Oracle® Identity Manager

Connector Guide for Sun Java System Directory

Release 9.0.4

E10446-13

September 2013

ORACLE®

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

E10446-13

Primary Author: Gauhar Khan

Contributing Authors: Debapriya Datta, Prakash Hulikere, Devanshi Mohan, Alankrita Prakash, Deena Purushothaman

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Sun Java System Directory.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

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

For generic information about connectors, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manage*r.

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

http://download.oracle.com/docs/cd/E14571_01/im.htm

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://download.oracle.com/docs/cd/E22999_01/index.htm

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 release 9.0.4.15 of the Sun Java System Directory connector.

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 software updates:

- 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 9.0.4.11
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.15

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 Reconciliation
- Adding New Attributes for Provisioning
- Adding New Object Classes for Reconciliation and Provisioning

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 "Limited 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 2-4 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
- Resolved Issues

Using the Connector Installer

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

See "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" 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 2-6 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
- No Support for Dual Mode Reconciliation
- Resolved Issues

Support for New Target System Version

Sun ONE Directory Server 6.3 has been added to the list of certified target system versions. See "Certified Components" 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 was populated with the organization name.
	Because provisioning was based on the Decode value, 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 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.

Software Updates in Release 9.0.4.11

The following are software updates in release 9.0.4.11:

- Support for Creating Copies of Connector Objects
- Enhanced Logging

- Resolved Issues

Support for Creating Copies of Connector Objects

To meet the requirements of specific use cases, you might need to create multiple copies of the Oracle Identity Manager objects that constitute the connector. The connector can work with multiple instances of these objects.

See Section 4.11, "Configuring the Connector for Multiple Installations of the Target System" for more information.

Enhanced Logging

The logging feature has been enhanced to include the exception stack trace in this release.

Resolved Issues

The following are issues resolved in release 9.0.4.11:

Bug Number	Issue	Resolution
9060464	When organizations were reconciled into Oracle Identity Manager from the target system, the decode values was truncated from the `Organization DN` that resulted in multiple organizations having the same name. For example: `ou=people,l=NA,dc=arrow,dc=com and ou=people,l=asia,dc=arrow,dc=com` Here, the organization name is `people` in both cases. Therefore, correct organization could not be added while creating users.	This issue has been resolved. The connector now supports the reconciliation of complete DN of the Organization Unit while performing lookup reconciliation. Therefore, you can now add the appropriate organization while creating users.
9030736	There was a mismatch of lookup values with the Code Key values and variables while provisioning a user to the Dar (Sun) directory, after the connector installation.	This issue has been resolved. The connector now supports separate lookup definitions for constants and configuration items.
8678353	The connector supported a password field length of 15 characters only. As a result, provisioning failed whenever the length of the password field exceeded 15 characters.	This issue has been resolved. The connector now supports password field length up to 200 characters. This in turn, enables you to provision the password field with value greater than 15 characters.
8597131	The `Organization DN` value on the process form did not map with the value of `Organization Unit` attribute of the target system.	This issue has been resolved. The `Organization DN` field on the process form has been renamed to `Container DN`. The `Container DN` field holds the value of the container in which the user exists.

Bug Number	Issue	Resolution
9243262	The connector ignored the value of `AttrType` parameter when the lookup was populated. The Code Key and Decode value was always populated with the same data, `DN`, even if for example the AttrType parameter was set to `cn`.	This issue has been resolved. The AttrType parameter in the scheduled task is renamed to `AttrName` to fetch the Decode value from the lookup.
9268648	In earlier release, all the active users present in the target system were searched and compared with active OIM Users. The OIM users which were missing were deleted. The delete reconciliation functionality failed when it was run for multiple installations of the iPlanet target system.	This issue has been resolved. The delete reconciliation functionality is now implemented with retro change log plug-in, which stores all the modified entries under `changelog`.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning
- Support for New Target System Version

Support for New Oracle Identity Manager Release

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

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

Support for Request-Based Provisioning

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

See Section 3.6.1.2, "Request-Based Provisioning" for more information.

Support for New Target System Version

Sun Java System Directory Server Enterprise Edition 7.0 has been added to the list of certified target system versions. See Section 1.1, "Certified Components" for information about the full list of certified target system versions.

Software Updates in Release 9.0.4.15

The following are software updates in release 9.0.4.15:

- Support for Connection Pooling
- Support for Importing Request Dataset XML Files
- Resolved Issues

Support for Connection Pooling

The connector supports the connection pooling feature introduced in Oracle Identity Manager release 9.1.0.2. In earlier releases, a connection with the target system was

established at the start of a reconciliation run and closed at the end of the reconciliation run. With the introduction of connection pooling, multiple connections are established by Oracle Identity Manager and held in reserve for use by the connector.

Support for Importing Request Dataset XML Files

From this release onward, the connector provides support for importing a request dataset XML file into Oracle Identity Manager by using the Deployment Manager on Oracle Identity Manager 11*g* release 1 (11.1.1.3).

The installation media of this release includes a request dataset file, SJSDSConnectorRequestDatasets.xml, which is available in the xml directory.

See Section 2.3.1.7.1, "Importing Request Datasets Using Deployment Manager" for more information.

Resolved Issues

The following are issues resolved in release 9.0.4.15:

Bug Number	Issue	Resolution
9299541	The connector did not use the time-stamp format specified in the `TARGET_TIMESTAMP_SEARCHFORMAT` parameter in the `IPNT.Parameter` lookup definition.	This issue has been resolved. The connector now uses the time-stamp format specified in the TARGET_TIMESTAMP_SEARCHFORMAT parameter.
9350018	The `modifyTimestamp` attribute was included in the software code.	This issue has been resolved. The `modifyTimestamp` attribute is now removed in the software code.
9892920	Reconciliation of disabled accounts did not work.	This issue has been resolved. The connector now supports reconciliation of disabled accounts.
9444122	The iPlanet Role Recon Task scheduled task did not work in SSL mode.	This issue has been resolved. The connector now supports iPlanet Role Recon Task in SSL mode.
12989431	LDAP user creation failed if there were more than eight characters in the middle name of the user.	This issue has been resolved. Creating or updating a user does not fail if there are more than eight characters in the middle name of the user.
13006479	The logging of operations duing connection pooling was not satisfactory.	This issue has been resolved. The logging for the connection pooling feature has been enhanced.
12916335	The request dataset XML file did not specify the required attributes during request-based provisioning.	This issue has been resolved. The User ID, Last Name, and Common Name fields are now marked mandatory during request-based provisioning.
12881318	During the provisioning of roles and groups, the organization name was populated inappropriately.	This issue has been resolved. During provisioning, only the role names and the group names are populated.
11799031	During a lookup reconciliation operation of a group, an organization, or a role, an error was encountered.	This issue has been resolved. A lookup reconciliation of a group, an organization, or a role is successful.

Bug Number	Issue	Resolution
10351023	The `Organization DN` field was not available for mapping on the iPlanet process forms.	This issue has been resolved. The `Organization DN` field is available for mapping on the iPlanet process forms.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates from Release 9.0.4 Through 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.11
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.15

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 Apply 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 Reconciliation
  - Adding New Attributes for Provisioning
  - Adding New Object Classes for Reconciliation and Provisioning

Documentation-Specific Updates in Release 9.0.4.3

The following are documentation-specific updates in release 9.0.4.3:

- In the "Certified Languages" 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 "Extending the Functionality of 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.

Documentation-Specific Updates in Release 9.0.4.11

Major changes have been made to the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of the information provided by the guide.

Documentation-Specific Updates in Release 9.0.4.12

The following is a documentation-specific update in release 9.0.4.12:

- The following information that was documented as a guideline in the "Guidelines to Apply While Using the Connector" section has been moved to the "Known Issues" chapter:

  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.
- Section 1.3, "Connector Architecture" has been modified.
- Section 3.5.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.3.x" has been added.
- The "Attribute Mappings Between Oracle Identity Manager and Sun Java System Directory" appendix has been removed.

Documentation-Specific Updates in Release 9.0.4.15

The following are the documentation-specific updates for this release of the connector.

- Section 2.3.1.7.2, "Copying Predefined Request Dataset" has been updated with the new dataset XML files.
- Table 2–1, " Files and Directories on the Installation Media" has been updated for XML files.
- Section 2.2.1.2, "Configuring the IT Resource" has been updated for missing parameters.

- In Section 2.3.2, "Configuring SSL," a note on deployment procedure has been removed.
- In Section 2.1, "Preinstallation,"
  a note on deployment procedure has been added.
- In Section 2.2, "Installation,"
  a note on deployment procedure has been added.
- In Section 2.3, "Postinstallation,"
  a note on deployment procedure has been added.
- Section 4.7, "Adding New Multivalued Attributes for Provisioning"
  has been added.
- Section 5.2.6, "Logging Errors"
  has been added to Section 5.2, "Troubleshooting Connector Problems."
- The following changes have been made to Section 2.3.1.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1," in the procedure for enabling logging in Oracle WebLogic Server:
  - The "Logger Name" entry has been modified in Step 1.a and Step1.b.
  - A note has been added after Step 4.

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

1.1 Certified Components

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

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.3.2 or later **Note:** In this guide, **Oracle Identity Manager release 9.0.3.*x*** has been used to denote Oracle Identity Manager release 9.0.3.2 and later releases in the 9.0.3.*x* series that the connector supports. ■ Oracle Identity Manager release 9.1.0.1 or later **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1).
Target systems	The target system can be one of the following: ■ Sun ONE Directory Server 5.2 ■ Sun Java System Directory Server Enterprise Edition 6.3, 7.0
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.
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.3.2 or later versions in the 9.0.3.*x* series, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.6 update 5 or later. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

The connector supports the following languages:

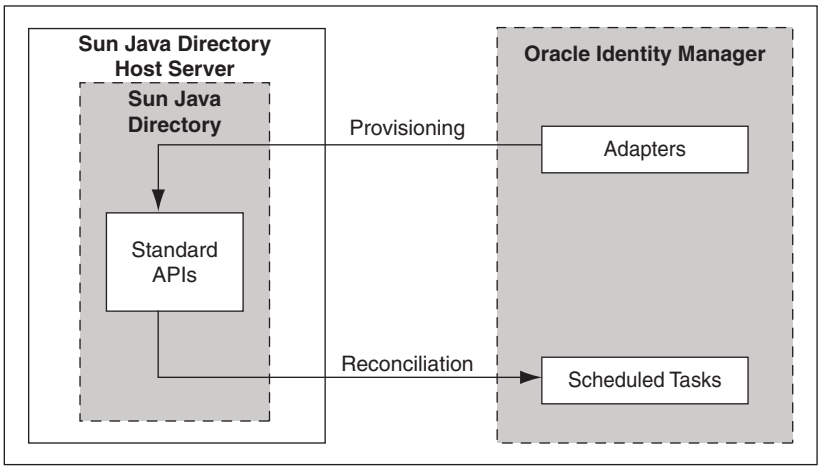
- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)

- Spanish

1.3 Connector Architecture

Figure 1–1 shows the connector integrating Sun Java System Directory with Oracle Identity Manager.

Figure 1–1 Connector Architecture



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

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

- Identity Reconciliation

  In the identity reconciliation mode, Sun Java System Directory Server is used as the trusted source and users are directly created and modified on it.

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

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

- Account Management

  In the account management mode, Sun Java System Directory Server is used as a target resource. The connector enables the target resource reconciliation and

provisioning operations. Through provisioning operations performed on Oracle Identity Manager, user accounts are created and updated on the target system for OIM Users. During reconciliation from the target resource, the Sun Java System Directory connector fetches into Oracle Identity Manager data about user accounts that are created or modified on the target system. This data is used to add or modify resources allocated to OIM Users.

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

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

1.4 Features of the Connector

1.4.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure Sun Java System Directory as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.4, "Configuring Reconciliation" for more information.

1.4.2 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the SearchFilter attribute of the scheduled tasks. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Section 3.4.1, "Limited Reconciliation" for more information.

1.4.3 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Section 3.4.2, "Batched Reconciliation" for more information.

1.4.4 Support for Both Full and Incremental Reconciliation

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

You can perform a full reconciliation run at any time.

1.4.5 Support for Adding New Single-Valued and Multivalued Attributes for Reconciliation and Provisioning

If you want to add to the standard set of single-valued and multivalued attributes for reconciliation and provisioning, then perform the procedures described in Chapter 4, "Extending the Functionality of the Connector."

1.4.6 Support for Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a record is deleted on the target system, then the corresponding iPlanet resource is revoked from the OIM User. In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted.

1.4.7 Support for High-Availability Configuration of the Target System

The connector can be configured to work with high-availability target system environments. If the primary installation becomes unavailable, then the connector reads information about backup target system installations from the lookup.iPlanet.BackupServers lookup definition and uses this information to switch to a backup target system installation. See Section Section 2.3.1.5, "Configuring High Availability of the Target System" for more information.

1.5 Lookup Definitions Used During Connector Operations

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

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

1.5.1 Lookup Definitions Synchronized with the Target System

The following lookup definitions are populated with values fetched from the target system by the scheduled tasks for lookup field synchronization:

> **See Also:** Section 3.3, "Lookup Field Synchronization" for information about these scheduled tasks

- For organizations and organization units: Lookup.IPNT.Organization
- For groups: Lookup.IPNT.UserGroup
- For roles: Lookup.IPNT.Role

1.5.2 Other Lookup Definitions

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

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.iPlanet.Configuration	This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.	Some of the entries in this lookup definition are preconfigured. See Section 2.3.1.4.1, "Setting Up the Lookup.iPlanet.Configuration Lookup Definition" for information about the entries for which you can set values.
Lookup.iPlanet.Constants	This lookup definition stores values that are used internally by the connector. The connector development team can use this lookup definition to make minor configuration changes in the connector.	You must not modify the entries in this lookup definition. See Section 2.3.1.4.3, "Setting Up the Lookup.iPlanet.Constants Lookup Definition" for more information about the entries for which you can set values.
AttrName.Recon.Map.iPlanet	This lookup definition holds mappings between the iPlanet User resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for user reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AttrName.Prov.Map.iPlanet	This lookup definition holds mappings between iPlanet User process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–3 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for user provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
Lookup.iPlanetGroupReconciliation.FieldMap	This lookup definition holds mappings between iPlanet Group resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–4 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.
AtMap.iPlanetGroup	This lookup definition holds mappings between iPlanet Group process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–4 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
Lookup.iPlanetRoleReconciliation.FieldMap	This lookup definition holds mappings between iPlanet Role resource object fields and target system attributes.	This lookup definition is preconfigured. Table 1–5 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for role reconciliation. Chapter 4, "Extending the Functionality of the Connector" provides more information.

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
AttrMap.iPlanetRole	This lookup definition holds mappings between iPlanet Role process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–5 lists the default entries in this lookup definition. You can add entries in this lookup definition if you want to map new target system attributes for group provisioning. Chapter 4, "Extending the Functionality of the Connector" provides more information.
lookup.iPlanet.BackupServers	This lookup definition holds mappings between primary iPlanet servers and secondary iPlanet servers.	It is optional to enter values in this lookup definition. Section 2.3.1.5, "Configuring High Availability of the Target System" provides information about this lookup definition
Lookup.IPNT.CommLang	During a provisioning operation, you use this lookup definition to specify a language for the user.	Section 2.3.1.4.2, "Setting Up the Lookup.IPNT.CommLang Lookup Definition" provides information about creating entries in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during reconciliation:

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

- For Oracle Identity Manager release 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.3, "Role Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.6, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Field	Description
User ID	uid	User ID
First Name	givenname	First name
Last Name	sn	Last name
Middle Initial	initials	Middle name
Department	departmentnumber	Department
Location	l	Location
Telephone	telephonenumber	Telephone
Email	mail	Email
Communication Language	preferredlanguage	Communication language
Title	title	Title
Container DN	NA	Container in which the user is present on the target system For example: `o=abc,dc=Company`
Group	uniquemember	The Group attribute which holds the User ID of its members.
Role	nsroledn	The User attribute which holds the roles for which the user is assigned.
nsuniqueid	nsuniqueid	Unique ID for User
Common Name	cn	Common Name
Status	nsaccountlock	The attribute which holds the value of user status in target system.

1.6.2 Group Attributes for Target Resource Reconciliation and Provisioning

Table 1–4 provides information about group attribute mappings for target resource reconciliation and provisioning.

Note: If you are using Oracle Identity Manager release 11.1.1, then you cannot reconcile data from group attributes of the target system. This is tracked by Bug 9799541 in Chapter 6, "Known Issues."

Table 1–4 Group Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Group Attribute	Description
Group Name	cn	Group name
Organization	NA	Container in which the group object is located on the target system
nsuniqueid	nsuniqueid	nsuniqueid of the group

1.6.3 Role Attributes for Target Resource Reconciliation and Provisioning

Table 1–5 provides information about role attribute mappings for target resource reconciliation and provisioning.

Note: If you are using Oracle Identity Manager release 11.1.1, then you cannot reconcile data from role attributes of the target system. This is tracked by Bug 9799541 in Chapter 6, "Known Issues."

Table 1–5 Role Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Role Attribute	Description
Role Name	cn	Role name
Organization	NA	Container in which the role object is located on the target system
nsuniqueid	nsuniqueid	nsuniqueid of the group

1.6.4 Reconciliation Rule for Target Resource Reconciliation

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

- For Oracle Identity Manager release 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process-matching rule:

Rule name: iPlanet Recon User

Rule element: (NsuniqueID Equals NsuniqueID) OR (User Login Equals User ID)

In the first rule component:

- NsuniqueID to the left of "Equals" is the NsuniqueID of the resource assigned to the OIM User.
- NsuniqueID to the right of "Equals" is the NsuniqueID of the resource on the target system.

In the second rule component:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.3.*x*:

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

    User ID attribute on the OIM User form.
- User ID is the UID field on the target system.

This rule supports the following scenarios:

- You can provision multiple Sun Java System Directory resources to the same OIM User, either on Oracle Identity Manager or directly on the target system.
- You can change the user ID of a user on the target system.

This is illustrated by the following use cases:

- Use case 1: You provision a Sun Java System Directory account for an OIM User, and you also create an account for the user directly on the target system.

When the first rule condition is applied, no match is found. Then, the second rule condition is applied and it is determined that a second account has been given to the user on the target system. The second account is linked with the OIM User at the end of the reconciliation run.

- Use case 2: An OIM User has a Sun Java System Directory account. You then change the user ID of the user on the target system.

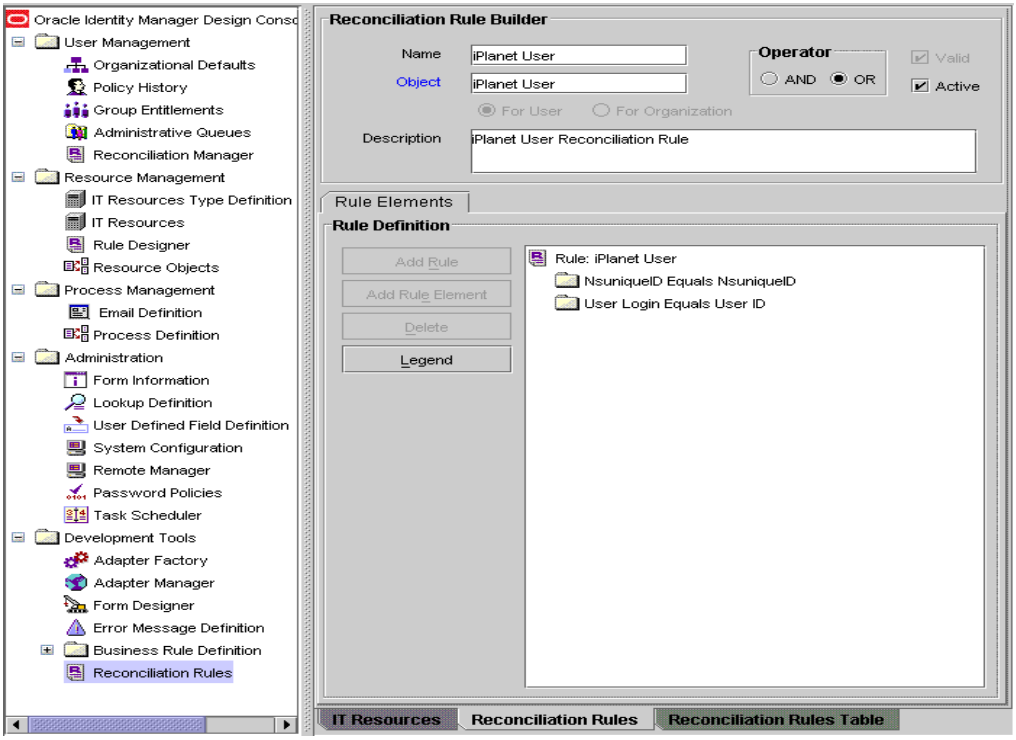
  During the next reconciliation run, application of the first rule condition helps match the resource with the record.

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **iPlanet User**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Resource Reconciliation

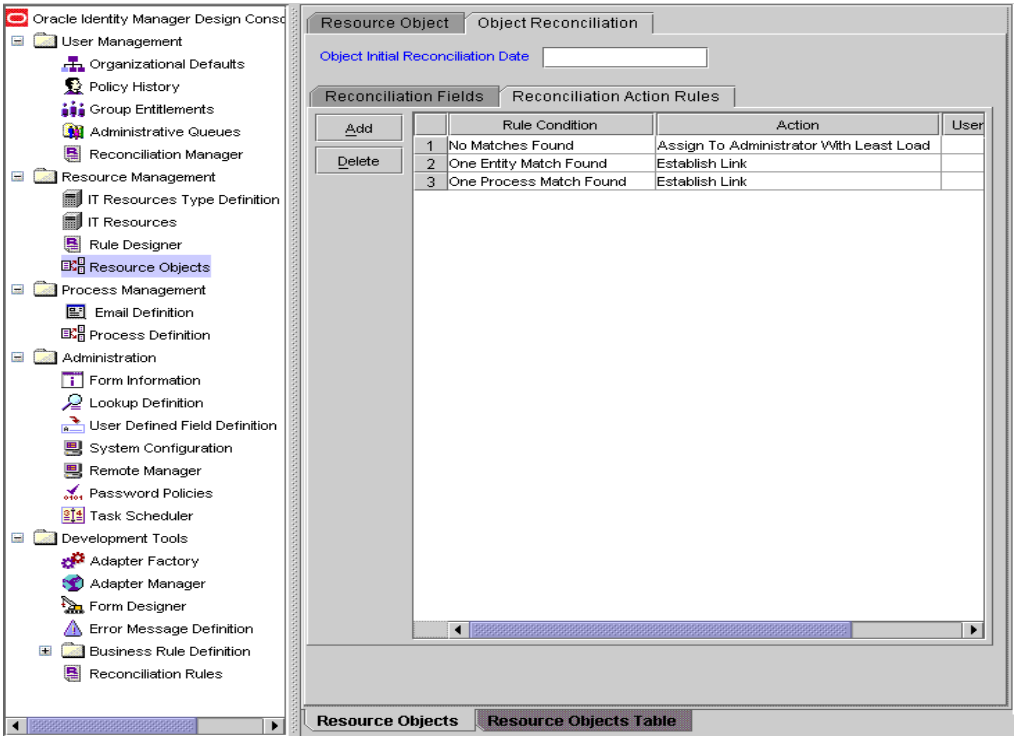
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **iPlanet User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



1.6.6 Provisioning Functions

Table 1–7 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–7 Provisioning Functions

Function	Adapter
Create User	iPlanet Create User
Delete User	iPlanet Delete User
Enable User	iPlanet Modify User
Disable User	iPlanet Modify User
Move User from One Container to Another	iPlanet Move User
Password Updated	iPlanet Modify User
First Name Updated	iPlanet Modify User
Last Name Updated	iPlanet Modify User
Department Updated	iPlanet Modify User
Email ID Updated	iPlanet Modify User
Location Updated	iPlanet Modify User
Middle Name Updated	iPlanet Modify User
Communication Language Updated	iPlanet Modify User
Telephone Updated	iPlanet Modify User
Title Updated	iPlanet Modify User
Container DN Updated	iPlanet Move User
Add User to Group	iPlanet Add User to Group
Remove User from Group	iPlanet Remove User From Group
Add User to Role	iPlanet Add Role to User
Remove User from Role	iPlanet Remove Role from user
Create OU	iPlanet Create OU
Change OU Name	iPlanet Change Org Name
Delete OU	iPlanet Delete OU
Move OU	iPlanet Move OU
Create iPlanet Group	iPlanet Create Group
Delete iPlanet Group	iPlanet Delete Group
Group Name Updated	Update iPlanet Group Details
Create iPlanet Role	iPlanet Create Role
Delete iPlanet Role	iPlanet Delete Role
Role Name Updated	Update iPlanet Role Details
Common Name Updated	iPlanet Modify User
User ID Updated	iPlanet Modify User

1.7 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

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

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–8 lists user attributes for trusted source reconciliation.

Table 1–8 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	cn	Common name
First Name	givenname	Given name
Last Name	sn	Last name
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

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

- For Oracle Identity Manager release 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule:

Rule name: Trusted Source recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is one of the following:
  - For Oracle Identity Manager Release 9.0.3.*x*:

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

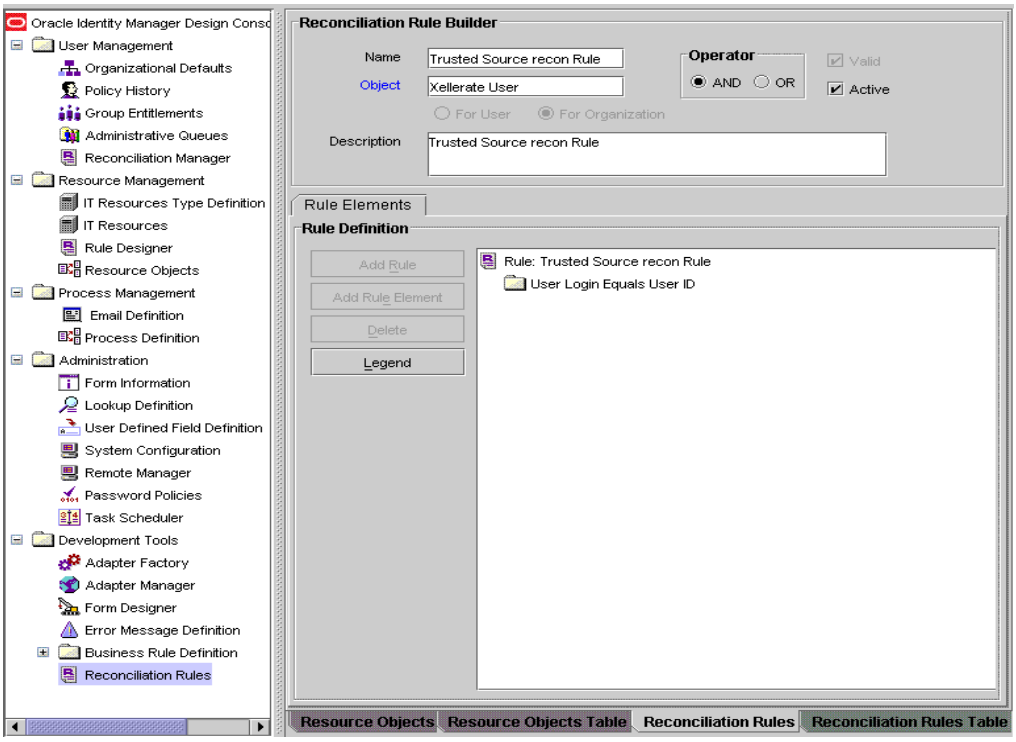
    User ID attribute on the OIM User form.
- User ID is the cn field of Sun Java System Directory.

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

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

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

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–9 lists the action rules for target resource reconciliation.

Table 1–9 Action Rules for Target Source Reconciliation

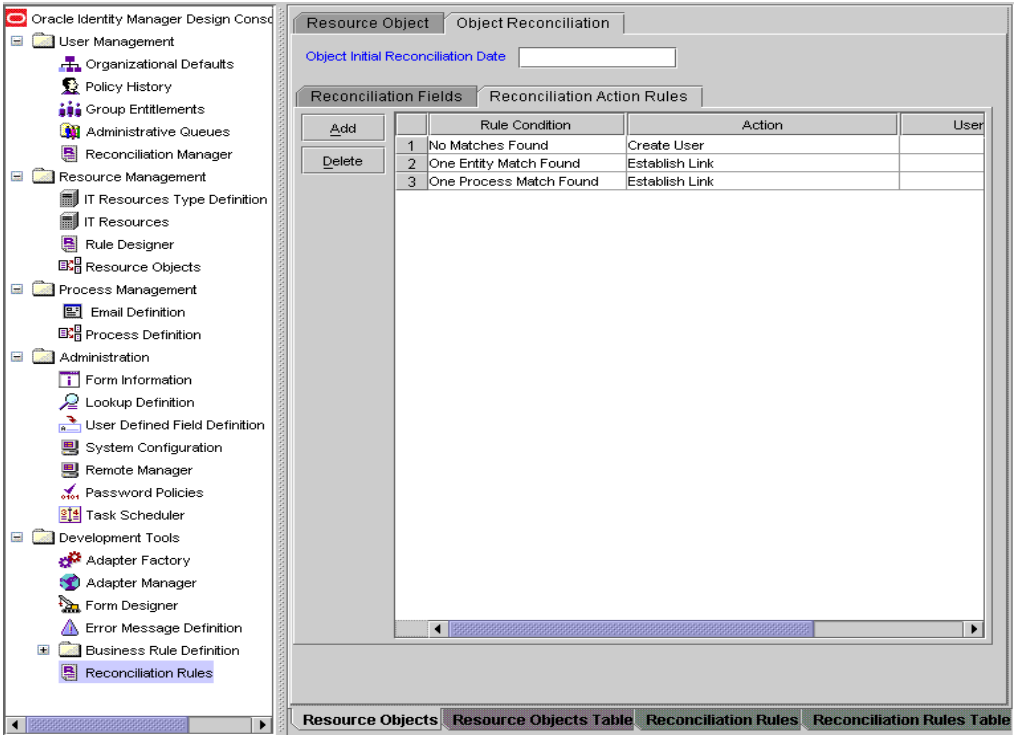
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

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

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

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



1.8 Roadmap for Deploying and Using the Connector

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

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.

- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2 Deploying the Connector

To deploy the connector, perform the procedures described in the following sections:

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

2.1 Preinstallation

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

The procedures described in the following sections are applicable to Sun Java System Directory Server 5.2.

See *Sun Java System Directory Server Administration Guide* for procedures applicable to other versions of Sun Java System Directory Server.

This section is divided into the following topics:

- Section 2.1.1, "Preinstallation on Oracle Identity Manager"
- Section 2.1.2, "Preinstallation on the Target System"

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Section 2.1.1.1, "Files and Directories on the Installation Media"
- Section 2.1.1.2, "Determining the Release Number of the Connector"
- Section 2.1.1.3, "Using External Code Files"

2.1.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 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.
Files in the dataset directory ■ ModifyResourceiPlanet User.xml ■ ProvisionResourceiPlanet User.xml	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/SJSDSProv.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
lib/SJSDSRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
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.

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

File in the Installation Media Directory	Description
xml/iPlanetResourceObject.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ 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.
xml/SJSDSConnectorRequestDatasets.xml	This file contains the request dataset for the connector. You import this file by using the Deployment Manager. See Section 2.3.1.7.1, "Importing Request Datasets Using Deployment Manager" for more information.

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

2.1.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then the procedure described in this section is optional.

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

You 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.

2.1.1.3 Using External Code Files

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

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 Oracle Web site at

   `http://download.oracle.com/otn-pub/java/jndi/1.2.1/ldap-1_2_4.zip`

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 directory:

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

   - For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:

     OIM_HOME/xellerate/ThirdParty

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ThirdParty

2.1.2 Preinstallation on the Target System

This section describes the following procedures, which have to be performed on the target system to create a user account with limited rights:

- Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"
- Section 2.1.2.2, "Creating a VLV Index"

2.1.2.1 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 Section 2.2.1.2, "Configuring the IT Resource."

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**.

2.1.2.2 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**.

2.2 Installation

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

The procedures described in the following sections are applicable to Sun Java System Directory Server 5.2.

See *Sun Java System Directory Server Administration Guide* for procedures applicable to other versions of Sun Java System Directory Server.

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

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.0.3.2 or Later Releases in the 9.0.3.x Series"

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

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

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1 or later involves the following procedures:

- Section 2.2.1.1, "Running the Connector Installer"
- Section 2.2.1.2, "Configuring the IT Resource"

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

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

Note: In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

- For Oracle Identity Manager release 9.1.0.*x*:
  OIM_HOME/xellerate/ConnectorDefaultDirectory
- For Oracle Identity Manager release 11.1.1:
  OIM_HOME/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Fusion Middleware User's Guide for Oracle Identity Manager
   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.
   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
4. From the Connector List list, select **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 in Step 1.

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.
   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
   c. From the Connector List list, select **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 Section 2.3.1.6, "Configuring Trusted Source Reconciliation."
   c. Compilation of adapters

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

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

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

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

   Note: At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

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

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

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

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

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

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.1.1.1, "Files and Directories on the Installation Media" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.2.1.2 Configuring the IT Resource

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. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, 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. Table 2–2 describes each parameter.

Table 2–2 IT Resource Parameters

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 Section 2.3.2, "Configuring SSL."
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 Section 2.3.2, "Configuring SSL." **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.

Table 2–2 (Cont.) IT Resource Parameters

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`.
Last Trusted Delete Recon TimeStamp	Starting with the first trusted delete reconciliation run, this parameter stores the time-stamp value at which trusted source delete reconciliation run ends. **Note:** You must not change the default value of this parameter.
Last Target Delete Recon TimeStamp	Starting with the first target delete reconciliation run, this parameter stores the time-stamp value at which target source delete reconciliation run ends. **Note:** You must not change the default value of this parameter.
Abandoned connection timeout	Enter the time (in seconds) after which a connection must be automatically closed if it is not returned to the pool. **Note:** You must set this parameter to a value that is high enough to accommodate processes that take a long time to complete (for example, full reconciliation). Default value: `600`
Backup Servers URL	Enter a value for this parameter when both the following conditions are true: ■ You specify `true` as the value of the Connection pooling supported parameter, which is described later in this table. ■ You want to configure high availability of the target system. Enter the complete URL of the secondary target system installations to which Oracle Identity Manager must switch to if the primary target system installation becomes unavailable. You must specify the complete URL in the following format: ldap://*SERVERADDRESS*:*PORT*/ ldap://*SERVERADDRESS1*:*PORT1*/ Default Value: `[NONE]` Sample value: `ldap://172.20.55.191:389/ ldap://172.20.55.171:387/` **Note:** Multiple URLs must be separated by space.
LDAP Connection TimeOut	Enter the timeout interval (in milliseconds) for which the connector must wait for a response from the target system before switching to one of the backup servers listed in the Backup Server URL parameter. Default Value: `3000` **Note:** This parameter is used only if you specify a value for the Backup Server URL parameter.
Connection pooling supported	Enter `true` if you want to enable connection pooling for this target system installation. Otherwise, enter `false`. Default value: `false`

Table 2–2 (Cont.) IT Resource Parameters

Parameter	Description
Connection wait timeout	Enter the maximum time (in seconds) for which the connector must wait for a connection to be available. Default value: `60`
Inactive connection timeout	Enter the time (in seconds) of inactivity after which a connection must be dropped and replaced by a new connection in the pool. Default value: `600`
Initial pool size	Enter the number of connections that must be established when the connection pool is initialized. The pool is initialized when it receives the first connection request from a connector. Default value: `1` Sample value: `3`
Max pool size	Enter the maximum number of connections that must be established in the pool at any point of time This number includes the connections that have been borrowed from the pool. Default value: `30` Sample value: `10`
Min pool size	Enter the minimum number of connections that must be in the pool at any point of time. This number includes the connections that have been borrowed from the pool. Default value: `2` Sample value: `5`
Native connection pool class definition	This parameter holds the name of the wrapper to the native pool mechanism that implements the GenericPool. **Note:** Do not specify a value for this parameter.
Pool excluded fields	This parameter holds a comma-separated list of IT parameters whose change must not trigger a refresh of the connector pool. Value: **Note:** Do not change the value of this parameter unless you are adding or deleting a parameter from the IT resource. You must ensure that the total length of the list does not exceed 2000 characters. If you are adding a parameter to the IT resource, then that parameter name must be added to the above list with a comma separator. If you are deleting a parameter from the IT resource, then that parameter must be removed from the list if it exists in the list. You must restart Oracle Identity Manager for changes that you make to this parameter to take effect.
Pool preference	This parameter specifies the preferred connection pooling implementation. Value: `Default` **Note:** Do not change this value of this parameter.
ResourceConnection class definition	This parameter holds the name of the implementation of the ResourceConnection class. Value: `com.thortech.xl.integration.iplanet.util.iplanetResourceConnectionlmpl.` **Note:** Do not change the value of this parameter.

Table 2–2 (Cont.) IT Resource Parameters

Parameter	Description
Target supports only one connection	This parameter indicates whether the target system can support one or more connections at a time. Value: `false` **Note:** Do not change the value of this parameter.
Timeout check interval	Enter the time interval (in seconds) at which the other timeouts specified by the other parameters must be checked Default value: `30`
Validate connection on borrow	Specify whether or not a connection must be validated before it is lent by the pool. The value can be `true` or `false`. It is recommended that you set the value to `true`. Default value: `true`
Prov Org Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning of Organization Units. Default Value: **AtMap.iPlanetOrg**

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

2.2.2 Installing the Connector on Oracle Identity Manager Release 9.0.3.2 or Later Releases 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:

- Section 2.2.2.1, "Copying the Connector Files"
- Section 2.2.2.2, "Importing the Connector XML File"
- Section 2.2.2.3, "Compiling Adapters"

2.2.2.1 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: Section 2.1.1.1, "Files and Directories on the Installation Media" 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 an Oracle Identity Manager cluster, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

2.2.2.2 Importing the Connector XML File

As mentioned in Section 2.1.1.1, "Files and Directories on the Installation Media," 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 If you are using OIM 9.1.0.x, path is: *OIM_HOME*/xellerate/ConnectorDefaultDirectory/<iPlanet Package>/xml directory. If you are using OIM 11x, path is: *OIM_HOME*/server/ConnectorDefaultDirectory/<iPlanet Package>/xml directory OR iPlanetResourceObject.xml file can also be found in the connector package stored in the local machine.

   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 Table 2–2 for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the LDAP Server IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

    See Also: If you want to define another IT resource, then refer to *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* 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.

2.2.2.3 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.

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

> **See Also:** Section 1.6.6, "Provisioning Functions" 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 cluster, 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.

2.3 Postinstallation

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

The procedures described in the following sections are applicable to Sun Java System Directory Server 5.2.

See *Sun Java System Directory Server Administration Guide* for procedures applicable to other versions of Sun Java System Directory Server.

Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Configuring Oracle Identity Manager"
- Section 2.3.2, "Configuring SSL"
- Section 2.3.3, "Configuring the Target System"

2.3.1 Configuring Oracle Identity Manager

Configuring the Oracle Identity Manager involves performing the following procedures:

- Section 2.3.1.1, "Changing to the Required Input Locale"
- Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"

- Section 2.3.1.3, "Enabling Logging"
- Section 2.3.1.4, "Setting Up Lookup Definitions in Oracle Identity Manager"
- Section 2.3.1.5, "Configuring High Availability of the Target System"
- Section 2.3.1.6, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.7, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.3.1.1 Changing to the Required Input Locale

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

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

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

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

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.0.3.*x* and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

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

For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:

OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

For Oracle Identity Manager release 11.1.1:

OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

  Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

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

  In this format:

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

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

2.3.1.3 Enabling Logging

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

- Section 2.3.1.3.1, "Enabling Logging on Oracle Identity Manager Release 9.0.3.x or Release 9.1.0.x"
- Section 2.3.1.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.3.1 Enabling Logging on Oracle Identity Manager Release 9.0.3.x or Release 9.1.0.*x*

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

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **Oracle WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.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

2.3.1.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

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

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

These log levels are mapped to ODL message type and level combinations as shown in Table 2–3.

Table 2–3 Log Levels and ODL Message Type:Level Combinations

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

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following block into <log_handlers> section:

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

   Add the following block into <loggers> section.

```
<logger name="XL_INTG.SJSDS" level="[LOG_LEVEL]" useParentHandlers="false">
     <handler name="sjsds-handler"/>
     <handler name="console-handler"/>
</logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–3 lists the supported message type and level combinations.

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

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

```
<log_handler name='sjsds-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
     <property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
```

```
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
  </log_handler>

<logger name="XL_INTG.SJSDS" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="sjsds-handler"/>
     <handler name="console-handler"/>
</logger>
```

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

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

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

Note:

- You can also configure the connector logging without adding separate handler and using existing log handler.
- It is advisable to modify logging.xml using the GUI screen in Enterprise Manager instead of manually editing the file.

2.3.1.4 Setting Up Lookup Definitions in Oracle Identity Manager

You must enter values in some of the lookup definitions that are created when you install the connector. To enter values in a lookup definition:

1. Log in to the Design Console.
2. Expand **Administration**, and double-click **Lookup Definition**.
3. Search for and open the lookup definitions described in the following sections. After you enter values in each lookup definitions, save the changes.

- Section 2.3.1.4.1, "Setting Up the Lookup.iPlanet.Configuration Lookup Definition"
- Section 2.3.1.4.2, "Setting Up the Lookup.IPNT.CommLang Lookup Definition"
- Section 2.3.1.4.3, "Setting Up the Lookup.iPlanet.Constants Lookup Definition"

2.3.1.4.1 Setting Up the Lookup.iPlanet.Configuration Lookup Definition

You can specify values for the following entries in the Lookup.iPlanet.Configuration lookup definition:

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

- TimeStampSearchFormat

  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'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.

2.3.1.4.2 Setting Up the Lookup.IPNT.CommLang Lookup Definition

Table 2–4 shows the default entries in the Lookup.IPNT.CommLang lookup definition.

Table 2–4 Entries in the Lookup.IPNT.CommLang Lookup Definition

Code Key	Decode
pt	BrazilianPortuguese
en	English
fr	French
de	German
it	Italian
ja	Japanese
ko	Korean
zh-CN	SimplifiedChinese
es	Spanish
zh-TW	TraditionalChinese

2.3.1.4.3 Setting Up the Lookup.iPlanet.Constants Lookup Definition

You can specify values for the following entries in the Lookup.iPlanet.Constants lookup definition:

- 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

2.3.1.5 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 2–5 shows samples entries for the Lookup.iPlanet.BackupServers lookup definition.

Table 2–5 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.

2.3.1.6 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. Depending on the version of Oracle Identity Manager, perform one of the following procedures:

   If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:

   a. Click the **Deployment Management** link on the left navigation bar.

   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.

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

   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.

   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.

3. Locate and open the iPlanetXLResourceObject.xml file located in the following directory:

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

     OIM_HOME/xellerate/ConnectorDefaultDirectory/*CONN_HOME*/xml

   - For Oracle Identity Manager release 11.1.1:

OIM_HOME/server/xellerate/ConnectorDefaultDirectory/*CONN_HOME*/xml

Details of this XML file are shown on the File Preview page.

Note: If you open the Oracle Identity Manager Administrative and User Console on a remote computer, then you cannot select the XML file from the ConnectorDefaultDirectory directory on the Oracle Identity Manager host computer.

4. Click **Add File**. The Substitutions page is displayed.
5. Click **Next**. The Confirmation page is displayed.
6. Click **Import**.
7. 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 Section 3.5, "Configuring Scheduled Tasks."

2.3.1.7 Configuring Oracle Identity Manager for Request-Based Provisioning

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

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

The following are features of request-based provisioning:

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

  Note: Direct provisioning allows the provisioning of multiple target system accounts on the target system.

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

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

- Section 2.3.1.7.1, "Importing Request Datasets Using Deployment Manager"
- Section 2.3.1.7.2, "Copying Predefined Request Dataset"
- Section 2.3.1.7.3, "Importing Request Datasets into MDS"
- Section 2.3.1.7.4, "Enabling the Auto Save Form Feature"
- Section 2.3.1.7.5, "Running the PurgeCache Utility"

2.3.1.7.1 Importing Request Datasets Using Deployment Manager

Note:

- You can perform this procedure instead of the procedures described in Section 2.3.1.7.2, "Copying Predefined Request Dataset" and Section 2.3.1.7.3, "Importing Request Datasets into MDS."
- See *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about importing objects from an XML file using the Deployment Manager.

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

To import a request dataset XML file by using the Deployment Manager:

1. Log in to 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 request dataset XML file, SJSDSConnectorRequestDatasets.xml, which is in the xml directory of the installation media.

   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. Close the Deployment Manager dialog box.

   The request dataset is imported into Oracle Identity Manager.

2.3.1.7.2 Copying Predefined Request Dataset

Predefined request dataset XML files are shipped with the connector. The following dataset XML files are available in the DataSets directory on the installation media:

- ModifyResourceiPlanet User.xml
- ProvisionResourceiPlanet User.xml

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

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\SJSDSStd

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

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

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

2.3.1.7.3 Importing Request Datasets into MDS

You can configure request-based provisioning by importing the request datasets into into the metadata store (MDS) by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

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

   Note: While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.3.1.7.2, "Copying Predefined Request Dataset," if you copy the files to the E:\MyDatasets\custom\connector\SJSDSStd directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

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

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

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

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

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

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

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

`t3://HOST_NAME_IP_ADDRESS:PORT`

In this format, replace:

- *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.
- *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS.

2.3.1.7.4 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

2.3.1.7.5 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.3.2 Configuring SSL

To enable SSL communication between Oracle Identity Manager and Sun Java System Directory, you must perform the following tasks:

1. Section 2.3.2.1, "Creating the CA and SSL Certificates"
2. Section 2.3.2.2, "Importing the CA and SSL Certificates into Sun Java System Directory"
3. Section 2.3.2.3, "Importing the CA and SSL Certificates into Oracle Identity Manager"
4. Section 2.3.2.4, "Enabling SSL Communication on Sun Java System Directory"

2.3.2.1 Creating the CA and SSL Certificates

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

- Section 2.3.2.1.1, "Generating the Certificate Signing Request on Sun Java System Directory"
- Section 2.3.2.1.2, "Using the Certificate Signing Request to Generate the CA and SSL Certificates"

2.3.2.1.1 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**.

2.3.2.1.2 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.

2.3.2.2 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:

- Section 2.3.2.2.1, "Importing the CA Certificate into Sun Java System Directory"
- Section 2.3.2.2.2, "Importing the SSL Certificate into Sun Java System Directory"

2.3.2.2.1 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**.

2.3.2.2.2 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**.

2.3.2.3 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 an Oracle Identity Manager cluster, you must perform this procedure on each node 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 2–6 shows the location of the certificate store for each of the supported application servers.

Table 2–6 Certificate Store Locations

Application Server	Certificate Store Location
Oracle WebLogic Server	■ If you are using Oracle jrockit_R27.3.1-jdk, then copy the certificate into the following directory: *JROCKIT_HOME*/jre/lib/security ■ If you are using the default Oracle WebLogic Server JDK, then copy the certificate into the following directory: *WEBLOGIC_HOME*/java/jre/lib/security/cacerts
IBM WebSphere Application Server	■ For a noncluster 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. If you are using Oracle Identity Manager release 11.1.1, then import each certificate into the WebLogic keystore by running the following command:

   ```
   keytool -import -keystore WEBLOGIC_HOME/server/lib/DemoTrust.jks -file
   CERT_FILE_NAME -storepass PASSWORD
   ```

   In this command:

   - *CERT_FILE_NAME* is the full path and name of the certificate file.
   - *PASSWORD* is the password of the keystore.

   The following is a sample command:

   ```
   keytool -import -keystore
   WEBLOGIC_HOME/server/lib/DemoTrust.jks -file
   /home/testoc4j/OIM/globalv.crt -storepass
   DemoTrustKeyStorePassPhrase
   ```

5. To confirm whether 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
```

6. For a noncluster 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.
7. For a cluster 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.

2.3.2.4 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.

2.3.3 Configuring the Target System

Configuring the target system consists of the following procedure:

Enabling Retro Change Log Plug-in on the Target System

The retro change log is a plug-in that is used to maintain application compatibility with earlier versions of the Directory Server. The retro change log is stored under the suffix `cn=changelog`. When you enable the retro change log plug-in, updates to all suffixes on that server are logged by default.

To enable the Retro Change Log Plug-in on the Target System, perform one of the following procedures depending on the version of Sun Java System Directory:

If you are using Sun ONE Directory Server 5.2:

1. Log in to the Sun One Server Console using administrator credentials.
2. Expand the **host name** directory.
3. Expand **Server Group.**
4. Select **Directory Server,** and then click **Open** on the right pane.

5. On the top-level Configuration tab on the Directory Server console, expand the **Plugins** node, and scroll down to select **Retro Change Log** plug-in.
6. In the right panel, select the **Enable Plug-in** check box and click **Save**.

> **Note:** To disable the plug-in, clear the **Enable plug-in** check box.

7. Restart the Directory Server after enabling the plug-in.

If you are using Sun Java System Directory Server Enterprise Edition 6.3:

1. Log in to the Sun Java Web Console using administrator credentials.
2. Select Directory Service Control Center (DSCC) and log in to access the Common Tasks tab.
3. Click the **Directory Servers** tab.
4. Click the server currently in use and ensure it is in the **Started** state.
5. Click the **Server Configuration** tab, and then on the **Plug-Ins** sub-tab.
6. Select the **Retro Change Log** check box and click **Save.**

> **See Also:** *Sun Java System Directory Server Administration Guide* for information about working with the Retro Change Log plug-in

3

Using the Connector

This chapter is divided into the following sections:

3.1 Guidelines to Apply While Using the Connector

Apply the following guidelines 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 see Section 3.1.1, "Enabling the Entry of Non-ASCII Characters in the User ID and E-mail Fields".

3.1.1 Enabling the Entry of Non-ASCII Characters in the User ID and E-mail Fields

If you are using Sun ONE Directory Server 5.2:

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.**

If you are using Sun Java System Directory Server Enterprise Edition 6.3:

1. Click the **Directory Servers** tab.
2. Select the server that is currently in use and ensure it is in the **Started** state.
3. Click the **Server Configuration** tab.
4. Click **Plugins.**
5. Select **7-Bit check.**
6. Deselect the **Enable plug-in** check box.

3.2 Performing First-Time Reconciliation

First-time or full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. The following is the sequence of steps involved in reconciling all existing user records:

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

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

---

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

   See Section 3.3, "Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Section 3.5, "Configuring Scheduled Tasks" for information about running scheduled tasks.

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

   See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about the attributes of this scheduled task.

   See Section 3.5, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, one of the following parameters of the Sun Java System Directory IT Resource IT resource is automatically set to the time stamp at which the reconciliation run began:

- For trusted source reconciliation, the Last Recon Trusted TimeStamp parameter is set.
- For target resource reconciliation, the Last Recon Target TimeStamp parameter is set.

> **See Also:** Section 2.2, "Installation" for information about the parameters of the IT resource

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

3.3 Lookup Field Synchronization

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. Table 3–1 describes the attributes of these scheduled tasks. Section 3.5, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

Note:

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

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

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`

Lookup Search Filter	Search filter in LDAP format	The value is one of the following:
		■ For group lookup reconciliation:
		`(objectclass=groupOfUniqueNames)`
		■ For role lookup reconciliation:
		`(objectClass=ldapsubentry)`
		■ For organization lookup reconciliation:
		`(objectclass=organization)`
		■ For organizational unit lookup reconciliation:
		`(objectclass=organizationalunit)`

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)
AttrName for Decode Value in Lookup	Attribute type of group, role, or organization that should be populated in the Decode value from the target system. It can be either `cn` or `dn`.	This value can be any attribute name in the target entry.
AttrName for Code value in Lookup	Attribute type of group, role, or organization that should be populated in the Code Key value from the target system.	The default value is `entrydn`. **Note:** You must not change this value.
ConfigurationLookup	Name of the lookup definition that stores configuration information used during connector operations Do not change the default value.	`Lookup.iPlanet.Configuration`

3.4 Configuring Reconciliation

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.

- Section 3.4.1, "Limited Reconciliation"
- Section 3.4.2, "Batched Reconciliation"
- Section 3.4.3, "Reconciliation Scheduled Tasks"

3.4.1 Limited 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 enclose the query condition in parentheses. For example:

  ```
  (&(objectClass=user)(sn!=Doe))
  ```
- 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.

3.4.2 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 Section 3.4.3.1, "User Reconciliation Scheduled Task."

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

3.4.3 Reconciliation Scheduled Tasks

This section discusses the following topics:

- Section 3.4.3.1, "User Reconciliation Scheduled Task"
- Section 3.4.3.2, "Group and Role Reconciliation Scheduled Task"

3.4.3.1 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. Table 3–2 describes the attributes of these scheduled tasks.

Note:

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

Table 3–2 Attributes of the User Reconciliation Scheduled Tasks

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:** Section 3.4.2, "Batched Reconciliation"	Default value: `0`
ConfigurationLookup	Name of the lookup definition that stores configuration information used during connector operations Do not change the default value.	`Lookup.iPlanet.Configuration`
ITResourceName	Name of the IT resource for setting up a connection with Sun Java System Directory	`iPlanet User`

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description	Default/Sample Value
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 `cn=changelog`.
		`ou=myou,dc=corp,dc=com` or `dc=corp, dc=com`
		For Delete Recon scheduled task:
		`cn=changelog`

SearchFilter	LDAP search filter used to locate an organization accounts
	See Section 3.4.1, "Limited Reconciliation" for more information.
		`(objectClass=inetOrgPerson)`
		For Delete Recon scheduled task:
		`(&(changetype=delete)(objectclass=changelogentry))`

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`
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`

3.4.3.2 Group and Role Reconciliation Scheduled Task

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

> **Note:** You cannot reconcile group data and role data from the target system if you are using Oracle Identity Manager release 11.1.1. This issue is tracked by Bug 9799541 in Chapter 6, "Known Issues."

- iPlanet Group Recon Task
- iPlanet Role Recon Task

You must specify values for the attributes of these scheduled tasks. Table 3–3 describes the attributes of these scheduled tasks.

Note:

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

Table 3–3 Attributes of the Group and Role Reconciliation Scheduled Tasks

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.	`Lookup.iPlanet.Configuration`

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
		For Role:
		`Lookup.iPlanetRoleReconciliation.FieldMap`
		For Group:
		`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`.
		For Role:
		`Yes`
		For Group:
		`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`

ResourceObjectName	Name of the resource object for reconciliation of Group or Role	For Role:
		`iPlanet Role`
		For Group:
		`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	For Role:
		`(objectClass=ldapsubentry)`
		For Group:
		`(objectClass=groupOfUniqueNames)`

3.5 Configuring Scheduled Tasks

You can apply the procedure described in this section to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–4 lists the scheduled tasks that form part of the connector.

Table 3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
iPlanet Organization Lookup Reconciliation	This scheduled task is used for organization lookup field synchronization. See Section 3.3, "Lookup Field Synchronization" for information about this scheduled task.
iPlanet Role Lookup Reconciliation	This scheduled task is used for role lookup field synchronization. See Section 3.3, "Lookup Field Synchronization" for information about this scheduled task.
iPlanet Group Lookup Reconciliation	This scheduled task is used for group lookup field synchronization. See Section 3.3, "Lookup Field Synchronization" for information about this scheduled task.
iPlanet User Trusted Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a trusted source. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.
iPlanet User Target Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a target resource. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.
iPlanet Trusted Delete User Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a trusted source. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.
iPlanet Target Delete User Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a target resource. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.
iPlanet Group Recon Task	This scheduled task is used for reconciliation of groups from the target system. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.
iPlanet Role Recon Task	This scheduled task is used for reconciliation of roles from the target system. See Section 3.4.3, "Reconciliation Scheduled Tasks" for information about this scheduled task.

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

- Section 3.5.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.3.x"
- Section 3.5.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

3.5.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.3.*x*

To configure the reconciliation scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed.
5. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, 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 user-configurable attributes of the scheduled task.

   See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* 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.

Stopping Reconciliation

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

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

3.5.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1

To configure scheduled tasks:

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

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

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

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

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

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

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

– **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.

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

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

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

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

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

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

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

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

Note:

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

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, do one of the following:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

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

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

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

3.6 Performing Provisioning Operations

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:

- Section 3.6.1, "Provisioning Users"
- Section 3.6.2, "Provisioning Organizational Units, Groups, and Roles"
- Section 3.6.3, "Enabling Provisioning of Users in Organizations and Organizational Units"

3.6.1 Provisioning Users

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

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

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

This following are types of provisioning operations:

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

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 3.6.1.1, "Direct Provisioning"
- Section 3.6.1.2, "Request-Based Provisioning"

3.6.1.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the user details page, click the **Resources** tab.
     b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **iPlanet User** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for iPlanet User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 5: Provide Process Data for iPlanet User Group Membership Details page, search for and select a group for the user on the target system and then click **Continue**.
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:
        a. Close the window displaying the "Provisioning has been initiated" message.
        b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.6.1.2 Request-Based Provisioning

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

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

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

- Section 3.6.1.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.6.1.2.2, "Approver's Role in Request-Based Provisioning"

3.6.1.2.1 End User's Role in Request-Based Provisioning

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

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

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

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

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

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.6.1.2.2 Approver's Role in Request-Based Provisioning

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

The following are steps that the approver can perform:

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

A message confirming that the task was approved is displayed.

3.6.2 Provisioning Organizational Units, Groups, and Roles

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

To provision an organizational unit:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Create an organization. To do so:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. Expand **Organizations,** and then click **Create**.
     b. Specify a name and the type for the organization that you want to create, and then click **Create Organization**.

        The organization is created.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome page, click **Administration** in the upper-right corner of the page.
     b. On the Welcome to Identity Administration page, from the Organizations section, click **Create Organization**.
     c. On the Create Organization page, enter values for the Name, Type, and Parent Organization (optional) fields, and then click **Save.**

        The organization is created.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. Select **Resource Profile** from the list.
     b. Click **Provision New Resource**.

        The Provision Resource to Organization page is displayed.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the organization details page, click the **Resources** tab.
     b. From the Actions menu, select **Provision.** Alternatively, click **Provision** on the toolbar. The Provision Resource to Organization page is displayed in a new window.
4. On the Step 1: Select a Resource page, search for and select the organizational unit you want to provision, and then click **Continue.**
5. On the Step 2: Verify Resource Selection page, verify the data that you provided, and then click **Continue.**
6. On the Step 5: Provide Process Data page, enter the details of the organizational unit that you want to provision and then click **Continue.**
7. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue.**

8. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the organizational unit has been provisioned to the organization.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. Close the window displaying the "Provisioning has been initiated" message.
     b. On the Resources tab, click **Refresh** to view the newly provisioned organizational unit.

To provision a group or role:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Search for and open the organization to which you want to provision a group or role by performing one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. From the Organizations menu, select **Manage.**
     b. Search for the organization and select the link for the organization from the list of organizations displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Organizations section, click **Advanced Search - Organizations,** provide a search criterion, and then click **Search.**

        Alternatively, search for the organization by selecting Organizations from the list on the left pane.
     b. From the organizations displayed in the search results table, click the row containing the organization to which to want to provision a group or role.

        The organization details page is displayed.
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, then:
     a. On the Organization Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource.**

        The Provision Resource to Organization page is displayed.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the organization details page, click the **Resources** tab.
     b. From the Actions menu, select **Provision.** Alternatively, click **Provision** on the toolbar. The Provision Resource to Organization page is displayed in a new window.
4. On the Step 1: Select a Resource page, select one of the following options, and then click **Continue:**
   - 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
Group Name	cn
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
Role Name	cn
nsuniqueid	nsuniqueid

5. On the Step 2: Verify Resource Selection page, verify the data that you provided, and then click **Continue.**
6. On the Step 5: Provide Process Data page, depending on whether you have selected a group or role while performing Step 4, enter the group or role details, and then click **Continue.**
7. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue.**
8. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the group or role has been provisioned to the organization.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. Close the window displaying the "Provisioning has been initiated" message.
     b. On the Resources tab, click **Refresh** to view the newly provisioned group or role.

3.6.3 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 Fusion Middleware User's Guide for Oracle Identity Manager*for detailed information about modifying lookup definitions

- ldapOrgDNPrefix=o
- ldapOrgUnitObjectClass=organization

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

Note: It is assumed that you have performed the procedure described in Section 2.3.1.7, "Configuring Oracle Identity Manager for Request-Based Provisioning."

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

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

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

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **iPlanet User** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **iPlanet User** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

4

Extending the Functionality of the Connector

The following sections describe procedures that you can perform to extend the functionality of the connector for addressing your specific business requirements:

- Section 4.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation"
- Section 4.3, "Adding New Attributes for Group Reconciliation"
- Section 4.4, "Adding New Attributes for Role Reconciliation"
- Section 4.5, "Adding New Attributes for Trusted Source Reconciliation"
- Section 4.6, "Adding New Attributes for Provisioning"
- Section 4.7, "Adding New Multivalued Attributes for Provisioning"
- Section 4.8, "Adding New Attributes for Provisioning of Group"
- Section 4.9, "Adding New Attributes for Provisioning of Role"
- Section 4.10, "Adding New Object Classes for Reconciliation and Provisioning"
- Section 4.11, "Configuring the Connector for Multiple Installations of the Target System"

4.1 Adding New Attributes for Target Resource Reconciliation

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning" 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 Fusion Middleware User's Guide for Oracle Identity Manager*for detailed instructions on performing the following procedure

To add a custom attribute for reconciliation:

1. While performing the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations", 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.

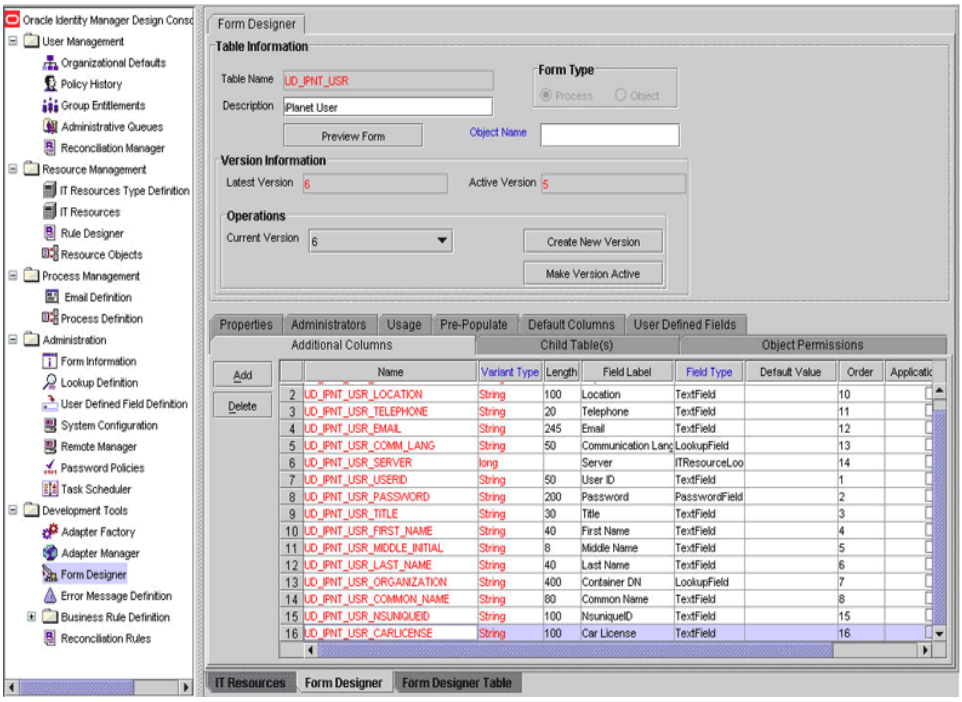
   b. Search for and open the **UD_IPNT_USR** form.

   c. Create a new version of the form.

   d. Add the new attribute on the form.

      For example, if you want to add the Car License attribute, then enter the following values on the Additional Columns tab:

Field	Value
Name	CARLICENSE
Variant Type	String
Length	100
Field Label	Car License
Order	16



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.

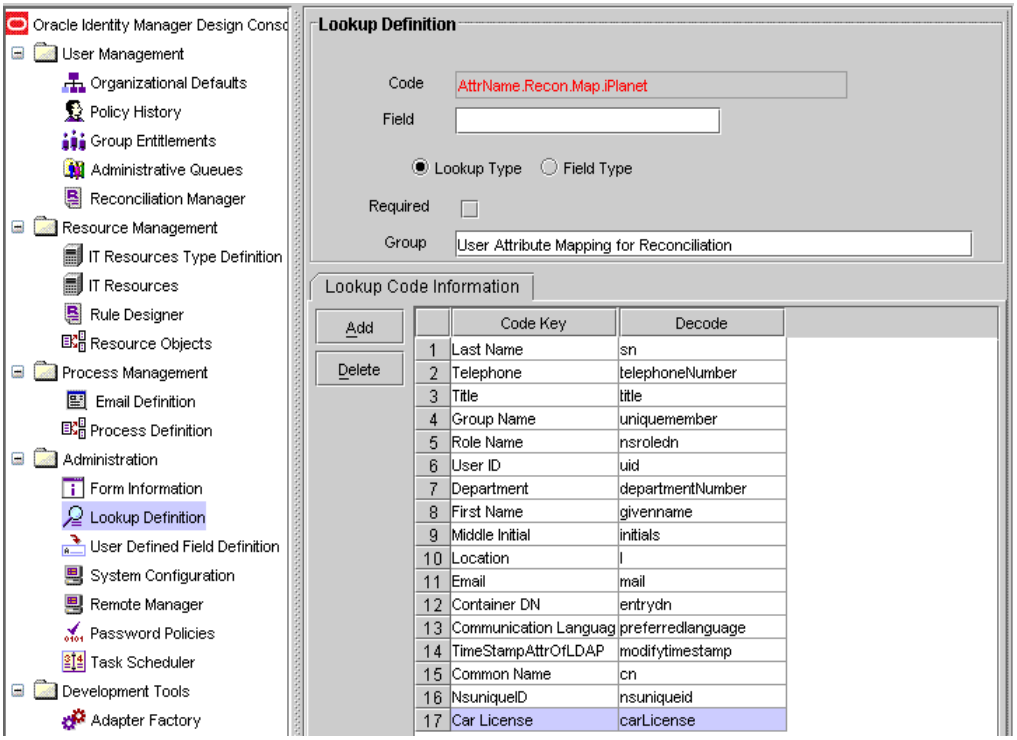
b. Search for and open the **AttrName.Recon.Map.iPlanet** lookup definition.

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

For example, enter `Car License` in the Code Key column and then enter `carLicense` in the Decode column.



d. Save and close the lookup definition.

e. Search for and open the **Lookup.iPlanet.Configuration** lookup definition.

f. 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.

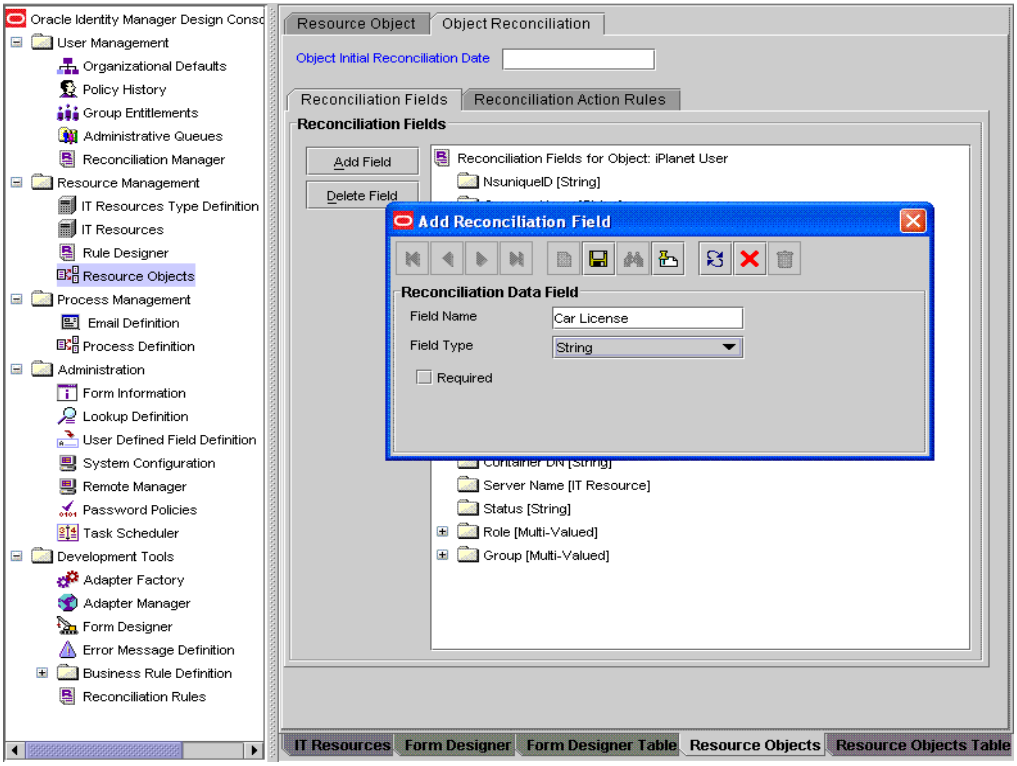
b. Search for the **iPlanet User** process.

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

For example, if you want to add the car license attribute, then specify the following values:

Field Name: `Car License`

Field Type: `String`



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

e. Click the **Save** icon.

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.

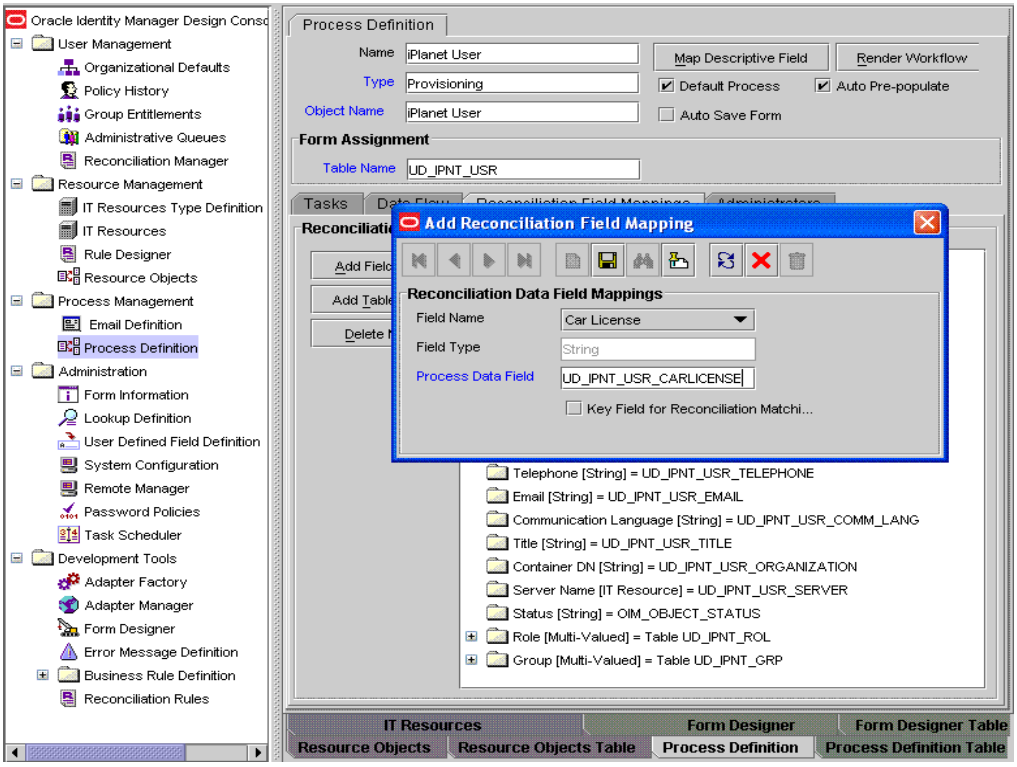
c. On the Reconciliation Field Mappings tab, create a reconciliation field mapping for the attribute.

For example, if you want to add the car license attribute, then specify the following values:

Field Name: `Car License`

Field Type: `String`

Process Data Field: `UD_IPNT_USR_CARLICENCSE`



4.2 Adding New Multivalued Attributes for Target Resource Reconciliation

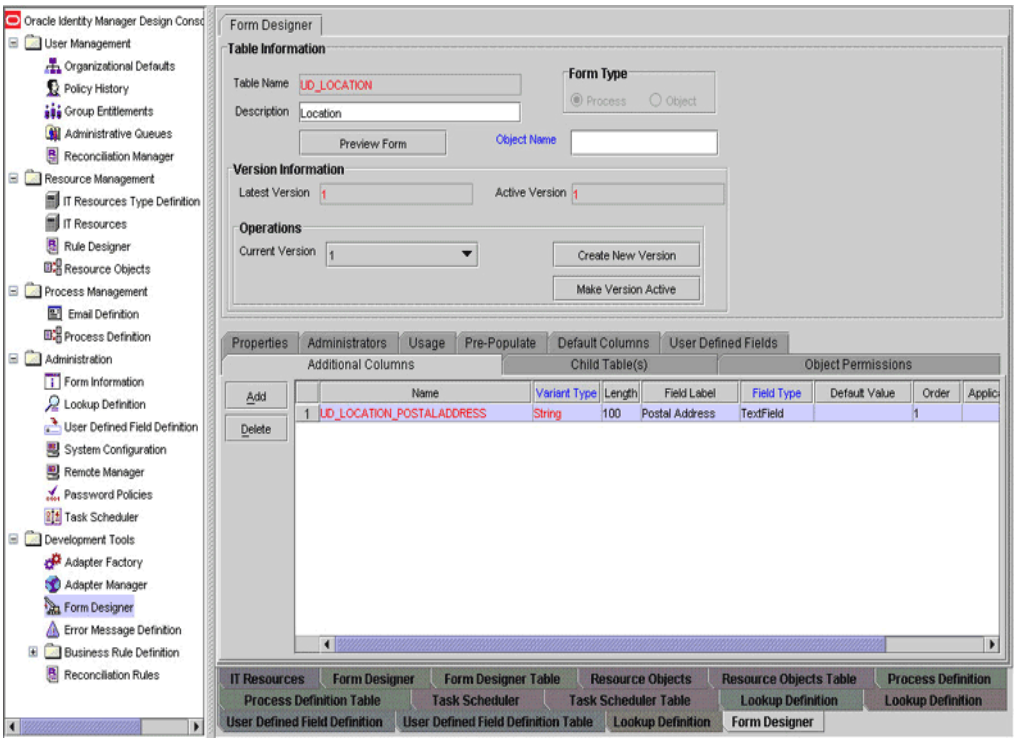
Note: You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

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.**

   The following screenshot shows a sample form:



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

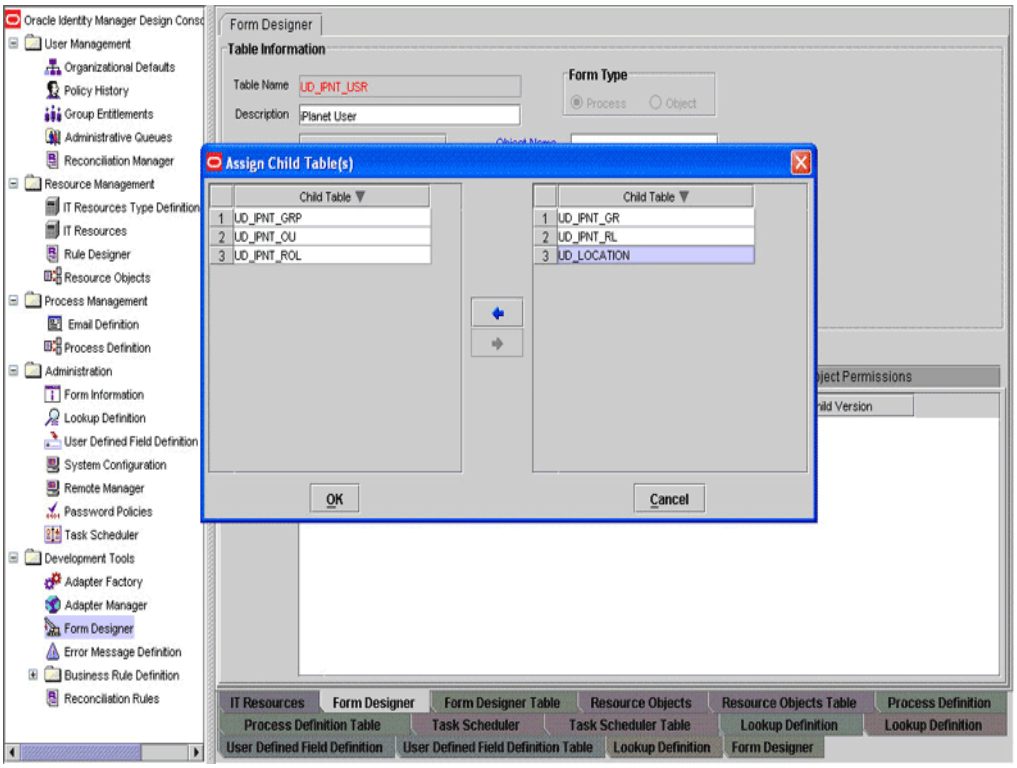
   a. Search for and open the **UD_IPNT_USR** process form.

   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**.

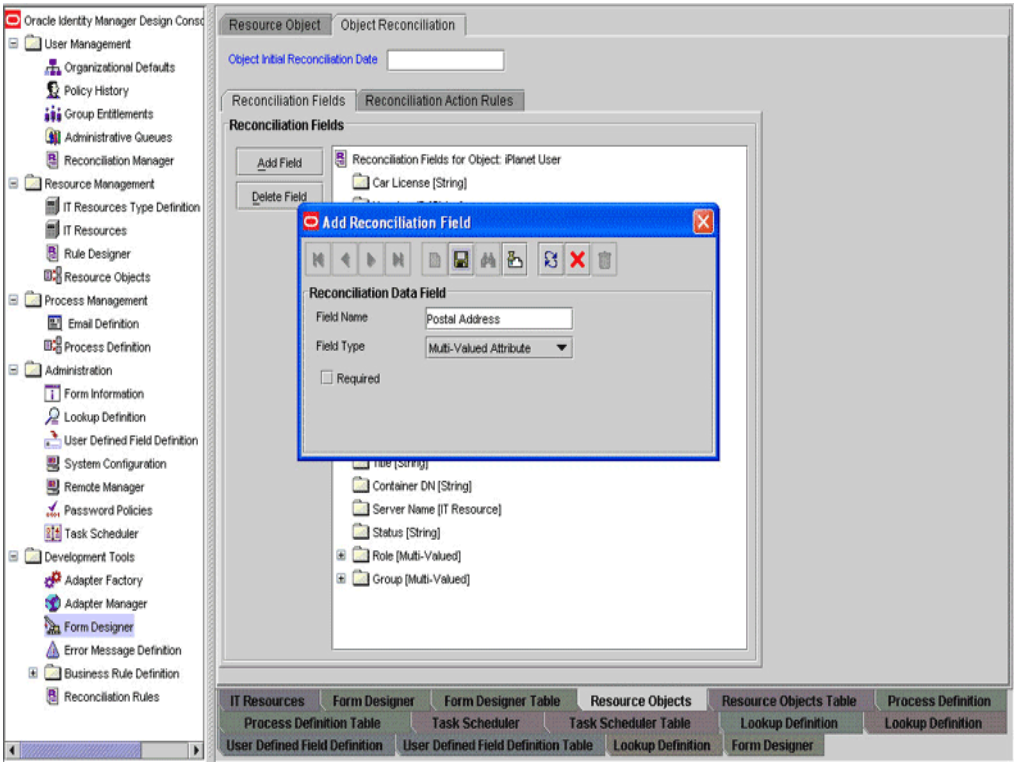
b. Double-click **Resource Objects**.

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 `Postal Address` 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 `Postal Address` in the **Field Name** field and select **String** from the Field Type list.

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

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

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

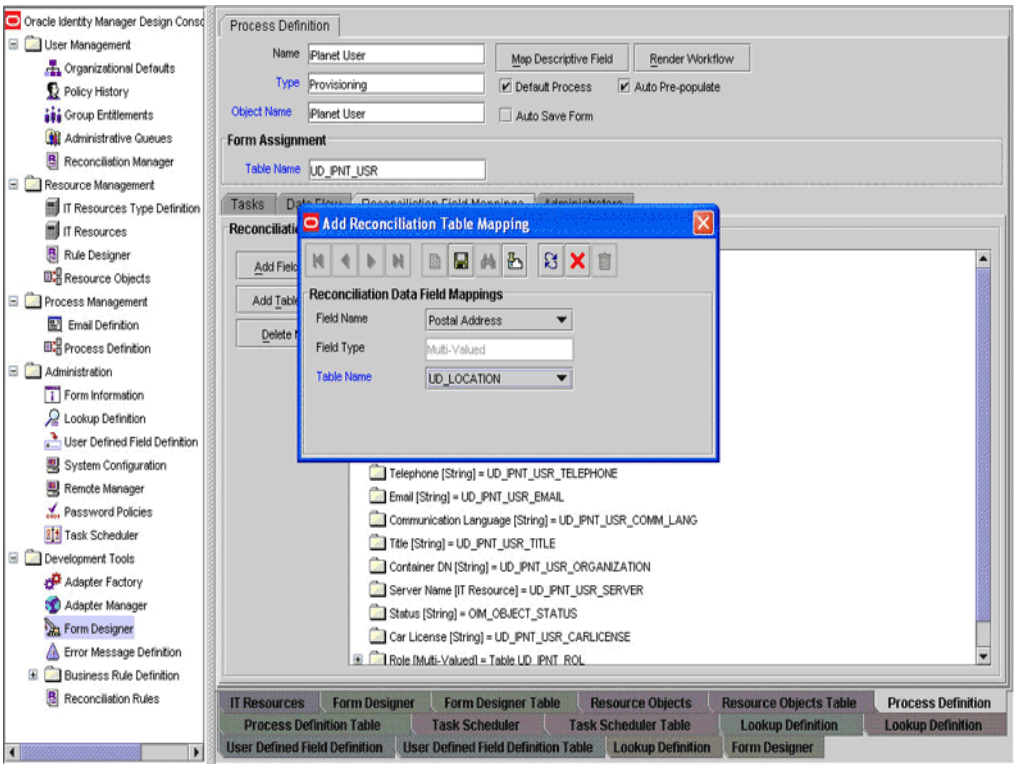
a. Expand **Process Management**.

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.**

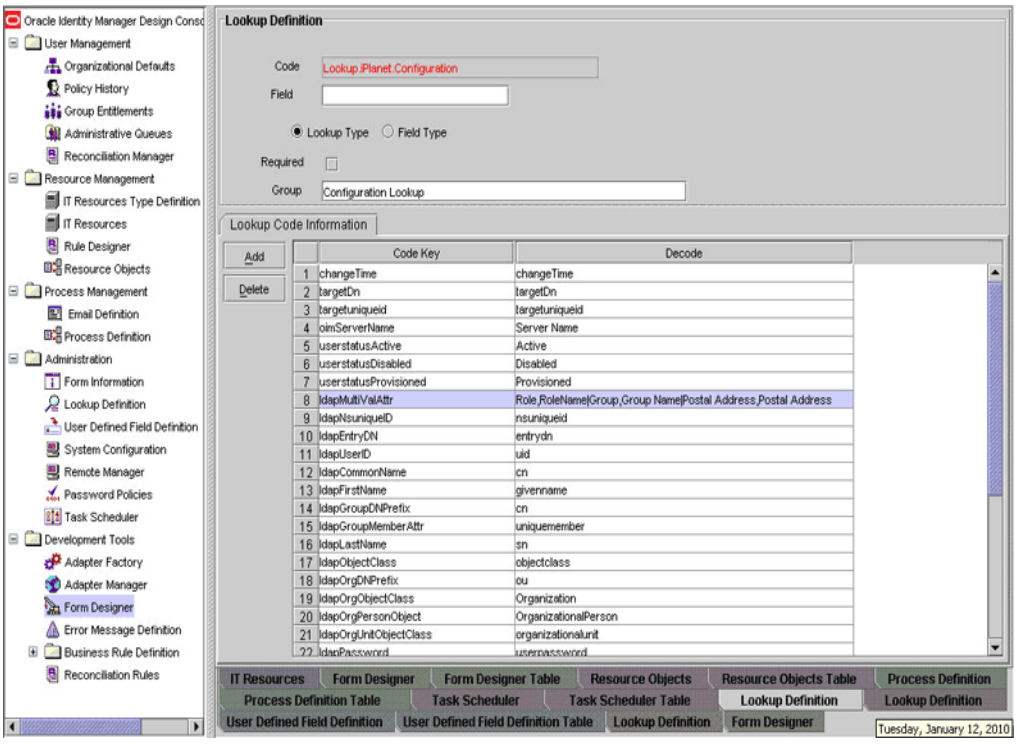
c. Search for and open the **Lookup.iPlanet.Configuration** lookup definition.

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

```
|Postal Address;Postal Address
```

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



e. Search for and open the `AttrName.Recon.Map.iPlanet` lookup definition.

f. 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.

4.3 Adding New Attributes for Group Reconciliation

By default, the attributes listed in Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning" 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 Section 2.1.2.1, "Creating a Target System User Account for Connector Operations", 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_GR** form for Group Recon.

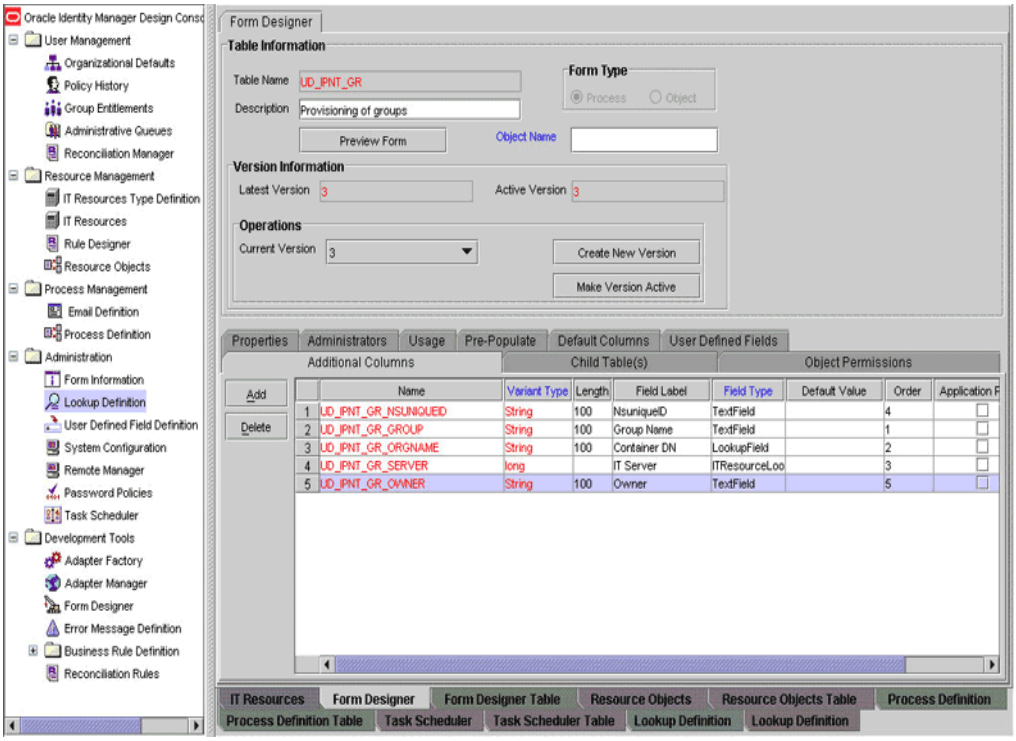
c. Create a new version of the form.

d. Add the new attribute on the form.

For example, if you want to add the Owner attribute, then enter the following values on the Additional Columns tab:

Field	Value
Name	OWNER
Variant Type	String
Length	100

Field	Value
Field Label	Owner
Order	5



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.

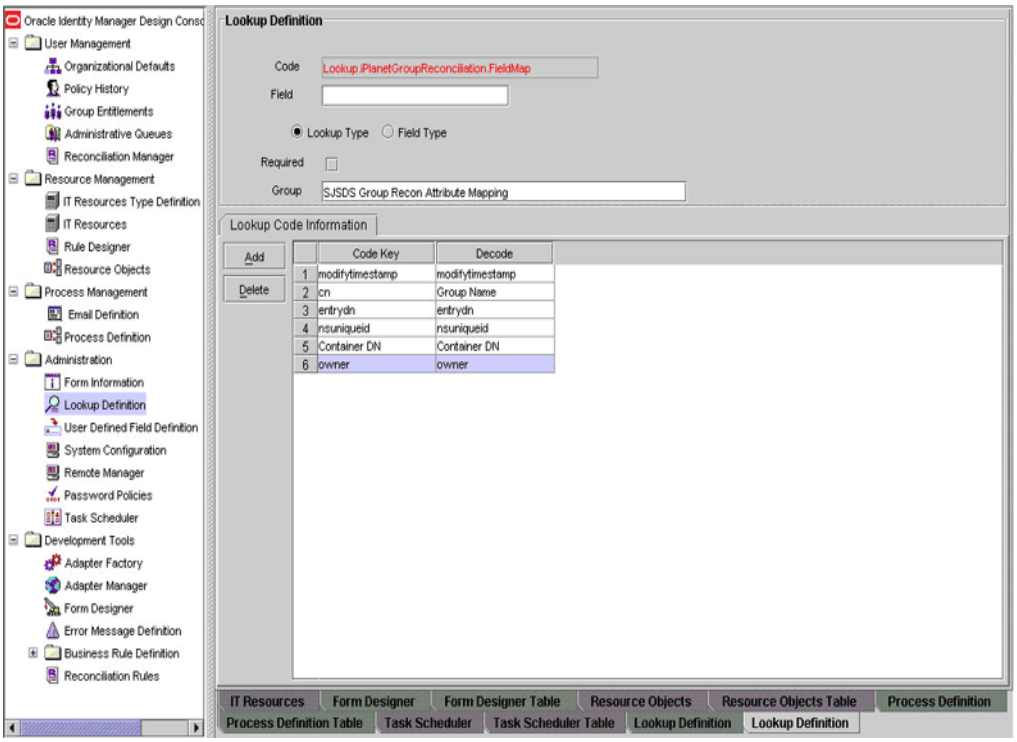
b. Search for and open the **Lookup.iPlanetGroupReconciliation.FieldMap** lookup definition for Group Recon.

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

For example, enter `owner` in the Code Key column and then enter `owner` in the Decode column.



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

   a. Open the Resource Objects form.

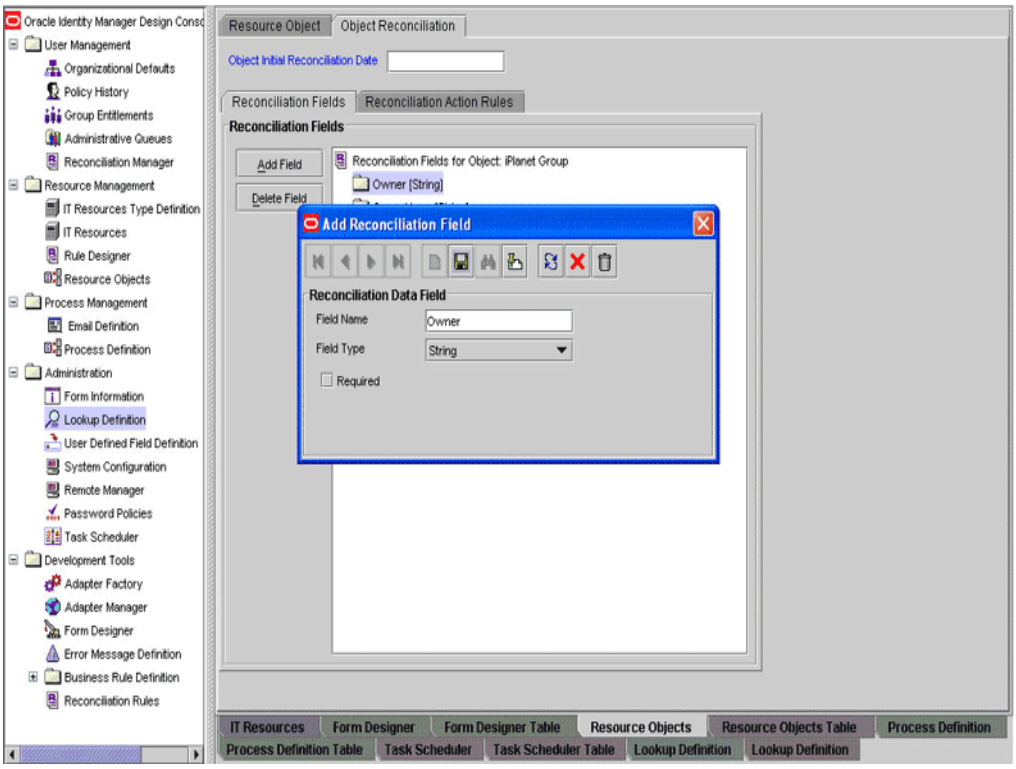
   b. Search for the **iPlanet Group** process.

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

      For example, if you want to add the Owner attribute, then specify the following values:

      Field Name: `Owner`

      Field Type: `String`



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

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 Group** process.

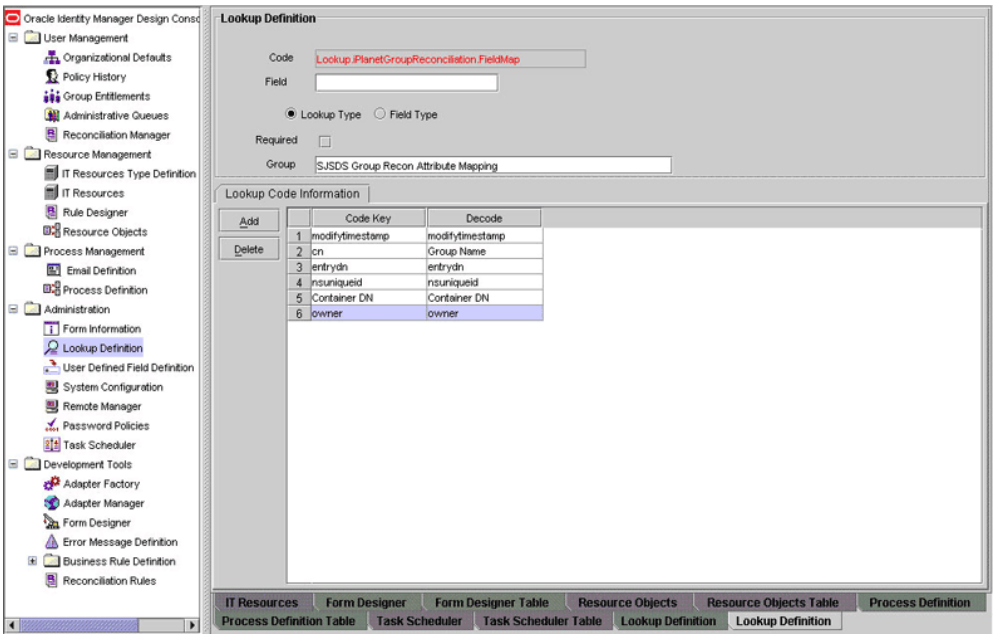
c. On the Reconciliation Field Mappings tab, create a reconciliation field mapping for the attribute.

For example, if you want to add the owner attribute, then specify the following values:

Field Name: `Owner`

Field Type: `String`

Process Data Field: `UD_IPNT_GR_OWNER`



4.4 Adding New Attributes for Role Reconciliation

By default, the attributes listed in Section 1.6.3, "Role Attributes for Target Resource Reconciliation and Provisioning" 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 Section 2.1.2.1, "Creating a Target System User Account for Connector Operations", 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 ||
      ```

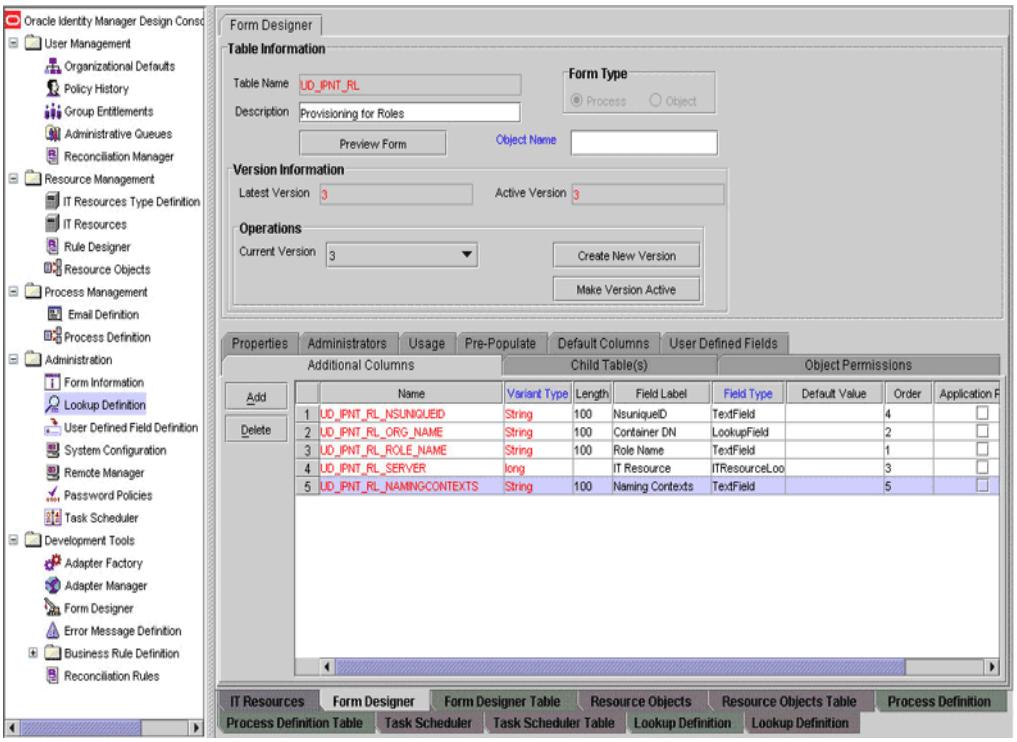
```
preferredDeliveryMethod || jpegPhoto || nsRoleDN || audio ||
internationaliSDNNumber || owner || postalAddress || roomNumber ||
givenName || carLicense || userPKCS12 || searchGuide || userPassword ||
teletexTerminalIdentifier || mobile || manager || entrydn || objectClass ||
userSMIMECertificate || 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_RL** form for Role Recon.
   c. Create a new version of the form.
   d. Add the new attribute on the form.

      For example, if you want to add the Naming Contexts attribute, then enter the following values on the Additional Columns tab:

Field	Value
Name	NAMINGCONTEXTS
Variant Type	String
Length	100
Field Label	Naming Contexts
Order	5



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.

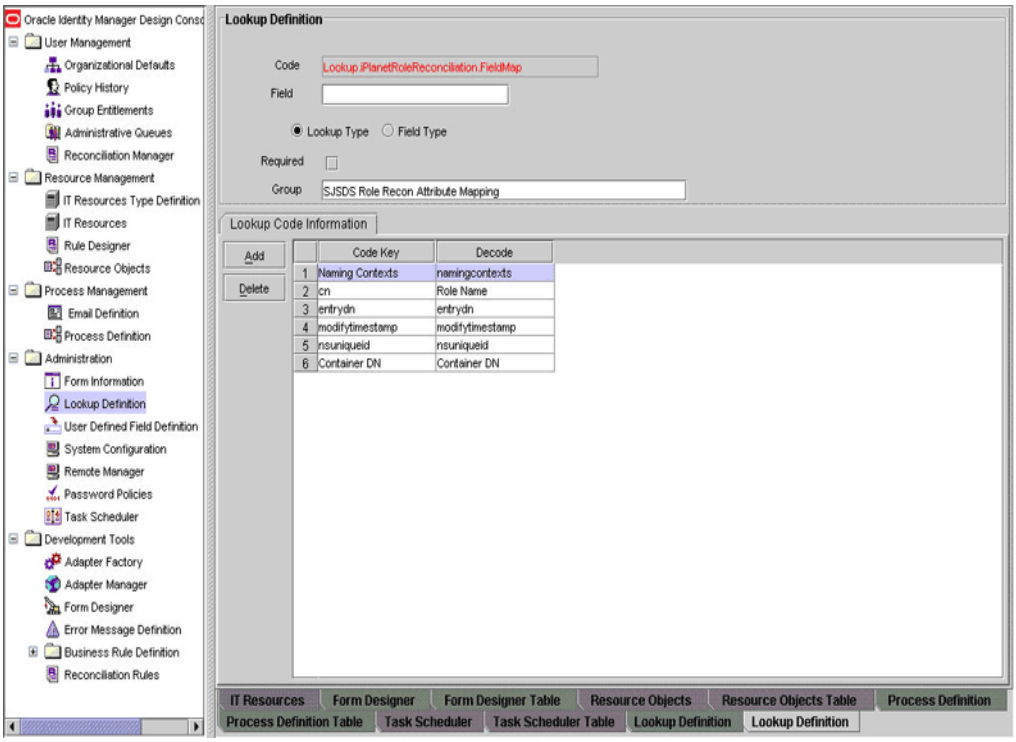
b. Search for and open the **Lookup.iPlanetRoleReconciliation.FieldMap** lookup definition for Role Recon.

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

For example, enter `Naming Contexts` in the Code Key column and then enter `namingcontexts` in the Decode column.



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

   a. Open the Resource Objects form.

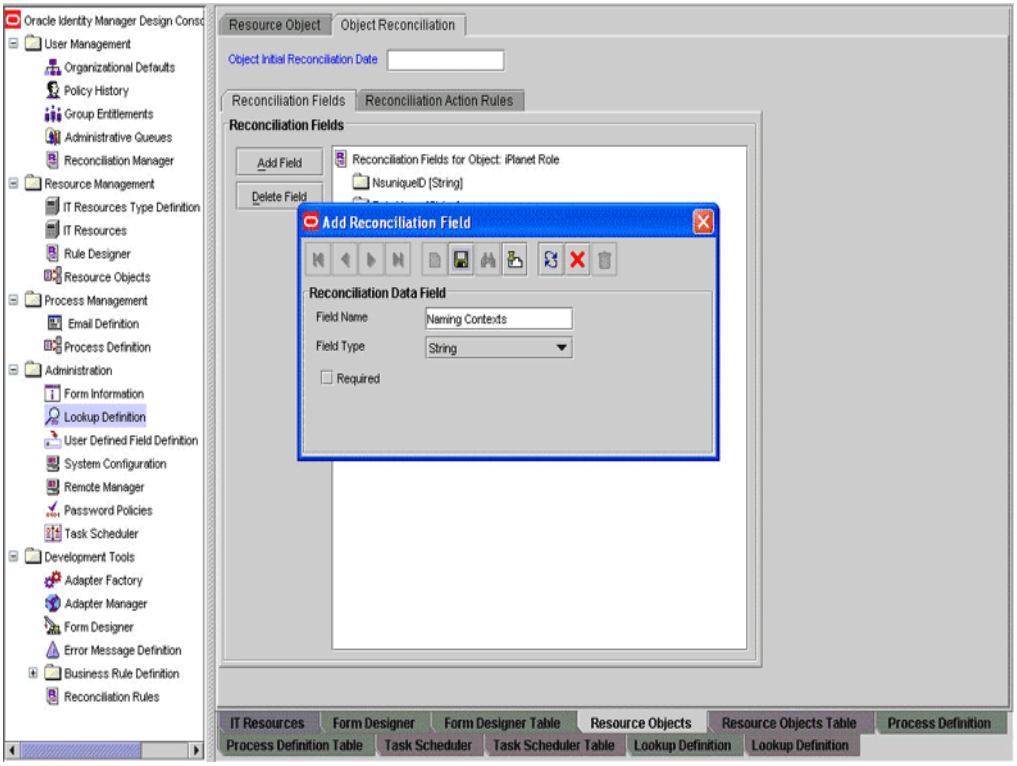
   b. Search for the **iPlanet Role** process.

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

      For example, if you want to add the Naming Contexts attribute, then specify the following values:

      Field Name: `Naming Contexts`

      Field Type: `String`



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

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 Role** process.

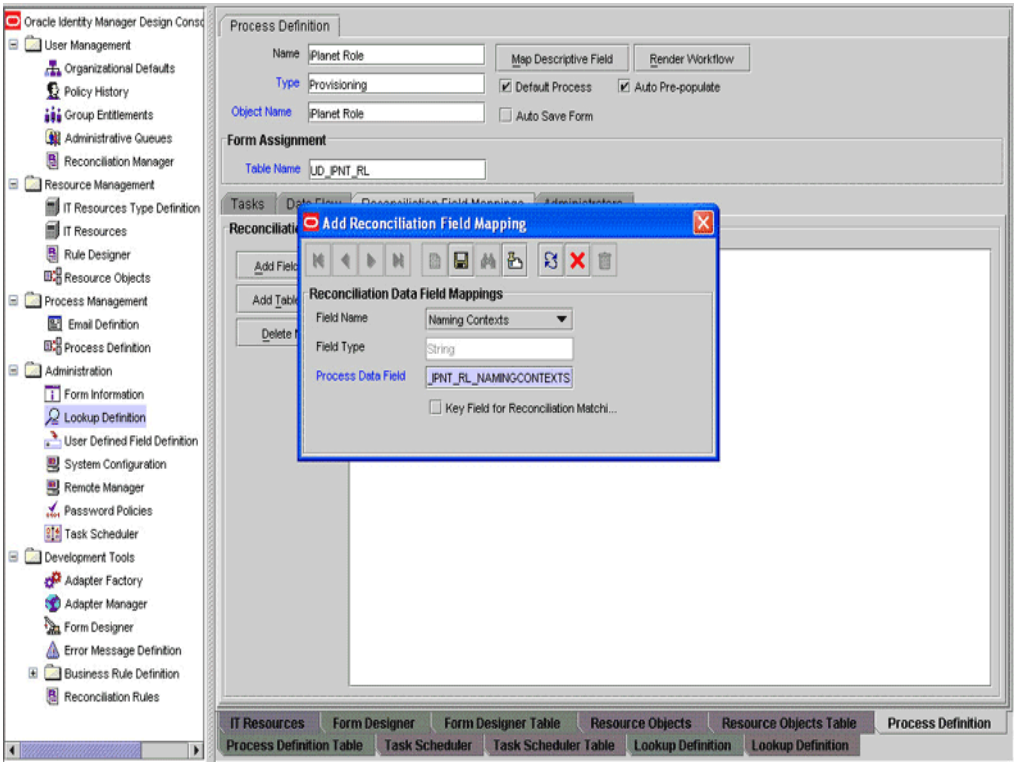
c. On the Reconciliation Field Mappings tab, create a reconciliation field mapping for the attribute.

For example, if you want to add the Naming Contexts attribute, then specify the following values:

Field Name: `Naming Contexts`

Field Type: `String`

Process Data Field: `UD_IPNT_RL_NAMINGCONTEXTS`



4.5 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 Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation."

By default, the attributes listed in Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning" 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:

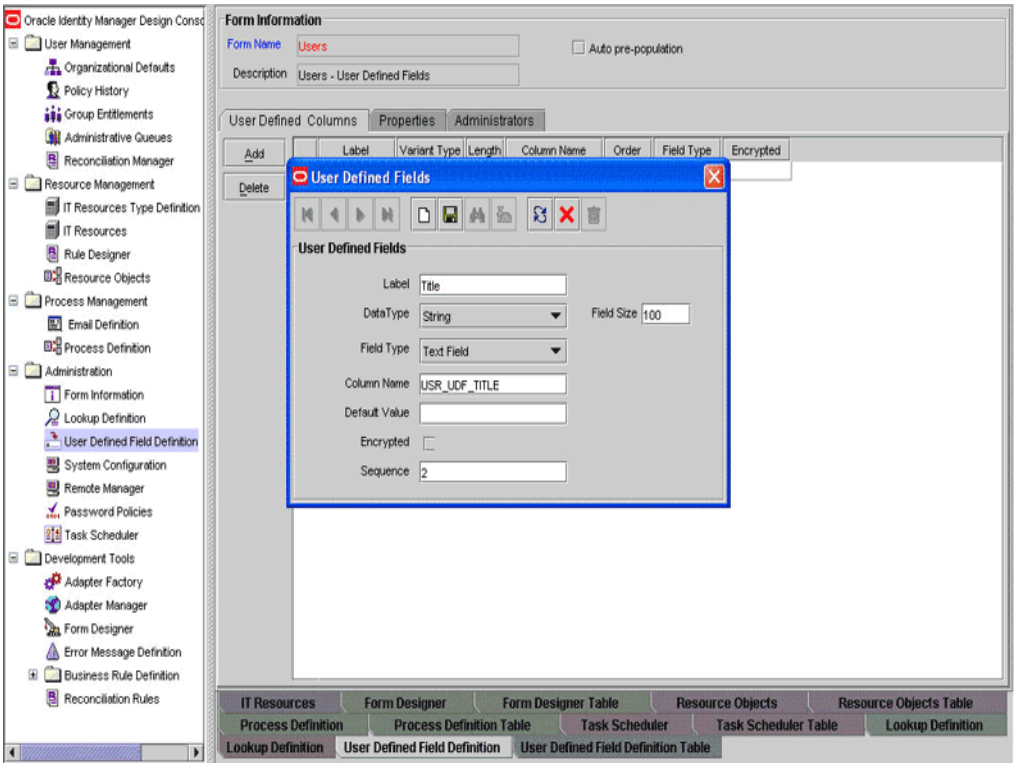
See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

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 **Administration**.
   b. Double-click **User Defined Field Definition.**
   c. Search for and open the **Users** form.

d. Click **Add**.

e. Enter the details of the attribute.

For example, if you are adding the Title attribute, then enter `Title` in the **Label** field, set the data type to **String**, set the Field Type to **Text Field**, enter `USR_UDF_TITLE` as the column name, and enter a value in the Field Size box.



f. Click **Save**.

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

a. Expand **Resource Management**.

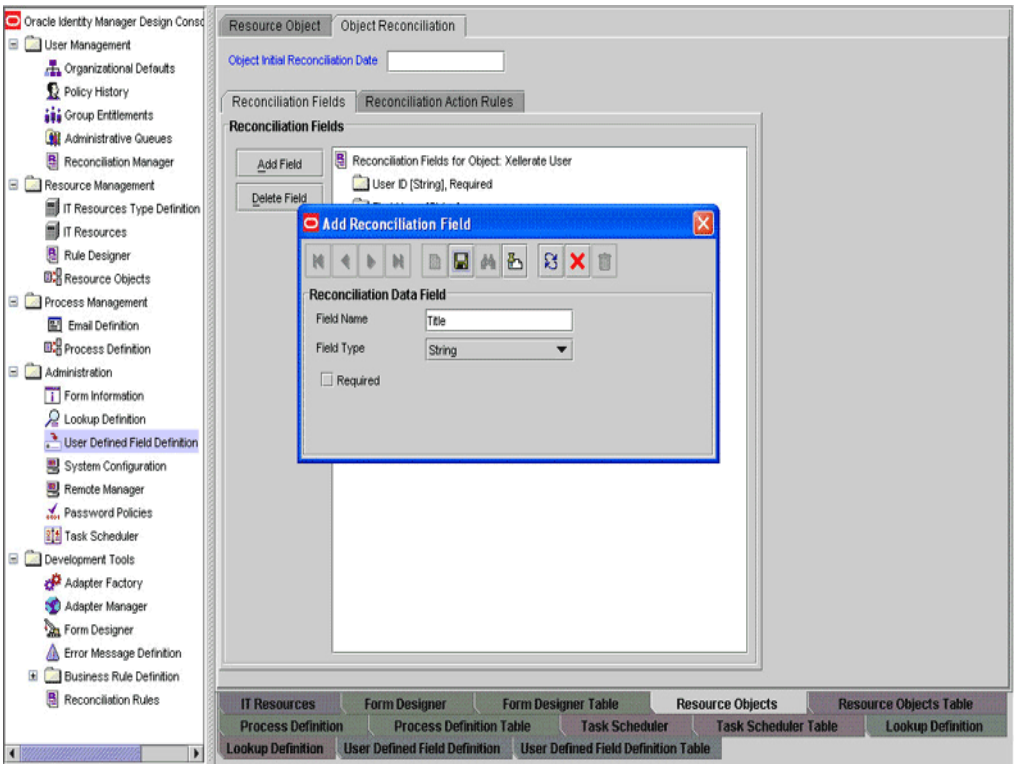
b. Double-click **Resource Objects.**

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

g. Click **Save**.

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

   a. Expand **Process Management**.

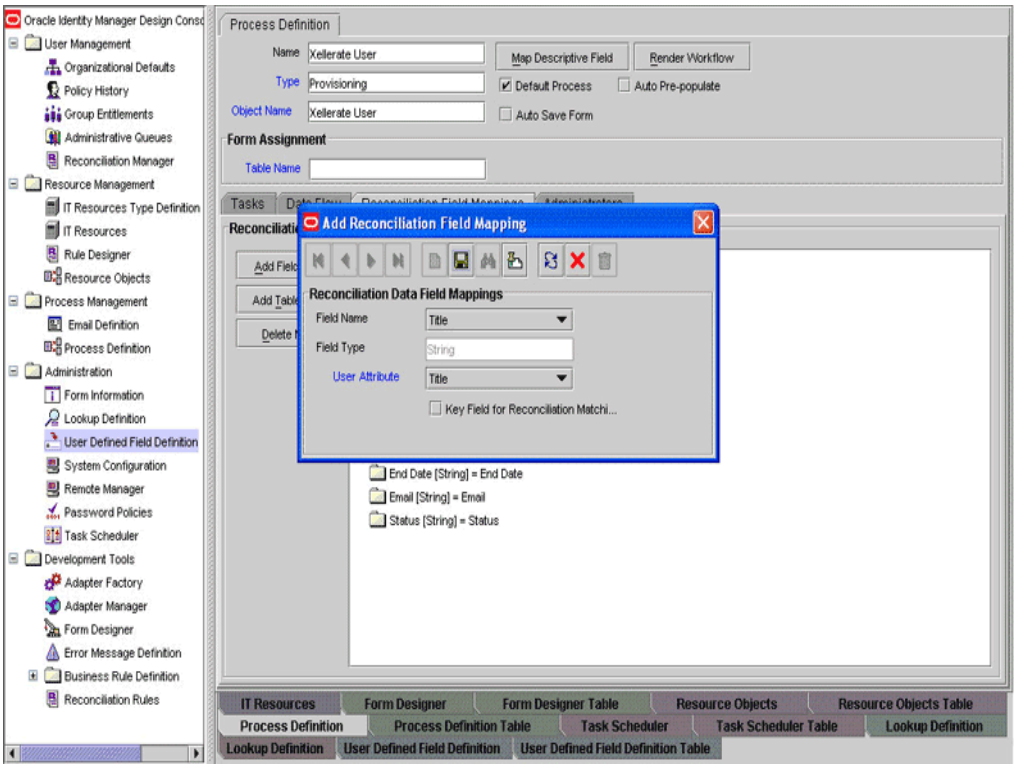
   b. Double-click **Process Definition**.

   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 user attribute that you want to add.

      For example, from the Field Name list select **Title,** and from the User Attribute list select **Title.**



f. Click **Save**.

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

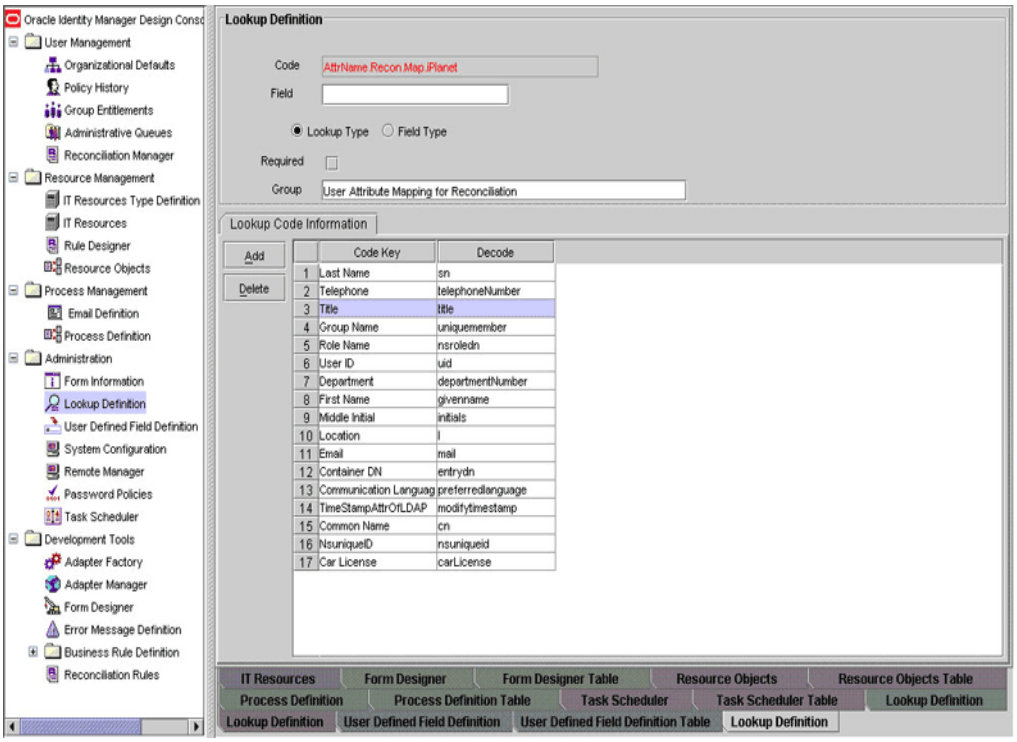
   a. Expand **Administration**.

   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**.

4.6 Adding New Attributes for Provisioning

By default, the attributes listed in Section 1.6.6, "Provisioning Functions" 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 Fusion Middleware User's Guide for Oracle Identity Manager* for detailed instructions on performing the following procedure

To add a new attribute for provisioning:

1. While performing the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations," 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:** Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

d. In the **Lookup.iPlanet.Configuration** 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>
```

Note: Perform steps 6 through 8 only if you want to perform request-based provisioning.

---

6. Update the request dataset.

When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, while performing Step 4 of this procedure, if you added Employee ID as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Employee ID"
attr-ref = "Employee ID"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this AttributeReference element:

– For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_IPNT_USR_EMP_ID is the value in the Name column of the process form, then you must specify `Employee ID` as the value of the name attribute in the AttributeReference element.

– For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 4.

– For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 4.

- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 4.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 4.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 4, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

7. Run the PurgeCache utility to clear content related to request datasets from the server cache.

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

8. Import into MDS the request dataset definitions in XML format.

See Section 2.3.1.7.3, "Importing Request Datasets into MDS" for detailed information about the procedure.

9. 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.

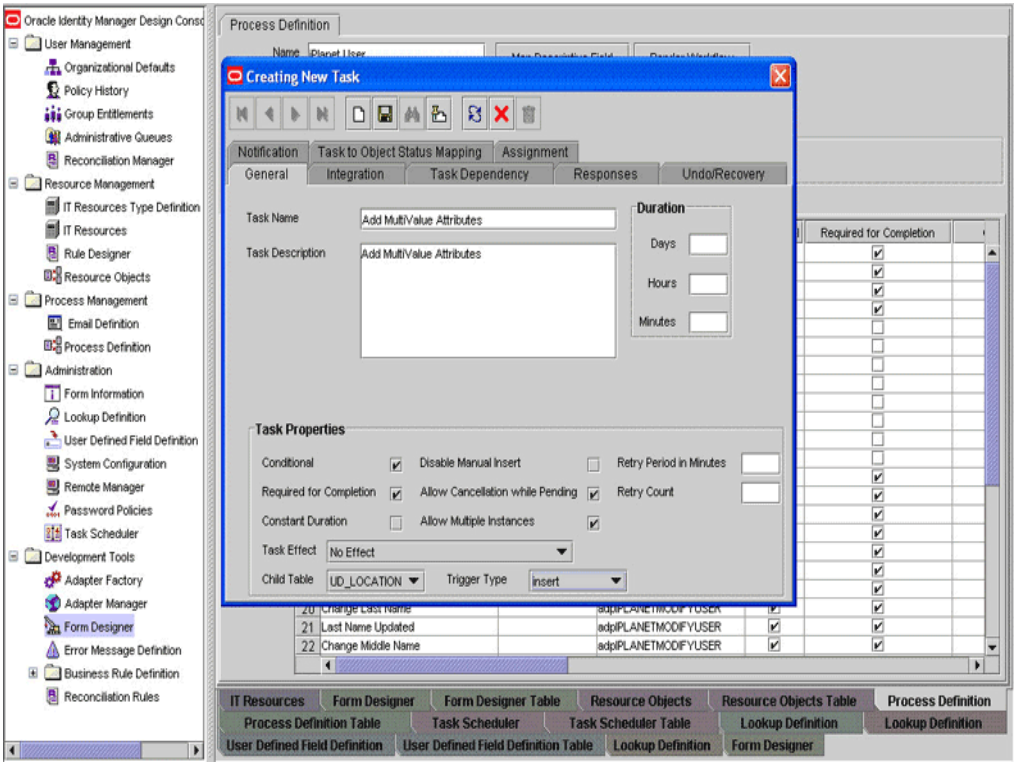
4. In the process definition, add a task for setting a value for the attribute:

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 **Postal Address** from the list.
- From Trigger Type list, select **Insert** for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalue 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.

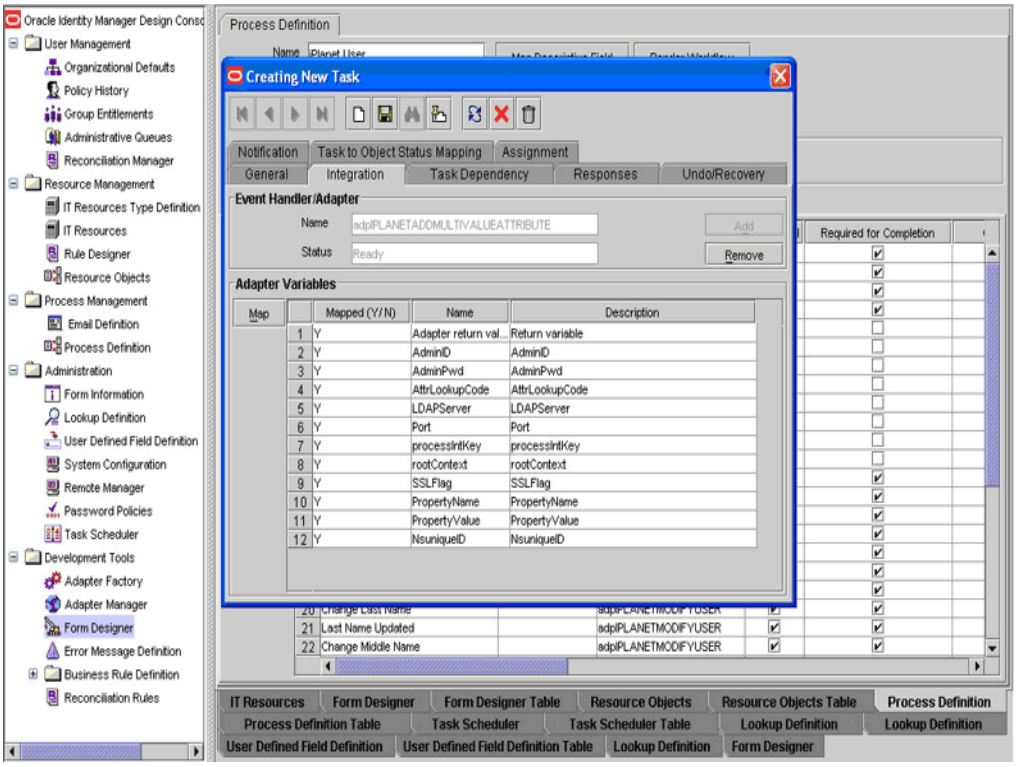
e. To map the adapter variables listed in this table, select the adapter, click **Map**, and then specify the data given in the following table:

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	homepostaladdress **Note:** This is a sample value.	NA

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
AttrLookupCode	String	IT Resources	Server	LDAP Server	For User: Prov Attribute Lookup Code For Group: AtMap.iPlanetGroup For Role: AttrMap.iPlanetRole
LDAPServer	String	IT Resources	Server	LDAP Server	Server Address
Port	String	IT Resources	Server	LDAP Server	Port
PropertyValue	String	Process Data and postal address	Postal 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.

4.7 Adding New Multivalued Attributes for Provisioning

To add new multivalued attributes for provisioning:

1. Create a child form for the multivalued attribute by performing Steps 1 through 3 as described in the Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation."
2. Perform the steps described in the Section , "Enabling Update of New Multivalued Attributes for Provisioning." While performing Step 4.e:
   - While mapping the **PropertyValue** variable, select the **Old value** check box.
   - Map the following additional variables:

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
ITResourceUDF	String	Literal	String	UD_IPNT_USR_SERVER	NA
ProcessInstKey	String	Process Data	Process Instance	NA	NA

4.8 Adding New Attributes for Provisioning of Group

By default, the attributes listed in Section 1.6.6, "Provisioning Functions" 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 Section 2.1.2.1, "Creating a Target System User Account for Connector Operations," 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 ||
```

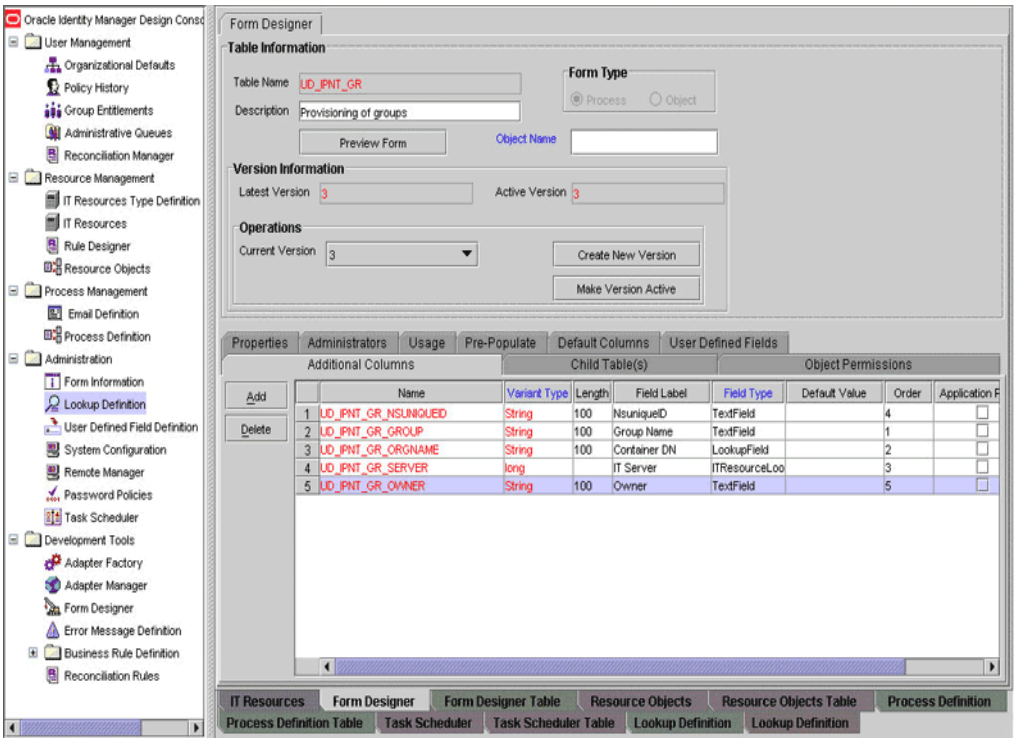
```
nsAccountLock || seeAlso || registeredAddress || postalCode || photo ||
title || uniqueMember || street || pager || departmentNumber || dc || o ||
cn || l || initials || telephoneNumber || preferredLanguage ||
facsimileTelephoneNumber || x121Address || employeeType") (version 3.0;acl
"OIMUserACI";allow (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_GR** form.
   c. Create a new version of the form.
   d. Add the new attribute on the form.

      For example, if you want to add the Owner attribute, then enter the following values on the Additional Columns tab:

Field	Value
Name	Owner
Variant Type	String
Length	100
Field Label	Owner
Order	5



e. Save the form.

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

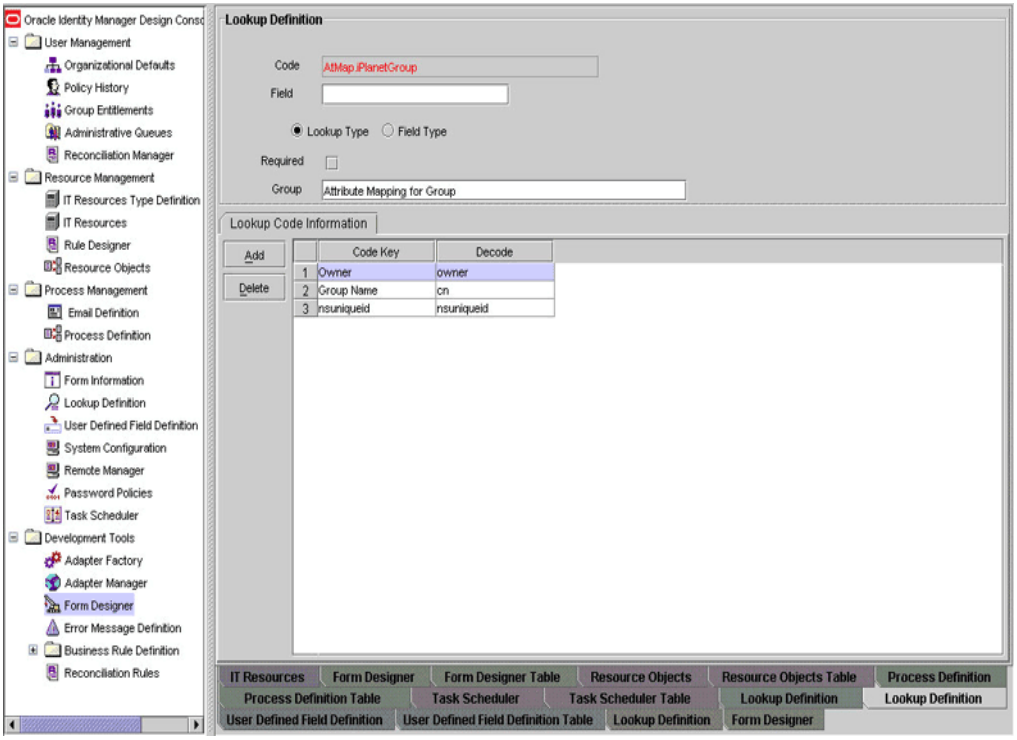
5. In the lookup definition for provisioning, create an entry for the new attribute as follows:

a. Open the Lookup Definition form.

b. Search for and open the **AtMap.iPlanetGroup** 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: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.



Note: Perform steps 6 through 8 only if you want to perform request-based provisioning.

6. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

      See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

      For example, while performing Step 4 of this procedure, if you added Owner as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Owner"
attr-ref = "Owner"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

      In this AttributeReference element:

      – For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_IPNT_GR_OWNER is the value in the Name column of the process form, then you must specify `Owner` as the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 4.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 4.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 4.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 4.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 4, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

7. Run the PurgeCache utility to clear content related to request datasets from the server cache.

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

8. Import into MDS, the request dataset definitions in XML format.

See Section 2.3.1.7.3, "Importing Request Datasets into MDS" for detailed information about the procedure.

9. 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

After you add an attribute for provisioning Group, 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 Group** process definition.

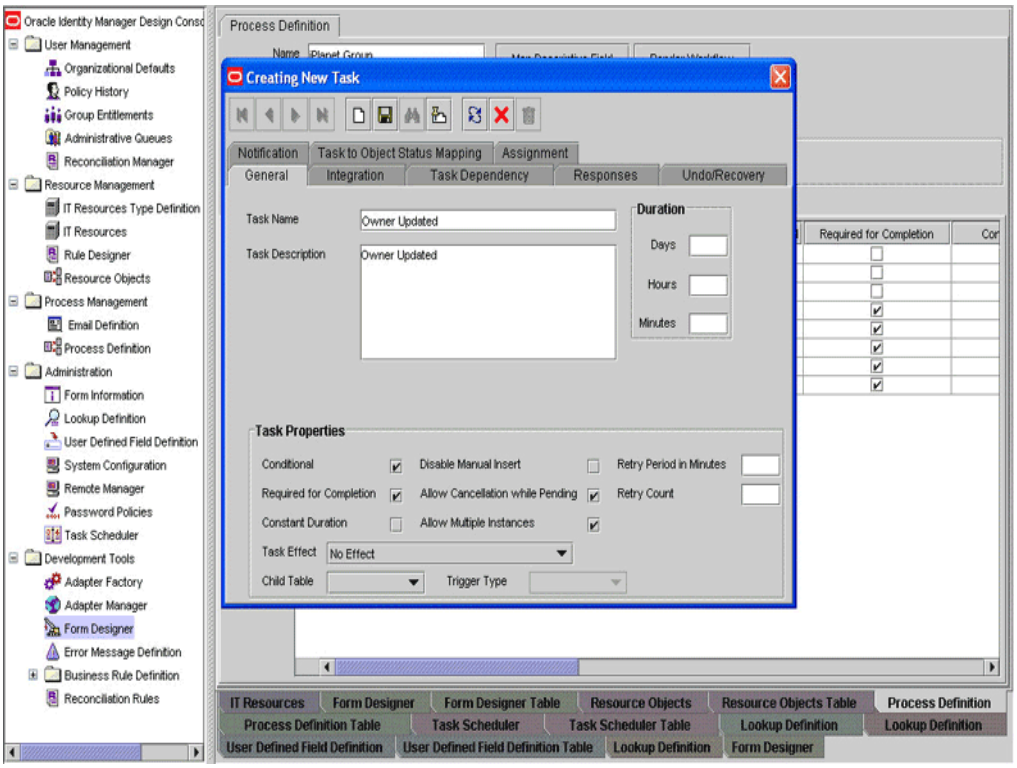
4. In the process definition, add a task for setting a value for the attribute:

a. Click **Add**, enter the name of the task for updating 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



c. On the **Integration** tab, click **Add**, and then click **Adapter**.

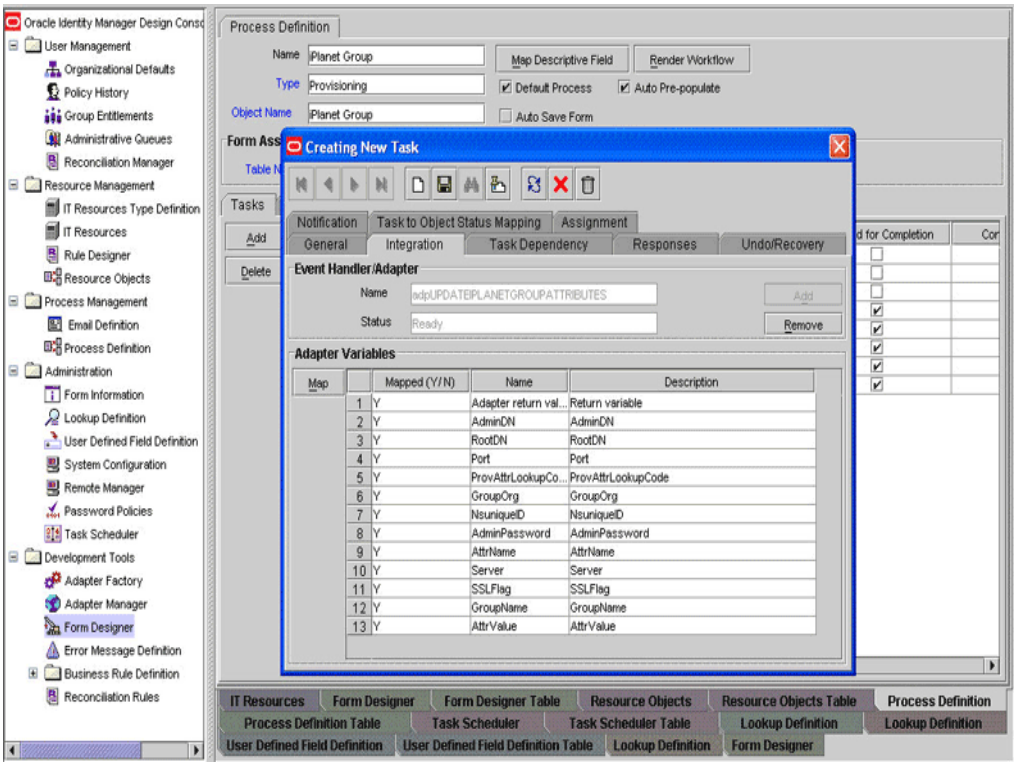
d. Select the **adpUPDATEIPLANETGROUPATTRIBUTES** adapter, click **Save**, and then click OK in the message.

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	AtMap.iPlanetGroup
LDAPServer	String	IT Resources	Server	LDAP Server	Server Address
Port	String	IT Resources	Server	LDAP Server	Port

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
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

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

To update a new multivalued attribute for provisioning of Groups, perform the steps mentioned in Enabling Update of New Multivalued Attributes for Provisioning section.

4.9 Adding New Attributes for Provisioning of Role

By default, the attributes listed in Section 1.6.6, "Provisioning Functions" 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 Section 2.1.2.1, "Creating a Target System User Account for Connector Operations," 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.

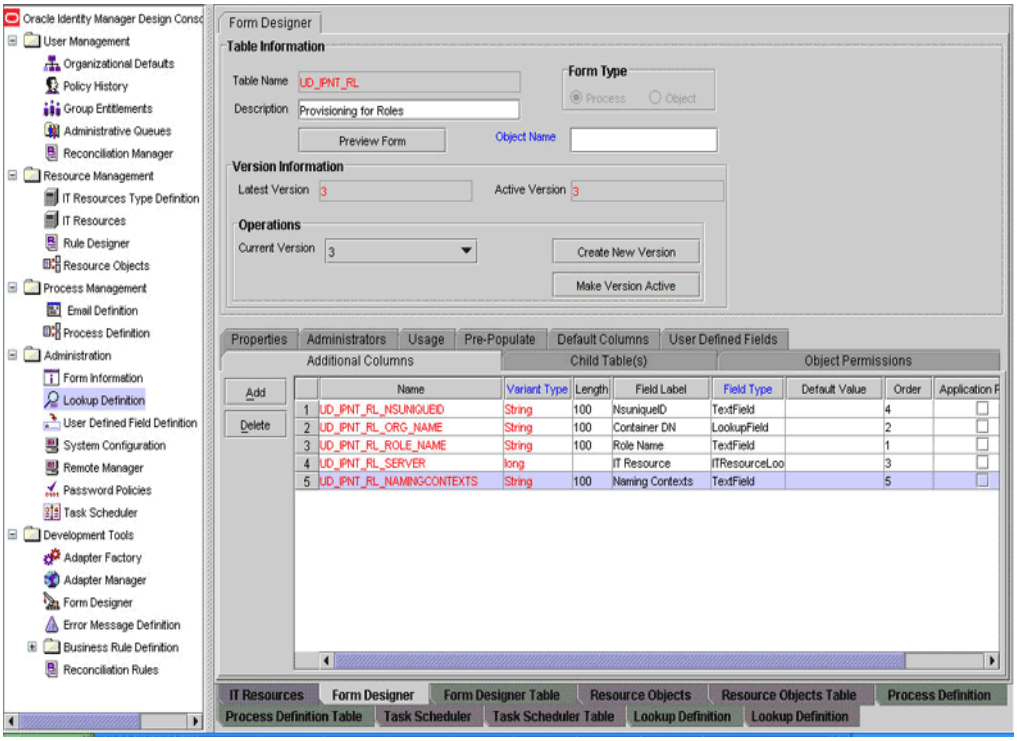
b. Search for and open the **UD_IPNT_RL** form.

c. Create a new version of the form.

d. Add the new attribute on the form.

For example, if you want to add the Naming Contexts attribute, then enter the following values on the Additional Columns tab:

Field	Value
Name	NAMINGCONTEXTS
Variant Type	String
Length	100
Field Label	Naming Contexts
Order	5



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:

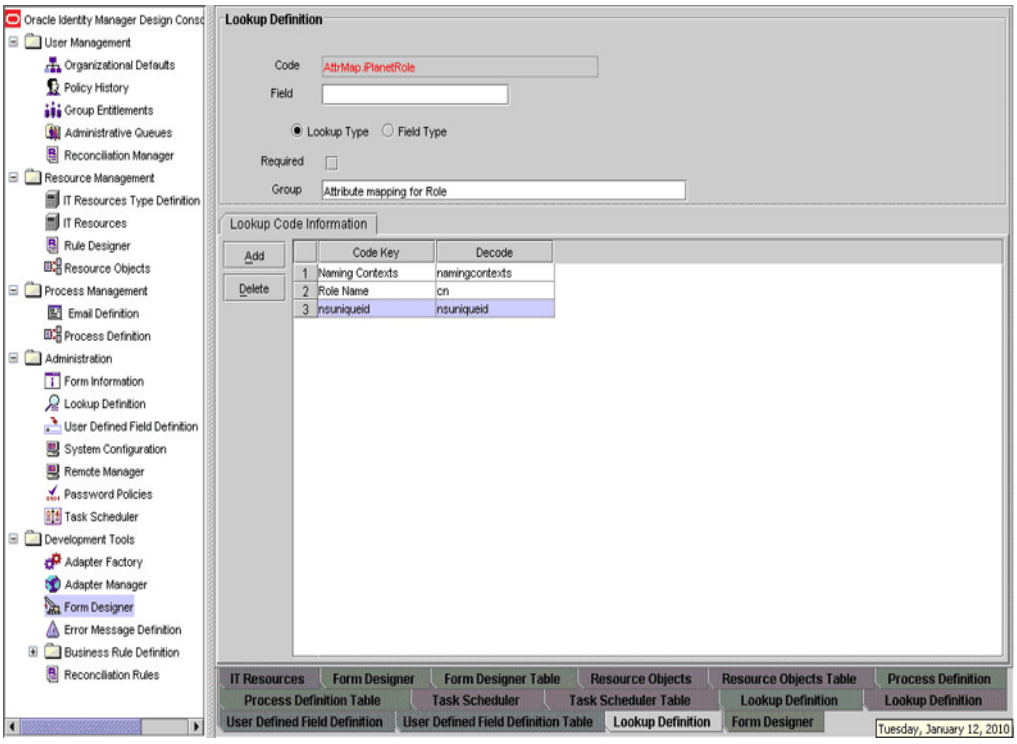
a. Open the Lookup Definition form.

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



Note: Perform steps 6 through 8 only if you want to perform request-based provisioning.

6. Update the request dataset.

   When you add an attribute on the process form, you also update the XML file containing the request dataset definitions. To update a request dataset:

   a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

   b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

      See Also: The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

      For example, while performing Step 4 of this procedure, if you added Naming Contexts as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Naming Contexts"
attr-ref = "Naming Contexts"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

      In this AttributeReference element:

      – For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_IPNT_RL_NAMINGCONTEXTS is the value in the Name column of the process form, then you must specify `Naming Contexts` as the value of the name attribute in the AttributeReference element.

- For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 4.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 4.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 4.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 4.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

While performing Step 4, if you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

7. Run the PurgeCache utility to clear content related to request datasets from the server cache.

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

8. Import into MDS, the request dataset definitions in XML format.

See Section 2.3.2.1.2, "Using the Certificate Signing Request to Generate the CA and SSL Certificates" for detailed information about the procedure.

9. 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 Role

After you add an attribute for provisioning 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. Double-click **Process Definition** and open the **iPlanet Role** process definition.

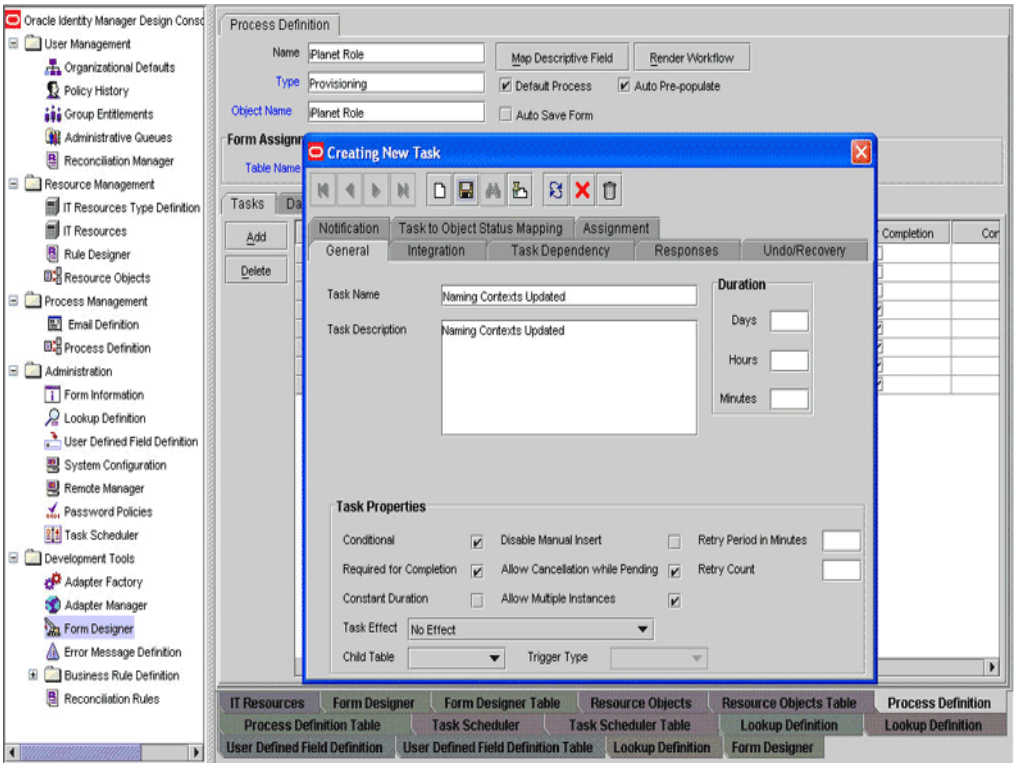
4. In the process definition, add a task for setting a value for the attribute:

a. Click **Add**, enter the name of the task for updating attribute, 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



c. On the **Integration** tab, click **Add**, and then click **Adapter**.

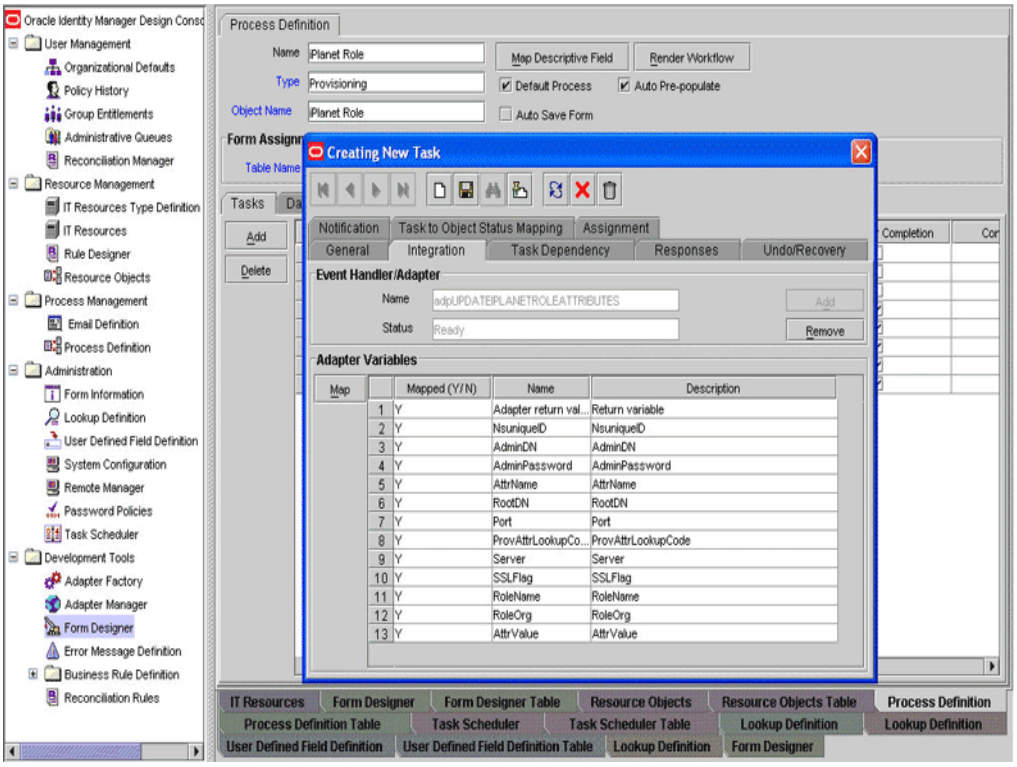
d. Select the **adpUPDATEIPLANETROLEATTRIBUTES** adapter, click **Save**, and then click OK in the message.

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	AttrMap.iPlanetRole
LDAPServer	String	IT Resources	Server	LDAP Server	Server Address
Port	String	IT Resources	Server	LDAP Server	Port

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
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 Role

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

To update a new multivalued attribute for provisioning of Roles, perform the steps mentioned in Enabling Update of New Multivalued Attributes for Provisioning section.

4.10 Adding New Object Classes for Reconciliation and Provisioning

To add a new object classes for reconciliation and provisioning:

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

1. Section 4.10.1, "Assigning Permissions for Using the Attribute"
2. Section 4.10.2, "Adding the Attributes of the Object Class to the Process Form"

3. Section 4.10.3, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning"
4. Section 4.10.4, "Adding the Attributes of the Object Class to the Resource Object"
5. Section 4.10.5, "Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation"
6. Section 4.10.6, "Adding attributes of the Object Class to the Provisioning Process"

4.10.1 Assigning Permissions for Using the Attribute

While performing the procedure described in Section 2.1.2.1, "Creating a Target System User Account for Connector Operations," 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**.

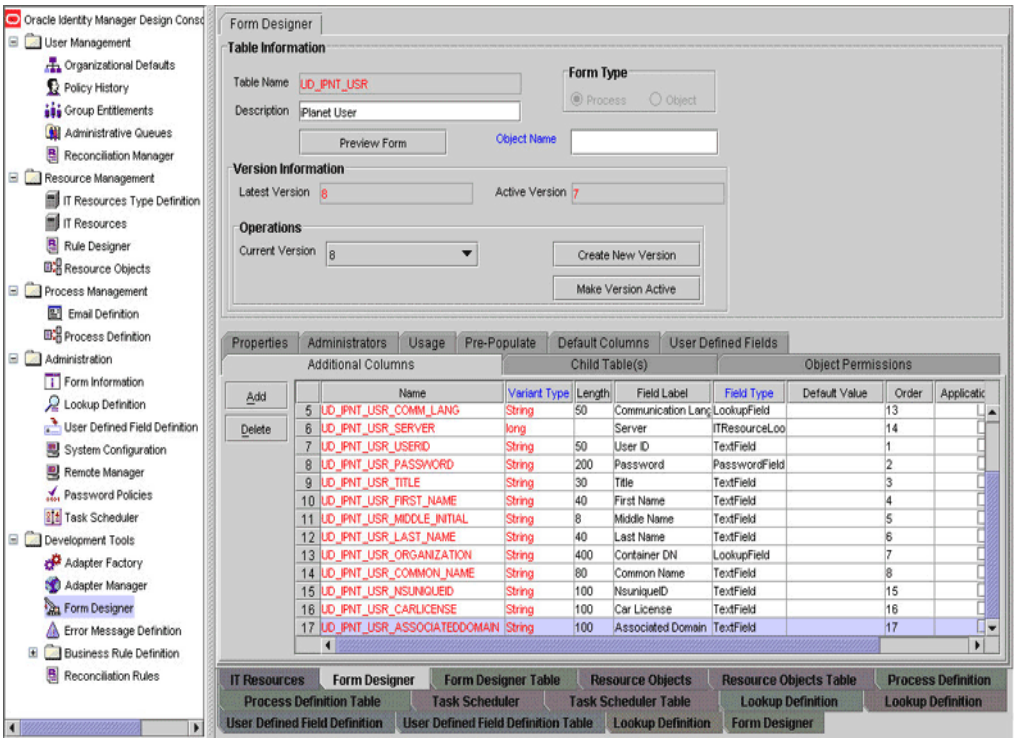
4.10.2 Adding the Attributes of the Object Class to the Process Form

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.**

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

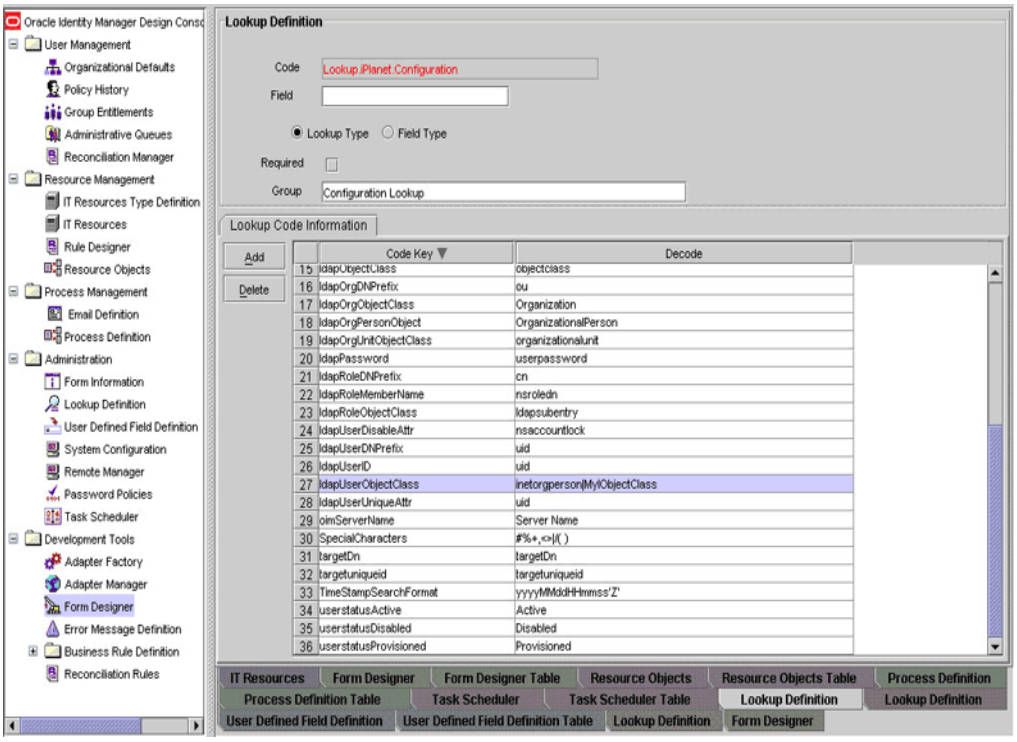
To add the object class and its attributes to the lookup definition for provisioning:

1. Expand the **Administration** folder.
2. Double-click **Lookup Definition.**
3. Search for and open the **Lookup.iPlanet.Configuration** 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`**

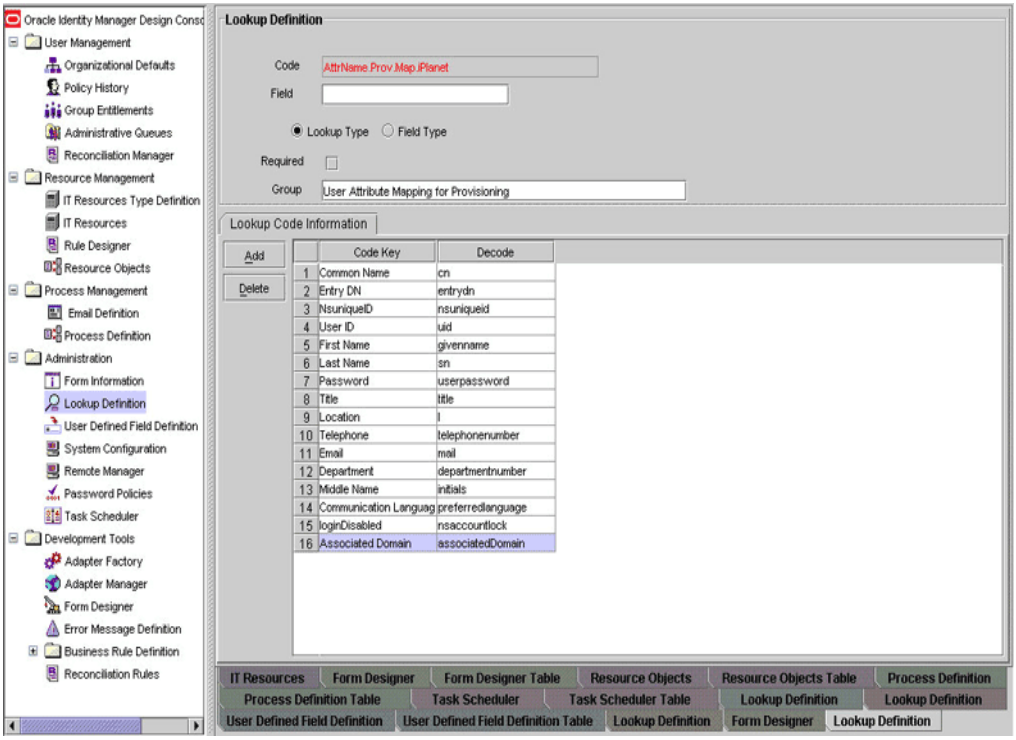


5. Search for and open the **AttrName.Prov.Map.iPlanet** lookup definition.
6. Click **Add** and then enter the Code Key and Decode values for an attribute of the object class. The Code Key value must be the name of the field on the process form and Decode value must be the name of the field on the target 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.

7. Click **Save.**



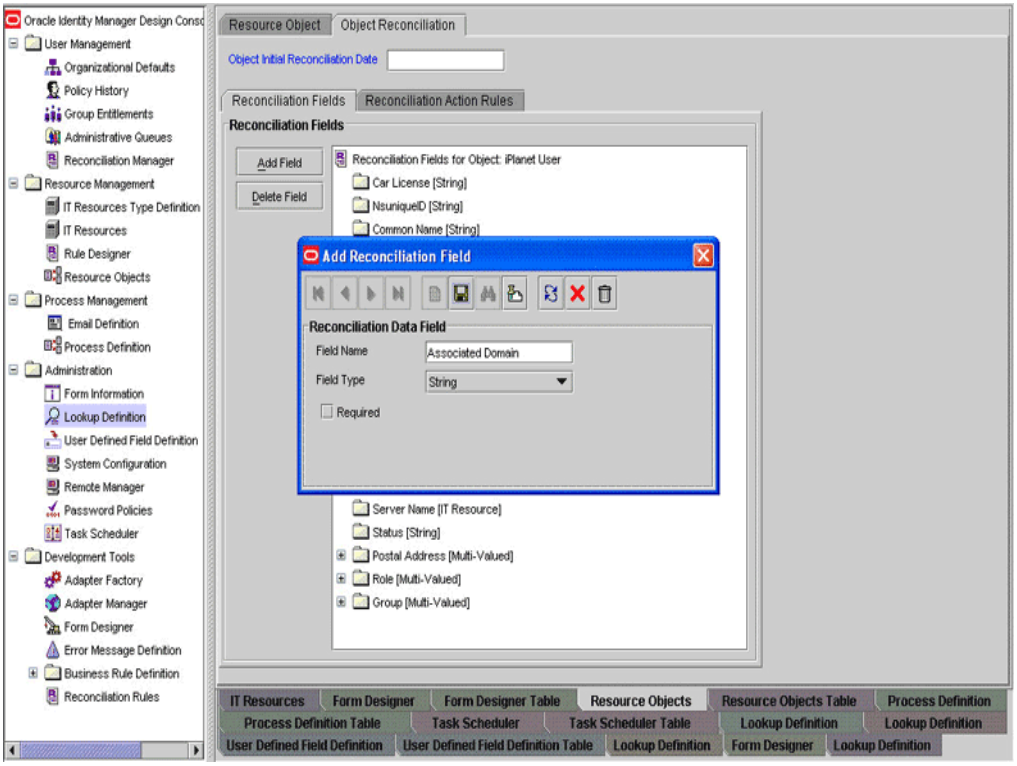
4.10.4 Adding the Attributes of the Object Class to the Resource Object

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

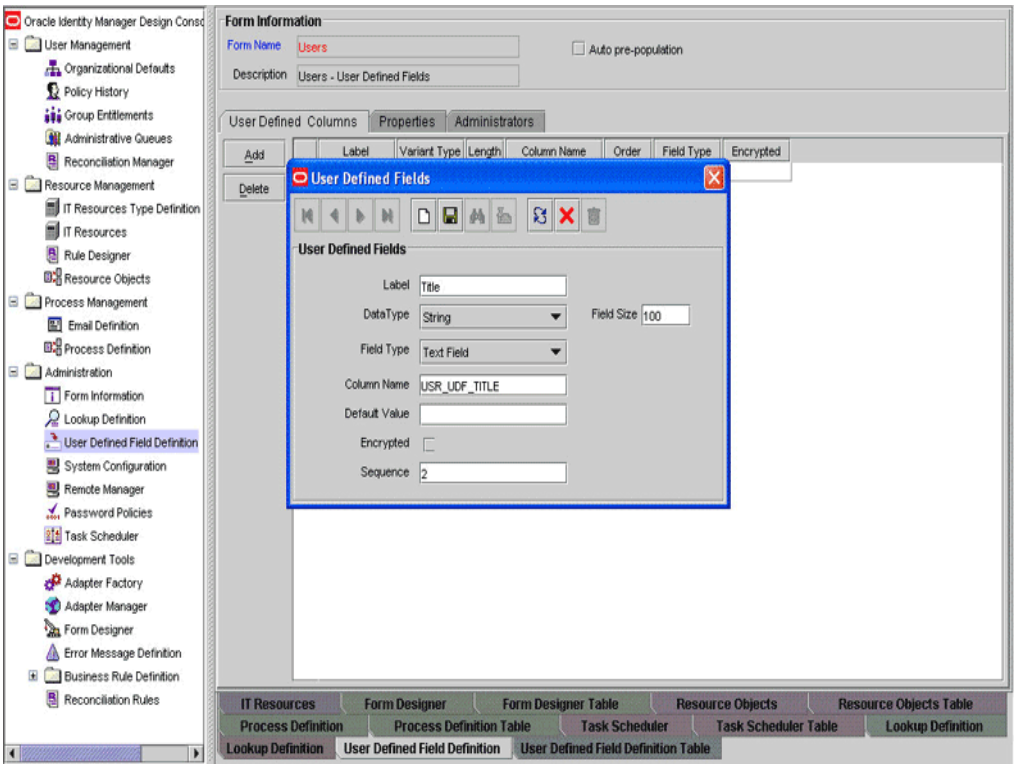
4.10.5 Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation

To add the object class and its attributes to the lookup definition for reconciliation, perform all the instructions given in Section 4.10.3, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" about the **AttrName.Recon.Map.iPlanet** lookup definition.

While performing Step 6 of Section 4.10.3, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning," 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.

To include the new object class for reconciliation, add the objectclass in the search filter as shown in the following screenshot.

Table 3–2 describes the search filter attributes of the scheduled tasks.



4.10.6 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.

4.11 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: For detailed instructions, see one of the following guides:

- For Oracle Identity Manager release 9.0.3.*x* or release 9.1.0.*x*:

  Oracle Fusion Middleware User's Guide for Oracle Identity Manager

- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

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.

5

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:

- Section 5.1, "Running Test Cases"
- Section 5.2, "Troubleshooting Connector Problems"

5.1 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 one of the following directories:

   Note: If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

   - For Oracle Identity Manager release 9.0.3.*x* or 9.1.0.*x*:

     OIM_HOME/xellerate/SJSDS/test/troubleshoot

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/SJSDS/test/troubleshoot

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

   - For Oracle Identity Manager release 9.0.3.*x* or 9.1.0.*x*:

     OIM_HOME/xellerate/SJSDS/test/troubleshoot

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/SJSDS/test/troubleshoot

   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. If you are using Oracle Identity Manager release 11.1.1, then copy the SJSDSProv.jar file from the lib directory on the installation media to a temporary directory on the Oracle Identity Manager host computer. For example, *OIM_HOME*/server/jars.
4. Add the following to the `CLASSPATH` environment variable:
   - For Oracle Identity Manager release 9.0.3.*x* or 9.1.0.*x*:

     ```
     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
     OIM_HOME/xellerate/lib/xlAPI.jar
     ```

   - For Oracle Identity Manager release 11.1.1:

     ```
     OIM_HOME/server/Jars/SJSDSProv.jar
     OIM_HOME/server/lib/xlLogger.jar
     OIM_HOME/server/ext/log4j-1.2.8.jar
     OIM_HOME/server/lib/xlUtils.jar
     OIM_HOME/server/lib/xlAPI.jar
     OIM_HOME/designconsole/lib/oimclient.jar
     ```

5. 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.

6. 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
```

5.2 Troubleshooting Connector Problems

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

- Section 5.2.1, "Connection Errors"
- Section 5.2.2, "Create User Errors"
- Section 5.2.3, "Modify User Errors"
- Section 5.2.4, "Delete User Errors"
- Section 5.2.5, "Reconciliation Errors"
- Section 5.2.6, "Logging Errors"

5.2.1 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.

5.2.2 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.
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.

5.2.3 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.
The Modify User operation failed because of an attempt to add a value to an attribute that does not exist in the `AttrName.Recon.Map.iPlanet` lookup definition. **Returned Error Message:** One or more attribute mappings are missing **Returned Error Code:** ATTR_MAPPING_NOT_FOUND	1. From the corresponding process task, get the value that is passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check if an entry has been made in the `AttrName.Recon.Map.iPlanet` lookup definition.
The operation failed because a duplicate value was being added to an attribute. **Returned Error Message:** Duplicate value **Returned Error Code:** DUPLICATE_VALUE_ERROR	Check the value specified.
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Could not move user to different container **Returned Error Code:** USER_MOVE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot add a user to a security group. **Returned Error Message:** Group does not exist **Returned Error Code:** GROUP_DOES_NOT_EXIST	The specified user security group does not exist in Sun Java System Directory. Check the group name.

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

5.2.4 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.

5.2.5 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.

5.2.6 Logging Errors

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

Problem Description	Solution
Not receiving logging in Debug level even after configuring logging.xml accordingly. . **Returned Error Message:** unable to read logging configuration.	1. Ensure that for every logger present in the logging.xml there is a corresponding log-handler present. 2. The level of log for console-handler should be "TRACE:32"

6

Known Issues

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

- **Bug 7207232**

  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.

Index

M

O

P

R

S

T

U

X