations.

     Default value: `#%+,<>|/`

     Note: Do not use a separator when you add or remove special characters from the default list of special characters.

   - TREE_DELETE_CONTROL_OID

Use this parameter to specify the OID of the object whose deletion you want to enable for connector operations.

Default value: `2.5.4.11` (this is the OID of organizational units)

- LDAP_REFERRAL

  Use this parameter if there are multiple root contexts in your organization. You can specify one of the following values:

  - `NONE`: Specifies that the LDAP search must not use the LDAP_REFERRAL parameter.
  - `follow`: Specifies that the LDAP search must follow referrals automatically.
  - `ignore`: Specifies that the LDAP search must ignore referrals.
  - `throw`: Specifies that the LDAP search must throw the `ReferralException` exception when a referral is encountered.

  Default value: NONE

2.6.5 Configuring High Availability of the Target System

Suppose you have set up multiple, replicated installations of the target system for high availability. You can use the Lookup.iPlanet.BackupServers lookup definition to ensure that if the primary target system installation becomes unavailable, then Oracle Identity Manager switches to one of the secondary target system installations. The Lookup.iPlanet.BackupServers lookup definition is one of the lookup definitions created when you deploy the connector.

For a single primary installation, you can have any number of secondary installations. In addition, if you configure the connector to work with multiple primary installations, then you can specify secondary installations for each primary installation.

To use the Lookup.iPlanet.BackupServers lookup definition, open it in the Design Console and enter code key and decode values for each combination of primary and secondary target system installation.

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

Table 2–1 shows samples entries for the Lookup.iPlanet.BackupServers lookup definition.

Table 2–1 Samples Entries for the Lookup.iPlanet.BackupServers Lookup Definition

Code Key	Decode
172.20.55.64	172.20.55.65
172.20.55.64	172.20.55.66
172.20.55.97	172.20.55.98

In this table, the first two entries represent two secondary installations (172.20.55.65 and 172.20.55.66) for one primary installation (172.20.55.64). The third entry shows a one-to-one combination of primary (172.20.55.97) and secondary (172.20.55.98) installations.

2.7 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, you must perform the following tasks:

1. Creating the CA and SSL Certificates
2. Importing the CA and SSL Certificates into Sun Java System Directory
3. Importing the CA and SSL Certificates into Oracle Identity Manager
4. Enabling SSL Communication on Sun Java System Directory

2.7.1 Creating the CA and SSL Certificates

Creating the CA and SSL certificates involves performing the following procedures:

- Generating the Certificate Signing Request on Sun Java System Directory
- Using the Certificate Signing Request to Generate the CA and SSL Certificates

2.7.1.1 Generating the Certificate Signing Request on Sun Java System Directory

To generate the certificate signing request:

1. Export the certificate file on the target system as follows:
   a. Log in to the Sun One Server Console by using administrator credentials.
   b. Expand the host name folder.
   c. Expand **Server Group**.
   d. Select **Directory Server**, and then click **Open** on the right pane.
   e. On the Tasks tab, click **Manage Certificates**.
   f. When you are prompted for the Security Device password, specify the password.

      Note: You use this password again while importing the SSL certificate into Sun Java System Directory.

   g. On the Server Certs tab of the Manage Certificates dialog box, click **Request**.
   h. On the first page of the Certificate Request Wizard, ensure that **Request Certificate Manually** is selected and then click **Next**.
   i. On the Requestor Information page of the wizard, enter the required information and then click **Next**.
   j. On the Token Password page of the wizard, enter the security device password that you provided earlier and then click **Next**.
   k. On the Request Submission page of the wizard, click **Save to file**.
   l. In the Save dialog box, specify a location and name for the file and then click **Save**.
   m. On the Request Submission page of the wizard, click **Done**.

2.7.1.2 Using the Certificate Signing Request to Generate the CA and SSL Certificates

To generate CA and SSL certificates, follow the procedure defined by the certificate authority (CA) that you want to use. While performing that procedure, use the certificate signing request that you created earlier. Download and save the certificate (`.cer`) files to the Sun Java System Directory host computer.

2.7.2 Importing the CA and SSL Certificates into Sun Java System Directory

The following sections describe the procedure to import the CA and SSL certificates into Sun Java System Directory:

- Importing the CA Certificate into Sun Java System Directory
- Importing the SSL Certificate into Sun Java System Directory

2.7.2.1 Importing the CA Certificate into Sun Java System Directory

To import the CA certificate to Sun Java System Directory:

1. Log in to the Sun One Server Console by using administrator credentials.
2. Expand the host name folder.
3. Expand **Server Group**.
4. Select **Directory Server**, and then click **Open** on the right pane.
5. On the Tasks tab, click **Manage Certificates**.
6. On the CA Certs tab of the Manage Certificates dialog box, click **Install**.
7. On the Certificate Location page of the Certificate Install Wizard, use the **Browse** button to navigate to the CA certificate file that you saved on this computer. Then, click **Next**.
8. On the Certificate Information page of the Certificate Install Wizard, click **Next**.
9. On the Certificate Type page of the Certificate Install Wizard, click **Next**.
10. On the Intended Purpose page of the Certificate Install Wizard, ensure that both check boxes are selected and then click **Done**.

2.7.2.2 Importing the SSL Certificate into Sun Java System Directory

To import the SSL certificate to Sun Java System Directory:

1. Log in to the Sun One Server Console by using administrator credentials.
2. Expand the host name folder.
3. Expand **Server Group**.
4. Select Directory Server, and then click **Open** on the right pane.
5. On the Tasks tab, click **Manage Certificates**.
6. On the Server Certs tab of the Manage Certificates dialog box, click **Install**.
7. On the Certificate Location page of the Certificate Install Wizard, use the **Browse** button to navigate to the SSL certificate file that you saved on this computer. Then, click **Next**.
8. On the Certificate Information page of the Certificate Install Wizard, click **Next**.
9. On the Certificate Type page of the Certificate Install Wizard, click **Next**.

10. On the Token Password of the Certificate Install Wizard, enter the security device password and then click **Done**.

2.7.3 Importing the CA and SSL Certificates into Oracle Identity Manager

To import the CA and SSL certificates into the certificate store of the Oracle Identity Manager host computer:

> **Note:** In a clustered environment, you must perform this procedure on all the nodes of the cluster.

1. Copy both certificate files to the Oracle Identity Manager host computer.
2. Change to the directory where you copy the certificate files.
3. For each certificate, enter a command similar to the following:

   ```
   keytool -import -alias ALIAS -file CER_FILE -keystore MY_CACERTS -storepass
   PASSWORD
   ```

   In this command:

   - *ALIAS* is the alias for the certificate (for example, the server name).
   - *CER_FILE* is the full path and name of the certificate (.cer) file.
   - *MY_CACERTS* is the full path and name of the certificate store.

     Table 2–2 shows the location of the certificate store for each of the supported application servers.

Table 2–2 Certificate Store Locations

Application Server	Certificate Store Location
BEA WebLogic Server	■ If you are using BEA jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ■ If you are using the default BEA WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	■ For a nonclustered configuration of any supported IBM WebSphere Application Server release, import the certificate into the following certificate store: *WEBSPHERE_HOME*/java/jre/lib/security/cacerts ■ For IBM WebSphere Application Server 6.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/AppServer/profiles/*SERVER_NAME*/config/cells/*CELL_NAME*/nodes/*NODE_NAME*/trust.p12 For example: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv02\config\cells\wkslaurel3224Node02Cell\nodes\wkslaurel3224Node02\trust.p12 ■ For IBM WebSphere Application Server 5.1.*x*, in addition to the `cacerts` certificate store, you must import the certificate into the following certificate store: *WEBSPHERE_HOME*/etc/DummyServerTrustFile.jks
JBoss Application Server	*JAVA_HOME*/jre/lib/security/cacerts
Oracle Application Server	*ORACLE_HOME*/jdk/jre/lib/security/cacerts

4. To confirm whether or not the certificate has been imported successfully, enter a command similar to the following:

   ```
   keytool -list -alias ALIAS -keystore MY_CACERTS -storepass PASSWORD
   ```

   For example:

   ```
   keytool -list -alias MyAlias -keystore C:\mydir\java\jre\lib\security\cacerts
   -storepass changeit
   ```

5. For a nonclustered configuration of IBM WebSphere Application Server, download the `jsse.jar` file from the Sun Web site and copy this file into the *WEBSPHERE_HOME*`/java/jre/lib/ext` directory.
6. For a clustered configuration of IBM WebSphere Application Server, download the `jnet.jar`, `jsse.jar`, and `jcert.jar` files from the Sun Web site and copy these files into the *WEBSPHERE_HOME*`/java/jre/lib/ext` directory.

2.7.4 Enabling SSL Communication on Sun Java System Directory

To enable SSL communication on Sun Java System Directory:

1. Log in to the Sun One Server Console by using administrator credentials.

2. Expand the host name folder.
3. Expand **Server Group**.
4. Select Directory Server, and then click **Open** on the right pane.
5. On the Configuration tab, select the **Encryption** tab.
6. Select **Enable SSL for this server**.
7. Select **Use this cipher family RSA**.
8. Select **Certificate**, and then click **Save**.
9. Restart Sun Java System Directory.

Determining the Port Number for SSL Communication with LDAP

To determine the port number for SSL communication with LDAP, perform the following steps:

1. Log in to Sun Java System Directory.
2. Click the **Configuration** tab, and then the **Network** tab.

The Secure Port number that is displayed is the SSL port number.

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.

3.1 Configuring Reconciliation of Users

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:

Note: By default, the target system server has a limitation on the maximum number of users whose data can be reconciled. If you want to reconcile user data in bulk amounts exceeding the maximum limit allowed by the target system server, then perform the following:

1. Open the Sun ONE Directory Server console.
2. Click the **Configuration** tab.
3. Select **Performance** on the left panel. On the Client Control tab, select the **Unlimited** check boxes for the Size limit and Look-through limit fields.

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

3.1.1 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 a value for the `searchfilter` attribute while configuring the scheduled task for user reconciliation.

You can use the Sun Java System Directory attributes to build a query condition. You specify this query condition as the value of the `searchfilter` attribute.

The following are sample query conditions that can be specified as the value of the `searchfilter` attribute:

- `(&(objectClass=inetOrgPerson)(givenname=John))`
- `(&(objectClass=inetOrgPerson)(sn=Doe))`
- `(&(&(sn=Doe)(givenname=John))(objectClass=inetOrgPerson))`
- `(|(|(sn=lastname)(givenname=firstname))(objectClass=inetOrgPerson))`

Other target system attributes, such as `cn`, `uid`, and `mail`, can also be used to build the query condition.

When you specify a value for the `searchfilter` attribute, then only the records that meet *both* of the following criteria are reconciled:

- Records that meet the matching criteria specified by the `searchfilter` attribute
- Records that are added or updated after the time-stamp value specified by the time-stamp IT resource parameter

Note: As mentioned earlier in the guide, the value of the time-stamp IT resource parameter is automatically updated by Oracle Identity Manager. You must not change the value of this parameter.

The following are guidelines to be followed while specifying a value for the `searchfilter` attribute:

- For the Sun Java System Directory attributes, you must use the same case (uppercase or lowercase) as given in the target system. This is because 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.
- You must not include special characters other than the equal sign (=), ampersand (&), vertical bar (|), and parentheses (()) in the query condition.

Note: An exception is thrown if you include special characters other than the ones specified here.

As mentioned earlier in this section, you specify a value for the `searchfilter` attribute while configuring the scheduled task for user reconciliation.

3.1.2 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 use the `BatchSize` user reconciliation scheduled task attribute. This attribute is used to specify the number of records that must be included in each batch fetched from the target system.

Note:

You must specify a numeric value for the `BatchSize` attribute.

If you specify 0 as the value, then all records are fetched from the target system. In other words, batched reconciliation is not performed.

Caution: For reconciliation of deleted users, you must accept the default value of `0`. If you change this value, then records of existing users will be deleted from Oracle Identity Manager.

You specify a value for the `BatchSize` attribute while performing the procedure 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

3.1.3 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 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.

Note: 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 opening 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.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML File" section on page 2-9, 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 `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, 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 of Users" section on page 3-10.

3.1.4.1 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
- Group and Role Reconciliation Scheduled Task

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task

The following scheduled tasks are used for lookup fields reconciliation:

- `iPlanet Organization Lookup Reconciliation`
- `iPlanet Role Lookup Reconciliation`
- `iPlanet Group Lookup Reconciliation`

You must specify values for the attributes of these scheduled tasks. The following table describes these attributes:

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 is 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=corp,dc=myorg,dc=com`

Attribute	Description	Default/Sample Value
ObjectClass	Name of the object class	The value is 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
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=corp,dc=myorg,dc=com
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 is one of the following: ■ For group and role lookup reconciliation: cn ■ For organization lookup reconciliation: o ■ For organizational unit lookup reconciliation: ou
ConfigurationLookup	Name of the lookup definition that stores configuration information used during connector operations Do not change the default value.	IPNT.Parameter

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

3.1.4.1.2 User Reconciliation Scheduled Task

The following scheduled tasks are used for user reconciliation:

- iPlanet User Trusted Recon Task
- iPlanet User Target Recon Task
- iPlanet Target Delete User Recon Task

- iPlanet Trusted Delete User Recon Task

You must specify values for the attributes of these scheduled tasks. The following table describes these attributes:

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
BatchSize	This attribute is used for batched reconciliation. It specifies the number of records that must be included in each batch. **Caution:** For reconciliation of deleted users, you must accept the default value of 0. If you change this value, then records of existing users will be deleted from Oracle Identity Manager. **See Also:** The "Batched Reconciliation" section on page 3-3	Default value: 0
ConfigurationLookup	Name of the lookup definition that stores configuration information used during connector operations Do not change the default value.	IPNT.Parameter
ITResourceName	Name of the IT resource for setting up a connection with Sun Java System Directory	iPlanet User
Organization	Name of the organization in Oracle Identity Manager to which you want to reconcile users **Note:** This attribute is specific to the iPlanet User Trusted Recon Task scheduled task.	Xellerate Users
Role	Name of the role in Oracle Identity Manager that you want to assign to newly reconciled users **Note:** This attribute is specific to the iPlanet User Trusted Recon Task scheduled task.	Consultant
SearchBase	DN in which the search for user accounts is rooted in **Note:** For the iPlanet Target Delete User Recon Task and iPlanet Trusted Delete User Recon Task scheduled tasks, ensure that the value of this attribute is the root context.	ou=myou,dc=corp,dc=com or dc=corp, dc=com
SearchFilter	LDAP search filter used to locate an organization accounts See "Partial Reconciliation" for more information.	(objectClass=inetOrgPerson)
SearchScope	Search scope used to locate user accounts **Note:** For the iPlanet Target Delete User Recon Task and iPlanet Trusted Delete User Recon Task scheduled tasks, ensure that the value of this attribute is subtree.	subtree or onelevel

Attribute	Description	Default/Sample Value
TrustedResourceObjectName	Name of the resource object for trusted source user reconciliation and deleted user reconciliation **Note:** This attribute is specific to the iPlanet User Trusted Recon Task and iPlanet Trusted Delete User Recon Task scheduled tasks.	Xellerate User
TargetResourceObjectName	Name of the resource object for target resource user reconciliation and deleted user reconciliation **Note:** This attribute is specific to the iPlanet User Target Recon Task and iPlanet Target Delete User Recon Task scheduled tasks.	iPlanet User

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

3.1.4.1.3 Group and Role Reconciliation Scheduled Task

The following scheduled tasks are used for group and role reconciliation:

- iPlanet Group Recon Task
- iPlanet Role Recon Task

You must specify values for the attributes of these scheduled tasks. The following table describes these attributes:

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
ConfigurationLookup	Name of the lookup definition that stores configuration information used during connector operations Do not change the default value.	IPNT.Parameter
Field Lookup Code	Name of the lookup definition that stores reconciliation field mappings for group or role connector operations Provide the corresponding reconciliation look up mappings	Lookup.iPlanetRoleReconciliation.FieldMap Lookup.iPlanetGroupReconciliation.FieldMap
isRoleRecon	Specifies if the recon is group or role reconciliation If it is group recon it is no. But, if it is role recon it is yes.	Yes/No
ITResourceName	Name of the IT resource for setting up a connection with Sun Java System Directory	iPlanet User
MultiValued Attributes	Set of multivalued attributes are added here separated by the | operator **Example:** <phones|pager>	None

Attribute	Description	Default/Sample Value
ResourceObjectName	Name of the resource object for reconciliation of Group or Role	iPlanet Role/iPlanet Group
SearchBase	DN in which the search for Group or Role is rooted in	ou=myou,dc=corp,dc=com or dc=corp, dc=com
SearchFilter	LDAP search filter used to locate Group or Role	(objectClass=groupOfUniqueNames)/ (objectClass=ldapsubentry)

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**.

3.2 Configuring Provisioning of Users

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

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

3.2.1 Compiling Adapters

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

You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-5.

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 Common Name 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
- iPlanet Add Multivalue Attribute
- iPlanet Remove Multivalue Attribute
- iPlanet Update Multivalue Attribute
- Update iPlanet Group Attributes
- Update iPlanet Role Attributes
- iPlanet Move Group
- iPlanet Move Role

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.

3.2.2 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

3.2.3 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.

     The default settings to enable provisioning of Groups in organizational units in the **AtMap.iPlanetGroup** lookup definition are listed in the following table:

Code Key	Decode
ldapGroupObjectClass	groupOfUniqueNames
ldapGroupDNPrefix	cn
Group Name	cn
ldapGroupName	cn
ldapOrgDNPrefix	ou
ldapObjectClass	objectclass
nsuniqueid	nsuniqueid

   - Select the role option if you want to create a group.

     The default settings to enable provisioning of Roles in organizational units in the **AttrMap.iPlanetRole** lookup definition are listed in the following table:

Code Key	Decode
ldapRoleObjectClass	ldapsubentry
ldapRoleDNPrefix	cn
Role Name	cn
ldapRoleName	cn
ldapOrgDNPrefix	ou
ldapObjectClass	objectclass
nsuniqueid	nsuniqueid

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.

3.3 Adding New Attributes for Target Resource Reconciliation

By default, the attributes listed in the "Reconciled Resource Object Fields" section are mapped for reconciliation between Oracle Identity Manager and the target system. With this patch, if required, you can map additional attributes for reconciliation.

> **See Also:** *Oracle Identity Manager Design Console* for detailed instructions on performing the following procedure

To add a custom attribute for reconciliation:

1. While performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-2 section, you create an ACI for the user account. You must add the attribute to the ACI as follows:
   a. Log in to the Sun One Server Console by using administrator credentials.
   b. Expand the host name folder.
   c. Expand **Server Group**.
   d. Select **Directory Server**, and then click **Open** on the right pane.
   e. On the Directory tab, right-click the root context.
   f. From the shortcut menu, click **Set Access Permissions**.
   g. In the Manage Access Control dialog box, select the name of the ACI that you create for the user account and then click **Edit**.

      The ACI that you create for the user account is displayed.
   h. Add the attribute to the list of attributes displayed in the ACI. Use two vertical bars as the delimiter.

      In the following sample ACI, the passportnumber attroibute has been added to the ACI:

      ```
      (targetattr = "passportnumber || physicalDeliveryOfficeName || homePhone ||
      preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
      internationaliSDNNumber || owner || postalAddress || roomNumber ||
      givenName || carLicense || userPKCS12 || searchGuide || userPassword ||
      teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
      userSMIMECertificate || displayName || destinationIndicator || telexNumber
      || employeeNumber || secretary || uid || userCertificate || st || sn ||
      description || mail || labeledUri || businessCategory || homePostalAddress
      || x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou ||
      nsAccountLock || seeAlso || registeredAddress || postalCode || photo ||
      title || uniqueMember || street || pager || departmentNumber || dc || o ||
      cn || l || initials || telephoneNumber || preferredLanguage ||
      facsimileTelephoneNumber || x121Address || employeeType") (version 3.0;acl
      "OIMUserACI";allow (read,write,delete,add)(userdn = "ldap:/// uid=OIMAdmin,
      ou=Org1, dc=corp,dc=oracle,dc=com ");)
      ```

   i. Click **OK**.
2. Determine the target system name for the attribute that you want to add as follows:

a. Log in to the target system.

b. On the Configuration tab of the user interface, click **Schema**.

c. Select the object class with which you want to perform reconciliation.

d. Search for the attribute that you want to add and record the name of the attribute. Later in this procedure, you enter this name while creating a lookup definition entry for the attribute.

3. Log in to the Oracle Identity Manager Design Console.

4. Add the new attribute on the process form as follows:

a. Open the Form Designer form.

b. Search for and open the **UD_IPNT_USR** form.

c. Create a new version of the form.

d. Add the new attribute on the form.

e. Save and close the form.

5. In the lookup definition for reconciliation, create an entry for the new attribute as follows:

a. Open the Lookup Definition form.

b. Search for and open the **AttrName.Recon.Map.iPlanet** lookup definition.

c. In the lookup definition, create an entry for the attribute that you want to add:

– Code Key: Enter the name of the attribute that you add on the process form.

– Decode Key: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

d. In the lookup definition, add the custom object class (containing the attribute) to the existing value of the `ldapUserObjectClass` attribute. For example, if the new attribute is in the accountdetails object class, then the value of the `ldapUserObjectClass` attribute must be set to:

```
<inetorgperson|accountdetails>
```

In general, the format of the `ldapUserObjectClass` attribute value must be as follows:

```
<inetorgperson|customObjectClass1|customObjectClass2| . . .
customObjectClassn>
```

6. In the resource object, add a reconciliation field for the attribute as follows:

a. Open the Resource Objects form.

b. Search for the **iPlanet User** process.

c. On the Reconciliation Fields subtab of the Object Reconciliation tab, create an entry for the attribute.

7. In the process definition, create a reconciliation field mapping for the attribute as follows:

a. Open the Process Definition form.

b. Search for the **iPlanet User** process.

c. On the Reconciliation Field Mappings tab, create a reconciliation field mapping for the attribute.

3.4 Adding New Attributes for Group or Role Reconciliation

By default, the attributes listed in the "Reconciled Resource Object Fields" section are mapped for reconciliation between Oracle Identity Manager and the target system. With this patch, if required, you can map additional attributes for reconciliation.

See Also: *Oracle Identity Manager Design Console* for detailed instructions on performing the following procedure

To add a custom attribute for reconciliation:

1. While performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-2, you create an ACI for the user account. You must add the attribute to the ACI as follows:
   a. Log in to the Sun One Server Console by using administrator credentials.
   b. Expand the host name folder.
   c. Expand **Server Group**.
   d. Select **Directory Server**, and then click **Open** on the right pane.
   e. On the Directory tab, right-click the root context.
   f. From the shortcut menu, click **Set Access Permissions**.
   g. In the Manage Access Control dialog box, select the name of the ACI that you create for the user account and then click **Edit**.

      The ACI that you create for the user account is displayed.
   h. Add the attribute to the list of attributes displayed in the ACI. Use two vertical bars as the delimiter.

      In the following sample ACI, the passportnumber attroibute has been added to the ACI:

      ```
      (targetattr = "passportnumber || physicalDeliveryOfficeName || homePhone ||
      preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
      internationaliSDNNumber || owner || postalAddress || roomNumber ||
      givenName || carLicense || userPKCS12 || searchGuide || userPassword ||
      teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
      userSMIMECertificate || displayName || destinationIndicator || telexNumber
      || employeeNumber || secretary || uid || userCertificate || st || sn ||
      description || mail || labeledUri || businessCategory || homePostalAddress
      || x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou ||
      nsAccountLock || seeAlso || registeredAddress || postalCode || photo ||
      title || uniqueMember || street || pager || departmentNumber || dc || o ||
      cn || l || initials || telephoneNumber || preferredLanguage ||
      facsimileTelephoneNumber || x121Address || employeeType") (version 3.0;acl
      "OIMUserACI";allow (read,write,delete,add)(userdn = "ldap:/// uid=OIMAdmin,
      ou=Org1, dc=corp,dc=oracle,dc=com ");)
      ```

   i. Click **OK**.
2. Determine the target system name for the attribute that you want to add as follows:
   a. Log in to the target system.

b. On the Configuration tab of the user interface, click **Schema**.

c. Select the object class with which you want to perform reconciliation.

d. Search for the attribute that you want to add and record the name of the attribute. Later in this procedure, you enter this name while creating a lookup definition entry for the attribute.

3. Log in to the Oracle Identity Manager Design Console.

4. Add the new attribute on the process form as follows:

a. Open the Form Designer form.

b. Do one of the following:

Search for and open the **UD_IPNT_GR** form for Group Recon.

Search for and open the **UD_IPNT_RL** form for Role Recon.

c. Create a new version of the form.

d. Add the new attribute on the form.

e. Save and close the form.

5. In the lookup definition for reconciliation, create an entry for the new attribute as follows:

a. Open the Lookup Definition form.

b. Do one of the following:

Search for and open the **Lookup.iPlanetGroupReconciliation.FieldMap** lookup definition for Group Recon.

Search for and open the **Lookup.iPlanetRoleReconciliation.FieldMap** lookup definition for Role Recon.

c. In the lookup definition, create an entry for the attribute that you want to add:

– Code Key: Enter the name of the attribute that you add on the process form.

– Decode Key: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

6. In the resource object, add a reconciliation field for the attribute as follows:

a. Open the Resource Objects form.

b. Do one of the following:

Search for the **iPlanet Group** process.

Search for the **iPlanet Role** process.

c. On the Reconciliation Fields subtab of the Object Reconciliation tab, create an entry for the attribute.

7. In the process definition, create a reconciliation field mapping for the attribute as follows:

a. Open the Process Definition form.

b. Do one of the following:

Search for the **iPlanet Group** process.

Search for the **iPlanet Role** process.

c. On the Reconciliation Field Mappings tab, create a reconciliation field mapping for the attribute.

3.5 Adding New Attributes for Trusted Source Reconciliation

Note:

- You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.
- If you want to add a multivalued attribute for target resource reconciliation, then see "Adding New Multivalued Attributes for Target Resource Reconciliation" on page 3-19.

By default, the attributes listed in the "Reconciled Xellerate User (OIM User) Fields" section 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: *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the OIM User process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **Users** process form.
   d. Click **Add**.
   e. Enter the details of the attribute.

      For example, if you are adding the Title attribute, then enter `Employee ID` in the **Name** field, set the data type to **String**, enter `Title` as the column name, and enter a field size value.
   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 `Title` in the **Field Name** field and select **String** from the Field Type list.

      Later in this procedure, you will enter the attribute name as the Decode value of the entry that you create in the lookup definition for reconciliation.

f. Click **Save**.

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 `Title = Title`.

   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 **AttrName.Recon.Map.iPlanet** 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 `Title` in the **Code Key** field and then enter `title` in the **Decode** field.

   e. Click **Save**.

   f. Select **Field Type**, and then click **Save**.

3.6 Adding New Multivalued Attributes for Target Resource Reconciliation

Note: You must ensure that 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 multivalued attributes Role and Group are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for target resource reconciliation.

To add a new multivalued attribute for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.

2. Create a form for the multivalued attribute as follows:

   a. Expand **Development Tools**.

   b. Double-click **Form Designer**.

   c. Create a form by specifying a table name and description, and then click **Save**.

   d. Click **Add** and enter the details of the attribute.

e. Click **Save** and then click **Make Version Active.**

3. Add the form created for the multivalued attribute as a child form of the process form as follows:

   a. Search for and open the **UD_IPNT_USR** process form.

   b. Click **Create New Version**.

   c. Click the **Child Table(s)** tab.

   d. Click **Assign**.

   e. In the Assign Child Tables dialog box, select the newly created child form, click the right arrow, and then click **OK**.

   f. Click **Save** and then click **Make Version Active.**

4. 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 **IPlanet User** resource object.

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

   e. In the Add Reconciliation Fields dialog box, enter the details of the attribute.

      For example, enter `carLicense` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

   f. Click **Save** and then close the dialog box.

   g. Right-click the newly created attribute.

   h. Select **Define Property Fields**.

   i. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

      For example, enter `Mailing Address` in the Field Name field and select **String** from the Field Type list.

   j. Click **Save**, and then close the dialog box.

5. Create a reconciliation field mapping for the new attribute as follows:

   a. Expand **Process Management**.

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

   c. Search for and open the **iPlanet User** process definition.

   d. On the Reconciliation Field Mappings tab of the `iPlanet User` process definition, click **Add Table Map**.

   e. In the Add Reconciliation Table Mapping dialog box, select the field name and table name from the list, click **Save**, and then close the dialog box.

   f. Right-click the newly created field, and select **Define Property Field Map**.

   g. In the **Field Name** field, select the value for the field that you want to add.

   h. Double-click the **Process Data Field** field, and then select **UD_ADDRESS**.

   i. Select **Key Field for Reconciliation Field Matching** and click **Save**.

6. 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 **AttrName.Recon.Map.iPlanet** lookup definition.

   d. In the Decode column for the **ldapMultiValAttr** Code Key, enter the field name and code key separated by a semicolon. Field Name and Code Key pairs are separated by vertical bars.

      For example, if `Mailing Address` is the attribute name, then append the following to the entry in the Decode column of the **ldapMultiValAttr** Code Key:

      ```
      |Mailing Address;Mailing Address
      ```

      As shown in this example, the vertical bar is used to separate field name and Code Key pairs and a semicolon is used to separate the Field Name and Code Key.

   e. Click **Add**, enter the Code Key and Decode values for the attribute, and then click **Save**. The Code Key value must be the name of the attribute on the process form. The Decode value must be the name of the attribute on the target system.

      For example, enter `PostalAddress` in the Code Key column and then enter `postaladdress` in the Decode field.

3.7 Adding New Attributes for Provisioning

By default, the attributes listed in the "Provisioning Module" section of the connector guide are mapped for provisioning between Oracle Identity Manager and the target system. With this patch, if required, you can map additional attributes for provisioning.

> **See Also:** *Oracle Identity Manager Design Console* for detailed instructions on performing the following procedure

To add a new attribute for provisioning:

1. While performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-2, you create an ACI for the user account. You must add the attribute to the ACI as follows:

   a. Log in to the Sun One Server Console by using administrator credentials.

   b. Expand the host name folder.

   c. Expand **Server Group**.

   d. Select **Directory Server**, and then click **Open** on the right pane.

   e. On the Directory tab, right-click the root context in which created the user account for connector operations.

   f. From the shortcut menu, click **Set Access Permissions**.

   g. In the Manage Access Control dialog box, select the name of the ACI that you create for the user account and then click **Edit**.

      The ACI that you create for the user account is displayed.

h. Add the attribute to the list of attributes displayed in the ACI. Use two vertical bars as the delimiter.

   In the following sample ACI, the passportnumber attroibute has been added to the ACI:

```
(targetattr = "passportnumber || physicalDeliveryOfficeName || homePhone ||
preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
internationaliSDNNumber || owner || postalAddress || roomNumber ||
givenName || carLicense || userPKCS12 || searchGuide || userPassword ||
teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
userSMIMECertificate || displayName || destinationIndicator || telexNumber
|| employeeNumber || secretary || uid || userCertificate || st || sn ||
description || mail || labeledUri || businessCategory || homePostalAddress
|| x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou ||
nsAccountLock || seeAlso || registeredAddress || postalCode || photo ||
title || uniqueMember || street || pager || departmentNumber || dc || o ||
cn || l || initials || telephoneNumber || preferredLanguage ||
facsimileTelephoneNumber || x121Address || employeeType") (version 3.0;acl
"OIMUserACI";allow (read,write,delete,add)(userdn = "ldap:/// uid=OIMAdmin,
ou=Org1, dc=corp,dc=oracle,dc=com ");)
```

i. Click **OK**.

2. Determine the target system name for the attribute that you want to add as follows:
   a. Log in to the target system.
   b. On the Configuration tab of the user interface, click **Schema**.
   c. Select the object class on which you want to perform provisioning operations.
   d. Search for the attribute that you want to add, and record the name of the attribute. Later in this procedure, you enter this name while creating a lookup definition entry for the attribute.
3. Log in to the Oracle Identity Manager Design Console.
4. Add the new attribute on the process form as follows:
   a. Open the Form Designer form.
   b. Search for and open the **UD_IPNT_USR** form.
   c. Create a new version of the form.
   d. Add the new attribute on the form.
   e. Save and close the form.
5. In the lookup definition for provisioning, create an entry for the new attribute as follows:
   a. Open the Lookup Definition form.
   b. Search for and open the **Attrname.Prov.Map.iPlanet** lookup definition.
   c. In the lookup definition, add an entry for the attribute that you want to add:
      – **Code Key:** Enter the name of the attribute that you add on the process form.
      – **Decode Key:** Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

d. In the lookup definition, add the custom object class (containing the attribute) to the existing value of the `ldapUserObjectClass` attribute. For example, if the new attribute is in the accountdetails object class, then the value of the `ldapUserObjectClass` attribute must be set to:

```
<inetorgperson|accountdetails>
```

In general, the format of the `ldapUserObjectClass` attribute value must be as follows:

```
<inetorgperson|customObjectClass1|customObjectClass2| . . .
customObjectClassn>
```

6. To test whether or not you can use the newly added attribute for provisioning, log in to the Oracle Identity Manager Administrative and User Console and perform a provisioning operation in which you specify a value for the newly added attribute.

Enabling Update of New Multivalued Attributes for Provisioning

After you add a multivalued attribute for provisioning, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new multivalued attribute for provisioning:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management**.
3. Double-click **Process Definition** and open the **iPlanet User** process definition.
4. In the process definition, add a task for setting a value for the attribute:
   a. Click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.
   b. In the Task Properties section, select the following fields:
      – Conditional
      – Required for Completion
      – Allow Cancellation while Pending
      – Allow Multiple Instances
      – Select the child table from the list.

        For the example described earlier, select **Mailing Address** from the list.
      – Select **Insert** as the trigger type for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalues data.
   c. On the **Integration** tab, click **Add**, and then click **Adapter**.
   d. Select the **adpIPLANETADDMULTIVALUEATTRIBUTE** adapter, click **Save**, and then click OK in the message.
   e. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Note: Some of the values in this table are specific to the Mailing Address/Postal Address example. These values must be replaced with values relevant to the multivalued attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response Code	NA	NA	NA
AdminID	String	IT Resources	Server	LDAP Server	Admin Id
AdminPwd	String	IT Resources	Server	LDAP Server	Admin Password
processIntKey	String	Process Data	Process Instance	NA	NA
rootContext	String	IT Resources	Server	LDAP Server	Root DN
SSLFlag	String	IT Resources	Server	LDAP Server	SSL
PropertyName	String	Literal	String	postaladdress **Note:** This is a sample value.	NA
AttrLookupCode	String	IT Resources	Server	LDAP Server	Prov Attribute Lookup Code
LDAPServer	String	IT Resources	Server	LDAP Server	Server Address
Port	String	IT Resources	Server	LDAP Server	Port
PropertyValue	String	Process Data and mailing address	Mailing address **Note:** This is a sample value.	NA	NA
NsuniqueID	String	Process Data	NsuniqueID	NA	NA

f. Click the Save icon and then close the dialog box.

5. In the process definition, add a task for removing the value of the attribute by performing Step 4. While performing Step 4.d, select the **adpIPLANETREMOVEMULTIVALUEATTRIBUTE** adapter.

3.8 Adding New Attributes for Provisioning of Group or Role

By default, the attributes listed in the "Provisioning Module" section of the connector guide are mapped for provisioning between Oracle Identity Manager and the target system. With this patch, if required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:

1. While performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-2, you create an ACI for the user account. You must add the attribute to the ACI as follows:

   a. Log in to the Sun One Server Console by using administrator credentials.

   b. Expand the host name folder.

   c. Expand **Server Group**.

   d. Select **Directory Server**, and then click **Open** on the right pane.

e. On the Directory tab, right-click the root context in which created the user account for connector operations.

f. From the shortcut menu, click **Set Access Permissions**.

g. In the Manage Access Control dialog box, select the name of the ACI that you create for the user account and then click **Edit**.

The ACI that you create for the user account is displayed.

h. Add the attribute to the list of attributes displayed in the ACI. Use two vertical bars as the delimiter.

In the following sample ACI, the passportnumber attroibute has been added to the ACI:

```
(targetattr = "passportnumber || physicalDeliveryOfficeName || homePhone ||
preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
internationaliSDNNumber || owner || postalAddress || roomNumber ||
givenName || carLicense || userPKCS12 || searchGuide || userPassword ||
teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
userSMIMECertificate || displayName || destinationIndicator || telexNumber
|| employeeNumber || secretary || uid || userCertificate || st || sn ||
description || mail || labeledUri || businessCategory || homePostalAddress
|| x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou ||
nsAccountLock || seeAlso || registeredAddress || postalCode || photo ||
title || uniqueMember || street || pager || departmentNumber || dc || o ||
cn || l || initials || telephoneNumber || preferredLanguage ||
facsimileTelephoneNumber || x121Address || employeeType") (version 3.0;acl
"OIMUserACI";allow (read,write,delete,add)(userdn = "ldap:/// uid=OIMAdmin,
ou=Org1, dc=corp,dc=oracle,dc=com ");)
```

i. Click **OK**.

2. Determine the target system name for the attribute that you want to add as follows:

a. Log in to the target system.

b. On the Configuration tab of the user interface, click **Schema**.

c. Select the object class on which you want to perform provisioning operations.

d. Search for the attribute that you want to add, and record the name of the attribute. Later in this procedure, you enter this name while creating a lookup definition entry for the attribute.

3. Log in to the Oracle Identity Manager Design Console.

4. Add the new attribute on the process form as follows:

a. Open the Form Designer form.

b. Do one of the following:

Search for and open the **UD_IPNT_GR** form.

Search for and open the **UD_IPNT_RL** form.

c. Create a new version of the form.

d. Add the new attribute on the form.

e. Save the form.

f. Make the version active, and close the form.

5. In the lookup definition for provisioning, create an entry for the new attribute as follows:
   a. Open the Lookup Definition form.
   b. Do one of the following:

      Search for and open the **AtMap.iPlanetGroup** lookup definition.

      Search for and open the **AttrMap.iPlanetRole** lookup definition.
   c. In the lookup definition, add an entry for the attribute that you want to add:
      – **Code Key:** Enter the name of the attribute that you add on the process form.
      – **Decode Key:** Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.
6. To test whether or not you can use the newly added attribute for provisioning, log in to the Oracle Identity Manager Administrative and User Console and perform a provisioning operation in which you specify a value for the newly added attribute.

Enabling Update of New Attributes for Provisioning of Group or Role

After you add an attribute for provisioning Group or Role, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new multivalued attribute for provisioning:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management**.
3. Do one of the following:
   - Double-click **Process Definition** and open the **iPlanet Group** process definition.
   - Double-click **Process Definition** and open the **iPlanet Role** process definition.
4. In the process definition, add a task for setting a value for the attribute:
   a. Click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.
   b. In the Task Properties section, select the following fields:
      – Conditional
      – Required for Completion
      – Allow Cancellation while Pending
      – Allow Multiple Instances
      – Select the child table from the list.

        For the example described earlier, select **Mailing Address** from the list.
   c. On the **Integration** tab, click **Add**, and then click **Adapter**.
   d. Do one of the following:
      – Select the **adpUPDATEIPLANETGROUPATTRIBUTES** adapter, click **Save**, and then click OK in the message.

– Select the **adpUPDATEIPLANETROLEATTRIBUTES** adapter, click **Save**, and then click OK in the message.

e. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response Code	NA	NA	NA
AdminID	String	IT Resources	Server	LDAP Server	Admin Id
AdminPwd	String	IT Resources	Server	LDAP Server	Admin Password
processIntKey	String	Process Data	Process Instance	NA	NA
rootContext	String	IT Resources	Server	LDAP Server	Root DN
SSLFlag	String	IT Resources	Server	LDAP Server	SSL
PropertyName	String	Literal	String	postaladdress **Note:** This is a sample value.	NA
AttrLookupCode	String	IT Resources	Server	LDAP Server	Prov Attribute Lookup Code
LDAPServer	String	IT Resources	Server	LDAP Server	Server Address
Port	String	IT Resources	Server	LDAP Server	Port
PropertyValue	String	Process Data and mailing address	Mailing address **Note:** This is a sample value.	NA	NA
NsuniqueID	String	Process Data	NsuniqueID	NA	NA

f. Click the Save icon and then close the dialog box.

Enabling Update of New Multivalued Attributes for Provisioning of Group or Role

After you add a multivalued attribute for provisioning Group or Role, you must enable update operations on the attribute.

To update a new multivalued attribute for provisioning of Groups or Roles, perform the steps mentioned in "Adding New Attributes for Provisioning" section.

3.9 Adding New Object Classes

To add a new object class, perform the following procedures:

Note: You must add the mandatory attributes of each object class that you add.

1. Assigning Permissions for Using the Attribute
2. Adding the Attributes of the Object Class to the Process Form
3. Adding the Object Class and its Attributes to the Lookup Definition for Provisioning

4. Adding the Attributes of the Object Class to the Resource Object
5. Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation
6. Adding attributes of the Object Class to the Provisioning Process

3.9.1 Assigning Permissions for Using the Attribute

While performing the procedure described in "Creating a Target System User Account for Connector Operations" on page 2-2, you create an ACI for the user account. You must add the attribute to the ACI as follows:

1. Log in to the Sun One Server Console by using administrator credentials.
2. Expand the host name folder.
3. Expand **Server Group**.
4. Select **Directory Server**, and then click **Open** on the right pane.
5. On the Directory tab, right-click the root context in which you created the user account for connector operations.
6. From the shortcut menu, click **Set Access Permissions**.
7. In the Manage Access Control dialog box, select the name of the ACI that you create for the user account and then click **Edit**.

   The ACI that you create for the user account is displayed.
8. Add the attribute to the list of attributes displayed in the ACI. Use two vertical bars as the delimiter.

   In the following sample ACI, the passportnumber attroibute has been added to the ACI:

```
(targetattr = "passportnumber || physicalDeliveryOfficeName || homePhone ||
preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
internationaliSDNNumber || owner || postalAddress || roomNumber || givenName ||
carLicense || userPKCS12 || searchGuide || userPassword ||
teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
userSMIMECertificate || displayName || destinationIndicator || telexNumber ||
employeeNumber || secretary || uid || userCertificate || st || sn ||
description || mail || labeledUri || businessCategory || homePostalAddress ||
x500UniqueIdentifier || modifyTimestamp || postOfficeBox || ou || nsAccountLock
|| seeAlso || registeredAddress || postalCode || photo || title || uniqueMember
|| street || pager || departmentNumber || dc || o || cn || l || initials ||
telephoneNumber || preferredLanguage || facsimileTelephoneNumber || x121Address
|| employeeType") (version 3.0;acl "OIMUserACI";allow
(read,write,delete,add)(userdn = "ldap:/// uid=OIMAdmin, ou=Org1,
dc=corp,dc=oracle,dc=com ");)
```

9. Click **OK**.

3.9.2 Adding the Attributes of the Object Class to the Process Form

To add the attributes of the object class to the process form:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Development Tools** folder.
3. Double-click **Form Designer.**

4. Search for and open the **UD_IPNT_USR** process form.
5. Click **Create New Version,** and then click **Add.**
6. Enter the details of the attribute.

   For example, if you are adding the Associated Domain attribute, enter `UD_IPNT_USR_ASSOCIATEDDOMAIN` in the **Name** field and then enter the other details of this attribute.
7. Click **Save,** and then click **Make Version Active.**

3.9.3 Adding the Object Class and its Attributes to the Lookup Definition for Provisioning

To add the object class and its attributes to the lookup definition for provisioning:

1. Expand the **Administration** folder.
2. Double-click **Lookup Definition.**
3. Search for and open the **AttrName.Prov.Map.iPlanet** lookup definition.
4. Add the object class name to the Decode value of the ldapUserObjectClass Code Key.

   Note: In the Decode column, use the vertical bar (`|`) as a delimiter when you add the object class name to the existing list of object class names.

   For example, if you want to add `MyObjectClass` in the Decode column then enter the value as follows:

   ```
   inetorgperson|MyObjectClass
   ```

5. Click **Add** and then enter the Code Key and Decode values for an attribute of the object class. The Code Key value must be the name of the field on the process form and Decode value must be the name of the field on the target system.

   For example, enter `Associated Domain` in the Code Key field and then enter `associatedDomain` in the Decode field.

   Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

6. Click **Save.**

3.9.4 Adding the Attributes of the Object Class to the Resource Object

To add the attributes of the object class to the resource object:

Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

1. Expand the **Resource Management** folder.
2. Double-click **Resource Objects.**
3. Search for and open the **iPlanet User** resource object.
4. For each attribute of the object class:
   a. On the Object Reconciliation tab, click **Add Field.**
   b. Enter the details of the field.

   For example, enter `Associated Domain` in the **Field Name** field and select **String** from the Field Type list.
5. Click the save icon.

3.9.5 Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation

To add the object class and its attributes to the lookup definition for reconciliation, perform all the instructions given in the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section on the **AttrName.Recon.Map.iPlanet** lookup definition. In other words, while performing Step 3 of the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section, search for and open the **AttrName.Recon.Map.iPlanet** lookup definition instead of the **AttrName.Prov.Map.iPlanet** lookup definition.

While performing Step 5 of the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section, note that the Code Key value must be the name of the reconciliation field in the iPlanet User resource object and Decode value must be the name of the field on the target system. For example, enter `Associated Domain` in the Code Key field and then enter `associatedDomain` in the Decode field.

3.9.6 Adding attributes of the Object Class to the Provisioning Process

To add the attributes of the object class to the provisioning process:

Note: You must perform this step for all the mandatory attributes of the object class. You can also perform this step for the optional attributes.

1. Expand the **Process Management** folder.
2. Double-click **Process Definition.**
3. Search for and open the **iPlanet User** provisioning process.
4. On the Reconciliation Field Mappings tab, click **Add Field Map.**
5. In the **Field Name** field, select the value for the field that you want to add.

   For example, select `Associated Domain = UD_IPNT_USR_ASSOCIATEDDOMAIN`
6. In the **Field Type** field, select the field type.
7. Click the save icon.

3.10 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 Example 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 create and configure one IT resource for each installation of the target system.

The IT Resources form is in the Resource Management folder. The `iPlanet User Resource` 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.

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the target system installation to which you want to provision the user.

Similarly, to reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the `ITResource` scheduled task attribute.

3.11 Guidelines to Be Applied While Using the Connector

Apply the following guidelines to while using the connector:

- If you have configured Sun Java System Directory for target resource 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 have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

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

4.1 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. Copy the contents of the `test` directory on the installation media, to the *`OIM_HOME`*`/xellerate/SJSDS/test/troubleshoot` directory.
2. Specify values for the parameters in the `TroubleShootIPlanet.properties` file.

   This file is in the *`OIM_HOME`*`/xellerate/SJSDS/test/troubleshoot` 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 These parameters are the same as the parameters of the IT resource that you configure by performing the procedure described earlier in this guide.
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

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

   ```
   OIM_HOME/xellerate/JavaTasks/SJSDSProv.jar
   OIM_HOME/xellerate/lib/xlLogger.jar
   OIM_HOME/xellerate/ext/log4j-1.2.8.jar
   OIM_HOME/xellerate/lib/xlUtils.jar
   ```

4. 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/SJSDS/test/troubleshoot`

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.

5. 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
     ```

4.2 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

4.2.1 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.

4.2.2 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.
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.

Problem Description	Solution
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.

4.2.3 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.
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.

Problem Description	Solution
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.
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.

Problem Description	Solution
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.

4.2.4 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.

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

- **Bug 7386568**

  When assigning roles to a user at the time of user creation, in the target system, the value of "ou" in the entrydn attribute changes to lower case. However, lookup value for Organization is case-sensitive, and as a result the reconciliation role is not updated in the Resource Object form.

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

Oracle Identity Manager Attribute	Sun Java System Directory Attribute	Description
Location	l	City of office address
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

L

M

O

P

R

S

T

U

X