Oracle® Identity Manager

Connector Guide for Oracle Internet Directory

Release 9.0.4

E10436-17

September 2013

ORACLE®

Oracle Identity Manager Connector Guide for Oracle Internet Directory, Release 9.0.4

E10436-17

Primary Author: Gauhar Khan

Contributing Authors: Alankrita Prakash, Gowri G. R

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 Oracle Internet 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 Identity Manager Connector Concepts*.

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

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

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Identity Manager Connector for Oracle Internet Directory?

This chapter provides an overview of the updates made to the software and documentation for release 9.0.4.14 of the Oracle Internet Directory connector.

Note: Release 9.0.4.14 of the connector comes after release 9.0.4.12. Release number 9.0.4.13 has not been used.

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 9.0.4.14
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.11
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.1_6673431
- Software Updates in Release 9.0.4.1

Software Updates in Release 9.0.4.14

The following are the software updates in release 9.0.4.14:

Resolved Issues

The following issues are resolved in release 9.0.4.14:

Bug Number	Issue	Resolution
10317533	Oracle Identity Manager, OID connector remove blanks in root DN. The following issue was observed when the Root DN IT resource parameter contained a DN value with a space character: During reconciliation, the connector searched for users within a DN that was determined after removing the space character in the DN value. For example, if the value of the Root DN IT resource parameter is dc=my example, dc=com, then during reconciliation, the connector searches for users within the following DN: dc=myexample, dc=com	This issue has been resolved. The connector does not remove space characters in DN values, which ensures that users are reconciled from the correct DN without causing reconciliation to fail.
10177001	User reconciliation does not handle escaped comma when parsing data for container DN.	This issue has been resolved. User reconciliation now handle escaped comma when parsing data for container DN.
10176147	OID connector throws the error "UNPARSEABLE DATE" during target reconciliation. During target resource reconciliation, if the connector found a non-date user attribute containing text that was 15 characters long and ended with the letter "z", then no reconciliation event was created. In addition, the following error message was written to the trace file: Unparseable error This error occurred because the connector tried parsing text from a string (retrieved from a non-date attribute) to produce a date.	This issue has been resolved. The connector parses text only from the date attributes, Start Date and End Date.
10140935	Last delete reconciliation time stamps are incorrectly set in IT resource. The timestamp of Oracle Identity Manager server was set depending on the difference in timezone of OIMserver and OID resource, the deleted records are not reconciled.	This issue has been resolved. The last modifytimestamp of the last deleted user record of a successful delete reconciliation is saved as the LastDeleteReconTimeStamp.

Bug Number	Issue	Resolution
9878591	Reconciliation of multivalued attributes fail in OID. If one multivalued attribute is added, it works properly. If two or more multivalued attributes are added, it doesn't work properly.	This issue has been resolved. Now, if two or more multivalued are added, reconciliation works properly.
9705232	Trusted user reconciliation for OID task completes, but throws an error when the user data is null.	This issue has been resolved. Now, when configuring trusted user reconciliation for OID, the task completes without throwing an error that user data is null.
9664304	OID 9.0.4.11 mapped user ID with CN during reconciliation.	The issue has been resolved. Now, if the value is changed in the lookup tables or in the Resource Object for OID, the User ID is not always mapped as CN.
9662334	Adding or removing user to or from group is slow for large groups.	This issue has been resolved. Now, adding or removing a user to or from OID group is not slow for a large group.
9443949	OID connector checks for wrong values in Oracle user enabled.	This issue has been resolved. Now, the values used by OID is ENABLED for user enabled and DISABLED for user disabled.
9438404	When creating a user in Oracle Identity Manager, OID adapter returns corrupted GUID.	The issue has been resolved. Now, modifications to the user are not failing. OID adapter returns valid orclguid value.
9273791	Configuring backup servers running on a different port than the primary port is not supported.	The solution is to provide the ITResource(IPAddress):portno instead of ITResource in the Lookup.OID.Backup server: Code key: serverAddress Decode: secondaryServerAddress:PortNo For example: Code key: 172.20.55.64 Decode: 172.20.55.65:389
9250007	Last reconciliation timestamps are set incorrectly. The timestamp of Oracle Identity Manager server is set resulting in loss of data of duplicate reconciliation of data depending on the difference in timezone of OIMserver and OID resource.	The modifytimestamp of the last user record of a successful reconciliation from OID target system is saved as the LastReconTimeStamp.
9481707	Unparseable date error occurs during user reconciliation.	This issue has been resolved. User reconciliation correctly parses the modifytimestamp value of the target system.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

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

Support for New Oracle Identity Manager Release

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

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

Support for Request-Based Provisioning

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

See Section 3.5.1.2, "Request-Based Provisioning" for more information.

Software Updates in Release 9.0.4.11

The following are resolved issues in release 9.0.4.11:

Bug Number	Issue	Resolution
8627514	During the Create User provisioning operation, Oracle Identity Manager stopped responding if SSL was configured between the target system and Oracle Identity Manager.	This issue has been resolved. Oracle Identity Manager does not stop responding when SSL is configured.
8840081	During the Create User provisioning operation, if you entered values for the Start Date and End Date process form fields, then the Create User task was rejected.	This issue has been resolved. The Create User provisioning operation is successful even when you enter values for the STart Date and End Date process form fields.
9146791	The group or role reconciliation runs were successful when performed for the first time. From the second time onward, these reconciliation runs failed.	This issue has been resolved. You can successfully perform the group or role reconciliation runs any number of times.
9238210	In the AttrName.Recon.Map.OID lookup definition if two or more Code Key values had the same Decode value, then the correct values were not retrieved.	This issue has been resolved. During reconciliation, correct values from the target system are retrieved even when two or more Code Key values had the same Decode value in the AttrName.Recon.Map.OID lookup definition
9246312	During trusted source reconciliation, the value of the manager attribute was not reconciled.	This issue has been resolved. The value in the manager attribute is now reconciled during trusted source reconciliation.

Software Updates in Release 9.0.4.7

The following are software updates in release 9.0.4.7:

- Provisioning and Reconciliation Based on the orclGUID Field
- Support for Reconciliation of Groups and Roles
- Support for Separate Scheduled Tasks
- Support for High-Availability
- Support for Adding New Attributes and Multivalued Attributes for Provisioning and Reconciliation of Groups or Roles
- Introduction of a Lookup Definition for Storing Constants

- Implementation of the Ignore-Event Functionality
- Addition of the SearchBase and SearchFilter Attributes in All the User Reconciliation, and Groups and Roles Reconciliation Scheduled Tasks
- Resolved Issues

Provisioning and Reconciliation Based on the orclGUID Field

From this release onward, the connector performs reconciliation and provisioning operations based on the orclGUID field. The orclGUID field is a unique, read-only field that is created after a Create User provisioning operation.

Support for Reconciliation of Groups and Roles

From this release onward, the connector supports reconciliation of groups and roles. The `OID Group Recon Task` and `OID Role Recon Task` scheduled tasks are used to automate reconciliation of groups and roles, respectively.

See the following sections for more information:

- Group Reconciliation
- Role Reconciliation
- Group and Role Reconciliation Scheduled Tasks

Support for Separate Scheduled Tasks

In the earlier release, you used a:

- Single scheduled task (`OID Lookup Reconciliation Task`) for reconciliation of lookup values for groups, roles, and organizations
- Single scheduled task (`OID User Recon`) for running trusted source and target resource reconciliation
- Single scheduled task (`OID User Recon delete`) for reconciliation of deleted users in trusted source and target resource modes

From this release onward, the connector has independent scheduled tasks created for all types of user, groups, roles, and lookup reconciliation.

See the following sections for more information:

- Lookup Fields Reconciliation Scheduled Tasks
- User Reconciliation Scheduled Tasks
- Group and Role Reconciliation Scheduled Tasks

Support for High-Availability

The high-availability feature for IT Resource 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 becomes unavailable.

See the "Configuring High Availability of the Target System" section for more information.

Support for Adding New Attributes and Multivalued Attributes for Provisioning and Reconciliation of Groups or Roles

By default, the attributes listed in the "Group Provisioning" section are mapped for provisioning of groups between Oracle Identity Manager and the target system. Similarly, by default, the attributes listed in the "Role Provisioning" section are

mapped for provisioning of roles between Oracle Identity Manager and the target system. From this release onward, you can map additional attributes for provisioning groups or roles.

See the "Adding New Attributes for Provisioning Groups or Roles" section for more information.

By default, no multivalued attributes are mapped for provisioning between Oracle Identity Manager and the target system for groups and roles. From this release onward, the connector enables you to add new multivalued attributes for reconciliation and provisioning of groups or roles.

See the "Adding New Multivalued Attributes for Provisioning" section for more information.

By default, the attributes listed in the "Group Reconciliation" and "Role Reconciliation" sections are mapped for group or role reconciliation between Oracle Identity Manager and the target system. From this release onward, you can add new attributes for group or role reconciliation.

See the "Adding New Attributes for Reconciliation of Groups or Roles" section for more information.

By default, no multivalued attributes are mapped for reconciliation between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation of groups or roles.

See the "Adding New Multivalued Attributes for Target Resource Reconciliation" section for more information.

Introduction of a Lookup Definition for Storing Constants

The `Lookup.OID.Constants` lookup definition stores constants defined in the Java classes that constitute the connector.

Caution: You must not change any entry in the `Lookup.OID.Constants` lookup definition. If you change any entry, then the connector will not function correctly

---

This information has been mentioned in the "Setting Up Lookup Definitions in Oracle Identity Manager" section.

Implementation of the Ignore-Event Functionality

For every operation that is performed, the connector compares the user attributes in the target system with the corresponding attributes in Oracle Identity Manager. If the values of the user attributes in the target system do not match with the corresponding attributes in Oracle Identity Manager, then an event record is created. Otherwise, no event record is created.

Addition of the SearchBase and SearchFilter Attributes in All the User Reconciliation, and Groups and Roles Reconciliation Scheduled Tasks

From this release onwards, you can specify a subset of the records that must be reconciled from the target system. The SearchBase and SearchFilter attributes have been added to all scheduled tasks for reconciliation of users, groups, and roles.

See the following sections for more information:

- Limited Reconciliation

- User Reconciliation Scheduled Tasks
- Group and Role Reconciliation Scheduled Tasks

Resolved Issues

The following table lists issues resolved in release 9.0.4.7:

Bug Number	Issue	Resolution
6694619	The connector did not provide an option to update the `Common Name` and `User ID` process form fields.	This issue has been resolved. In order to enable modifications to the `Common Name` and `User ID` process form fields, the Common Name Updated and User ID Updated operations have been added to the connector.
7581912	The Group Name Updated, Role Name, Updated, or Change OU Name provisioning operations were successful when performed for the first time. From the second time onward, these provisioning operations failed.	This issue has been resolved. You can successfully perform the Group Name Updated, Role Name, Updated, or Change OU Name provisioning operations any number of times.
7605087	During trusted source reconciliation, if there was a mismatch in the case (uppercase/lowercase) between a user's OU in Oracle Identity Manager and the user's OU on the target system, then the OU field was not populated. This was because the target system was case-sensitive and Oracle Identity Manager was not case-sensitive toward OU names. OU names were converted to lowercase when they were brought to Oracle Identity Manager through reconciliation. As a workaround to this problem, it was recommended that you set lowercase names for OUs that you created.	This issue has been resolved. The OU field is now being populated.
7615302	Provisioning and reconciliation of manager data for a user was not supported.	This issue has been resolved. You can now provision and reconcile manager data for a user. The Manager field has been added to the list of fields that are available for provisioning and reconciliation.
8258219	An error was encountered when you updated a process form field whose name contained the "Date" string. For example, if the name of the process form field was `Date of Joining`, then an error was encountered when you updated the value of this field.	This issue has been resolved. No error is encountered when you update a process form field whose name contained the "Date" string.
8346748	By default, during a Create User provisioning operation, the user ID that you specify was mapped to the `cn` field of target system. If you had customized the mapping so that the user ID (that you specify in Oracle Identity Manager) was assigned to the `uid` field of the target system, then after the Create User provisioning operation, that value of the `uid` field was `null`.	This issue has been resolved. When you create a user account on the target system through Oracle Identity Manager, the value of the `uid` field of the target system is the user ID that you specify in Oracle Identity Manager.

Bug Number	Issue	Resolution
8597107	The `Organization DN` field on the process form was neither mapped to the `Organization Unit` attribute, nor `Organization` 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. The Container DN value is a part of the DN value. For example, if the DN value of a target system user is `cn=User,ou=People, o=xyz`, then the Container DN value is `ou=People`.
8620552	Target system user fields were not updated when they were updated along with the Organization Name field.	This issue has been resolved. All fields that are updated along with the Organization Name field are now being updated successfully.
8810993	A user reconciliation run failed if the lookup definition contained the same decode value for different code key values.	This issue has been resolved. You can now successfully run user reconciliation if the look up definition contained the same decode value for different code key values.

Software Updates in Release 9.0.4.6

The following are the software updates in release 9.0.4.6:

- Support for Reconciliation and Provisioning of Multivalued Attributes
- Support for New Target System

Support for Reconciliation and Provisioning of Multivalued Attributes

From this release onward, the connector supports the reconciliation and provisioning of multivalued attributes. See Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation" for the procedure to add new multivalued attributes for reconciliation and provisioning.

Support for New Target System

From this release onward, the connector adds support for Oracle Internet Directory 11*g*R1 as the target system.

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

Software Updates in Release 9.0.4.5

The following are resolved issues in release 9.0.4.5:

Bug Number	Issue	Resolution
7564492, 6334595, 6317860	Incremental reconciliation was not supported. If you deleted one user from one organization on the target system and then performed trusted source delete reconciliation, then all users were deleted from all organizations in Oracle Identity Manager. During reconciliation, user data was fetched from the target system, regardless of whether or not it had been modified.	Incremental reconciliation is now supported.
6312504	IT resource parameters for the names of the lookup definitions for reconciliation and provisioning were set to NULL when you restarted Oracle Identity Manager.	The names of the lookup definitions are set as the default values of the IT resource parameters. These parameters are not set to NULL when you restart Oracle Identity Manager.
6168631	In earlier releases, you had to use the orcladmin account on the target system for reconciliation and provisioning operations.	This issue has been resolved. You can now create a user on the target system, assign the minimum required permissions to the user, and then use it for connector operations.
6312344	The default value of the Organization DN field on the Administrative and User Console was cn=user.	The Organization DN field has been changed to a lookup field, and the default value has been removed. You can now select a value in this lookup field.
6804852	The Manager ID field was not available for reconciliation and provisioning.	The Manager ID field has been added to the list of fields that are available for reconciliation and provisioning.
7233799	At the end of a successful provisioning operation, the "Mapping Not Found" message was recorded in the log file. This message has now been removed.	This issue has been resolved. The "Mapping Not Found" message is no longer recorded in the log file at the end of a successful provisioning operation. The following are some of the entries in the AttrName.Prov.Map.OID lookup definition. You must ensure that these entries are not changed. ldapUserID: cn ldapFirstName: givenName ldapLastName: sn ldapPassword: userPassword
6987536	The Start Date and End Date fields of the target system were not used by the connector.	This issue has been resolved. The Start Date and End Date fields have been added for reconciliation and provisioning operations.
7022721	The process form had two fields for two object classes. This imposed a limitation on the number of objectclasses to which a user could be assigned during a Create User provisioning operation.	This issue has been resolved. The Objectclassess field replaces the two fields on the process form. You can enter a list of objectclasses in this field during a provisioning operation. Use the vertical bar (|) as the delimiter character in the list of objectclasses.

Bug Number	Issue	Resolution
7047363	You could not add to the default attribute mappings for reconciliation.	This issue has been resolved. You can now use the AttrName.Recon.Map.OID lookup definition to add attributes for reconciliation. See "Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation" in the connector guide for more information.
6490731	The length of the Password field was 14 bytes.	The length of the Password field has been increased to 30 bytes.
7434067	A reconciliation error was encountered if you applied a custom reconciliation query that filtered user records by both role assignment and group membership. For example, application of the following reconciliation query would result in an error: role=role1&group=group1	This issue has been resolved. Any combination of the following attributes can be used in the query: ■ givenname ■ sn ■ givenname&sn ■ group ■ role ■ givenname&group ■ givenname&role ■ group&role Limitation: The custom reconciliation query must not include field values that contain any of the following characters: ■ & (ampersand) ■ | (vertical bar) ■ = (equal sign) In addition, the field values must not contain the word "group" or "role." The following are examples of query conditions that are invalid: givenname="mary&brown" This value is invalid because it contains the ampersand (&). givenname="johngroup" This value is invalid because it contains the word group.
7360833	The name of the IT resource type for all LDAP-based connectors was LDAP Server.	This issue has been resolved. The IT resource type for the Oracle Internet Directory connector has been renamed to "OID IT Resource."
7308328	A space after a comma in the DN value would cause a reconciliation error.	This issue has been resolved. DN values that have a space after the comma are now correctly reconciled. You implement this solution by copying the JAR files as part of the deployment procedure.
7218933	The "INSUFFICIENT_INFORMATION_PROVIDED" message was displayed if any process form field was left empty during a provisioning operation. The field itself was not pointed out by the message.	This issue has been resolved. The name of the field in which a value has not been provided is included in the message displayed on the console.
7120339	The INSUFFICIENT_INFORMATION_PROVIDED error message was not mapped in the resource bundle.	This issue has been resolved. The error message is now mapped in the resource bundle.

Bug Number	Issue	Resolution
7165810	When you changed the name of an organizational unit through a provisioning operation, the existing OU was deleted and then re-created with the new name that you specified.	This issue has been resolved. The name of the OU is actually changed when you perform the Change OU Name provisioning operation. The OU is not deleted and re-created with the new name. You implement this solution by copying the JAR files as part of the deployment procedure.
6275476	On the target system, DNs of groups are not case-sensitive. In Oracle Identity Manager, group DNs are case-sensitive. This caused problems during reconciliation of group membership details.	▪ This issue has been resolved. Group DNs are converted to lowercase before they are reconciled into the group lookup definition in Oracle Identity Manager. In other words, Oracle Identity Manager does not perform a case-sensitive check on group names. ▪ You implement this solution by copying the JAR files as part of the deployment procedure.
7423099	Special characters were not supported in the First Name and Last Name fields on the process form.	This issue has been resolved. See "Provisioning Module" in the connector guide for information about the special characters that are supported in process form fields. You implement this solution by copying the JAR files as part of the deployment procedure.
6489877	The connector supported neither Mode 1 nor Mode 2 secure connections to Oracle Internet Directory.	The connector supports Mode 1 secure connections to Oracle Internet Directory. See "Configuring SSL" in the connector guide for detailed information.
7564599	During a Create Group provisioning operation, it was mandatory to specify a parent OU for the group.	This issue has been resolved. If a parent OU is not specified, then the group is created under the DN context.
7601582	The User Deletion Successful message was displayed when the Delete User provisioning operation was performed on a user who had already been deleted on the target system.	The message has been corrected.
7301659	The orclguid field of the target system stores identifier for each LDAP entry in Oracle Internet Directory. The connector did not fetch and store the orclguid of target system users.	This issue has been resolved. The connector now retrieves and stores the orclguid field of target system users.

Software Updates in Release 9.0.4.4

The following are resolved issues in release 9.0.4.4:

Bug Number	Issue	Resolution
7257647	The connector did not support batched or paged reconciliation. There were performance issues related to this limitation.	The connector now supports paged reconciliation. You can implement this feature if the target system is Oracle Internet Directory 10.1.4.0.1 or later. See "Paged Reconciliation" on page 3-5 for more information.

Bug Number	Issue	Resolution
7306055	There was scope for improvement in the performance of the following provisioning operations: ▪ Adding or removing a user from a group ▪ Granting or removing a role from a user	The performance of provisioning operations that involve group or role membership changes has been enhanced.

Software Updates in Release 9.0.4.3

The following is a software update in release 9.0.4.3:

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" on page 2-13 for details.

Software Updates in Release 9.0.4.2

The following are resolved issues in release 9.0.4.2:

Bug Number	Issue	Resolution
7003824	If you added an object class and its attributes, then subsequent Create User provisioning operations failed. An error message similar to the following one was displayed as the outcome of the provisioning operations: `"Unable to add attributes of the object[LDAP: error code 65 - associatedDomain attribute not found. Mandatory Attribute missing.]"`	This issue has been resolved. You can now add an object class and then perform Create User provisioning operations. See Section 4.9, "Adding New Object Classes for Provisioning and Reconciliation" for more information. **Note:** A trusted source reconciliation run fails if it involves user-defined fields (UDFs). This issue is tracked through Bug 7047363.

Software Updates in Release 9.0.4.1_6673431

The following are resolved issues in release 9.0.4.1_6673431:

Bug Number	Issue	Resolution
6673431	Delete reconciliation was run after trusted source reconciliation. This sequence resulted in deletion of some OIM Users who were not actually deleted on the target system.	This issue has been resolved. During a trusted source reconciliation run, the API that implements Delete reconciliation is called before reconciliation of existing target system records.

Software Updates in Release 9.0.4.1

The following is a software update in release 9.0.4.1:

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

The `xliOID.jar` file has been split into two files, `OIDProv.jar` and `OIDRecon.jar`. Corresponding changes have been made in the following sections:

- Files and Directories on the Installation Media on page 1-7
- Determining the Release Number of the Connector on page 1-8
- Copying the Connector Files on page 2-14

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

Documentation-Specific Updates in Release 9.0.4.14

The following are documentation-specific updates in release 9.0.4.14:

- In the Section 2.3.1.7, "Configuring High Availability of the Target System", the ITResource(IPAddress):portno is used instead of ITResource in the Lookup.OID.Backup server:

  Code key: serverAddress

  Decode: secondaryServerAddress:PortNo

  For example:

  Code key: 172.20.55.64

  Decode: 172.20.55.65:389

- A note has been added in Section 2.2.2, "Configuring the IT Resource," regarding the modifytimestamp code key and decode entry which is newly added to the AttrName.Recon.Map.OID lookup definition.
- Section 4.9.2, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" has been updated for the new lookup definition named AttrName.Prov.Map.OID.
- In Section 1.1, "Certified Components," Oracle Internet Directory release 9.*x* has been removed and Oracle Internet Directory release 10.1.4.*x* has been changed to 10.1.*x*.
- In Section 2.3.1.1, "Configuring Trusted Source Reconciliation," the path to locate and open the xml files has been updated.
- In Section 2.3.1.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1," the logger name has been corrected.

- In Section 2.3.2.1, "Configuring the Target System," step 3 has been added to configure full reconciliation.
- In Section 2.2.2, "Configuring the IT Resource," the description for the following parameters have been updated:
  - Root DN
  - Last Trusted Recon TimeStamp
  - Last Target Recon TimeStamp
  - Last Trusted Delete Recon TimeStamp
  - Last Target Delete Recon TimeStamp
- In the "Create OID Role" row of Table 1–9, " User Provisioning Functions Supported by the Connector", a note has been added.
- Section 2.3.1.1.2, "Adding the Default Password Policy for Xellerate User Resource Object" has been added.
- Section 2.1.2.1.2, "Creating a Target System User Account for Connector Operations using Oracle Internet Directory Command-Line Utilities" has been added.
- Step 2 of Section 4.4, "Adding New Attributes for Trusted Source Reconciliation" has been modified.
- Information specific to Oracle Identity Manager release 9.0.3.*x* has been removed as this release is no longer supported.

Documentation-Specific Updates in Release 9.0.4.12

The following are documentation-specific updates in release 9.0.4.12:

- In Chapter 5, "Testing and Troubleshooting," a step for setting a value for the DXL.HomeDir attribute has been added.
- In Section 1.8.1, "User Provisioning Functions," a note has been added in the "Rename OU" row.
- From Section 2.1.1.1, "Files and Directories on the Installation Media," the "Files in the Batch/custom directory" row has been removed.
- In Section 2.3.2.1, "Configuring the Target System," information about configuring role reconciliation has been added.
- From Chapter 6, "Known Issues," the following issues have been removed:
  - **Bug 7560319**

    The Time Zone field on the process form can accept invalid values during provisioning operations.
  - **Bug 7609477**

    If only the Manager ID field of a user on the target system is modified, then the user is not reconciled during the next reconciliation run.
  - **Bug 8283518**

    When you import the connector XML file by using the Deployment Manager, child tables for roles and groups are created in the database but not linked with the parent table.
  - **Bug 8874848**

During the Change OU Name provisioning operation, the Update Organization name task is rejected and the following error message is displayed:

```
Organization unit does not exist
```

– **Bug 9251778**

Note: This issue is encountered only when you install the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1.

The procedure for downloading the ldap.jar and ldapbp.jar files on the Manual Prerequisite Steps page of the connector installer is not in sync with the procedure described in Section 2.1.2.2, "Using External Code Files."

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 Releases 9.0.4.7

The following documentation-specific updates have been made in release 9.0.4.7:

- In the "User Reconciliation" and "Provisioning Module" section, new fields have been added to list of fields that are reconciled and provisioned.
- In the "Supported Functionality" section, the names of some of the functions have been modified. In addition, new functions have been added.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Oracle Identity Manager" row.
- In the "Configuring the IT Resource" section, new IT resource parameters have been added.
- The content in the "Setting Up Lookup Definitions in Oracle Identity Manager" section has been modified.
- The "Stopping Reconciliation" section has been added, which contains information about stopping a scheduled task has been added.
- In the "Configuring Trusted Source Reconciliation" section, the names of the scheduled tasks used for trusted source reconciliation and trusted delete user reconciliation have been modified.
- The name of a lookup definition in the "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning" section has been changed.
- From the "Using the Connector" chapter, the "Adding the Object Class and its Attributes to the Lookup Definition for Reconciliation" section has been removed.
- The content in the "Configuring the Mapping of the User ID Field" section has been modified.
- From the "Testing and Troubleshooting" chapter, the "Testing Partial Reconciliation" section has been removed.
- In the "Known Issues" chapter:
  - The following issue has been removed:

Bug 7605087

During trusted source reconciliation, if there is a mismatch in the case (uppercase/lowercase) between a user's OU in Oracle Identity Manager and the user's OU on the target system, then the OU field is not populated. This is because the target system is case-sensitive and Oracle Identity Manager is not case-sensitive toward OU names. OU names are converted to lowercase when they are brought to Oracle Identity Manager through reconciliation.

As a workaround to this problem, it is recommended that you set lowercase names for OUs that you create.

- Issues tracked by bug numbers 8283518, 8294433, 8874848, and 8880450 have been added.

Documentation-Specific Updates in Release 9.0.4.6

The following documentation-specific updates have been made in release 9.0.4.6:

- In the "Using the Connector" chapter:
  - The "Configuring the Connector for Multiple Installations of the Target System" section has been removed. This feature is not supported by default.
  - The following sections have been added:
    * Adding New Attributes for Target Resource Reconciliation
    * Adding New Attributes for Provisioning Users
- In the "Lookup Fields Reconciliation Scheduled Tasks" section:
  - The name of the reconciliation scheduled task has been changed from `OID Group Lookup Reconciliation Task` to `OID Lookup Reconciliation Task`.
  - The `AttrType` attribute has been added to the list of `OID Lookup Reconciliation Task` reconciliation scheduled task attributes.
  - The `LookupCodeName` attribute values for groups, roles, and organization and organization unit have been changed.
- The "Customizing the xlconfig.xml File" section has been moved from the "Postinstallation on Oracle Identity Manager Server" section to a new location. The instructions described in the "Customizing the xlconfig.xml File" section are now performed before installing the connector.
- In the "Setting Up Lookup Definitions in Oracle Identity Manager" section:
  - The name of the lookup definition has been changed from `global.AttrName.Prov.Map.OID.Preferred-Language` to `Lookup.OID.PrefLang`.
  - The `global.AttrName.Prov.Map.OID.Location` and `global.AttrName.Prov.Map.OID.Time-Zone` definitions have been removed as they have been converted into text fields.
- In the "Deploying the Connector" chapter, the procedure to add custom object classes and custom attributes on the target system has been removed.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.5

The following documentation-specific update has been made in releases 9.0.4.1 through 9.0.4.5:

- New points have been added in the "Known Issues" chapter.

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 Oracle Internet Directory.

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

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

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

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

This chapter contains the following sections:

1.1 Certified Components

Table 1–1 lists certified components for the connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ 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	Oracle Internet Directory release 10.1.*x*, or 11*g*R1
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 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
Target system user account	User account to which the BROWSE, ADD, DELETE, READ, WRITE, and SEARCH rights have been assigned You provide the credentials of this user account configuring the IT resource. The procedure is described later in this guide. If you try to perform an operation for which the required permission has not been assigned to the user account, then the "Insufficient Access Rights" message is displayed.

1.2 Certified Languages

The connector supports the following languages:

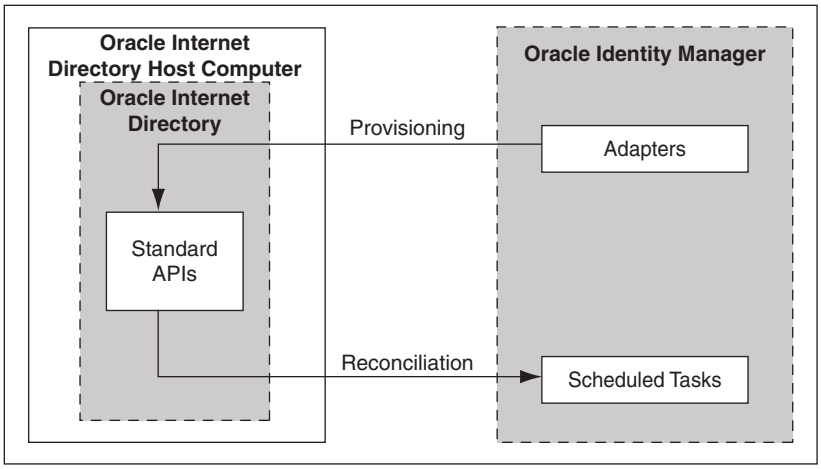
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about supported special characters

1.3 Connector Architecture

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

Figure 1–1 Architecture of the Connector



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

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager 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, Oracle Internet Directory 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, Oracle Internet Directory 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 Oracle Internet

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 Oracle Internet Directory as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "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 3.3.2, "Limited Reconciliation" for more information.

1.4.3 Support for Paged Reconciliation

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

Paged reconciliation is implemented using the PageSize attribute of the scheduled task.

See Section 3.3.3, "Paged Reconciliation" for more information about paged reconciliation.

1.4.4 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 Oracle Internet Directory 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.

See Section 3.3.4.1, "Scheduled Tasks for User Reconciliation" for more information about scheduled tasks used for reconciling deleted user records.

1.4.5 Support for Both Full and Incremental Reconciliation

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

You can perform a full reconciliation run at any time.

See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

1.4.6 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"

1.4.7 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.OID.Backup server lookup definition and uses this information to switch to a backup target system installation. The timeout interval stored in the ldapConnectTimeOut entry of the Lookup.OID.Configuration lookup definition is used to determine when to switch to the backup target system installation.

See Section 2.3.1.7, "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 3.2, "Scheduled Tasks for Lookup Field Synchronization" for information about these scheduled tasks

- For organizations and organization units: Lookup.OID.Organization
- For groups: Lookup.OID.Group
- For roles: Lookup.OID.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.OID.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 2.3.1.6.1, "Setting Up the Lookup.OID.Configuration Lookup Definition" for information about the entries for which you can set values.
Lookup.OID.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.
AttrName.Recon.Map.OID	This lookup definition holds mappings between the OID User resource object fields and target system attributes.	This lookup definition is preconfigured. It is used for both trusted source reconciliation and target resource reconciliation. 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.OID	This lookup definition holds mappings between OID User process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–10 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.OIDGroupReconciliation.FieldMap	This lookup definition holds mappings between OID 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.

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
AttrName.Group.Prov.Map.OID	This lookup definition holds mappings between OID Group process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–12 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.OIDRoleReconciliation.FieldMap	This lookup definition holds mappings between OID 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.
AttrName.Role.Prov.Map.OID	This lookup definition holds mappings between OID Role process form fields and target system attributes.	This lookup definition is preconfigured. Table 1–13 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.OID.Backup server	This lookup definition holds mappings between primary Oracle Internet Directory servers and secondary Oracle Internet Directory servers.	It is optional to enter values in this lookup definition. Section 2.3.1.7, "Configuring High Availability of the Target System" provides information about this lookup definition.
Lookup.OID.PrefLang	During a provisioning operation, you use this lookup definition to specify a language for the user.	Section 2.3.1.6.2, "Setting Up the Lookup.OID.PrefLang Lookup Definition" provides information about creating entries in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation

This section discusses the following topics:

- Section 1.6.1, "User Attributes for Target Resource Reconciliation"
- Section 1.6.2, "Group Attributes for Target Resource Reconciliation"
- Section 1.6.3, "Role Attributes for Target Resource Reconciliation"
- Section 1.6.4, "Reconciliation Rules for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"

1.6.1 User Attributes for Target Resource Reconciliation

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

Table 1–3 User Attributes for Target Resource Reconciliation

Resource Object Field	Target System Attribute	Description
User ID	uid	Unique ID of a user account
First Name	givenname	First name
Last Name	sn	Last name
Middle Name	middleName	Middle name
Department	departmentNumber	Department
Location	l	Location
Telephone	telephoneNumber	Telephone number
Email	mail	E-mail address
Time Zone	orclTimeZone	Timezone
Preferred Language	preferredlanguage	Preferred language for communication
Title	title	Designation
Start Date	orclActiveStartDate	Date from which the user account is active
End Date	orclActiveEndDate	Date up to which the user account is active
orclGUID	orclGuid	GUID
manager	manager	Distinguished name (DN) of the user's manager.
Container DN	NA	Container in which the user account is present on the target system For example: `ou=abc,dc=Company, dc=corp,dc=com`
Common Name	cn	Common name on the target system
UserGroup	groupOfUniqueNames	Name of the group to which a user account belongs
UserRole	OrganizationalRole	Name of the role that is assigned to a user account

1.6.2 Group Attributes for Target Resource Reconciliation

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 lists the group attributes of the target system from which values are fetched during reconciliation. The OID Group Recon Task scheduled task is used to reconcile group data.

Table 1–4 Group Attributes for Target Resource Reconciliation

Resource Object Field	Target System Attribute	Description
Group Name	cn	Group name
orclGuid	orclguid	GUID

1.6.3 Role Attributes for Target Resource Reconciliation

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 lists the role attributes of the target system from which values are fetched during reconciliation. The OID Role Recon Task scheduled task is used to reconcile role data.

Table 1–5 Role Attributes for Target Resource Reconciliation

Resource Object Field	Target System Attribute	Description
Role Name	cn	Role name
orclGuid	orclguid	GUID

1.6.4 Reconciliation Rules for Target Resource Reconciliation

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for generic information about reconciliation matching and action rules

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

- Section 1.6.4.1, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.4.2, "Viewing Reconciliation Rules for Target Resource Reconciliation in the Design Console"

1.6.4.1 Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

Rule name: OID User Recon Rule

Rule element: (ORCLGUID Equals orclGuid) OR (User Login Equals User ID)

In the first rule component:

- User Login is the User ID field on the OIM User form.
- User ID is the user ID field of the OID account.

In the second rule component:

- ORCLGUID is the ORCLGUID field on the OIM User form.
- orclGuid is the orclguid field on the target system.

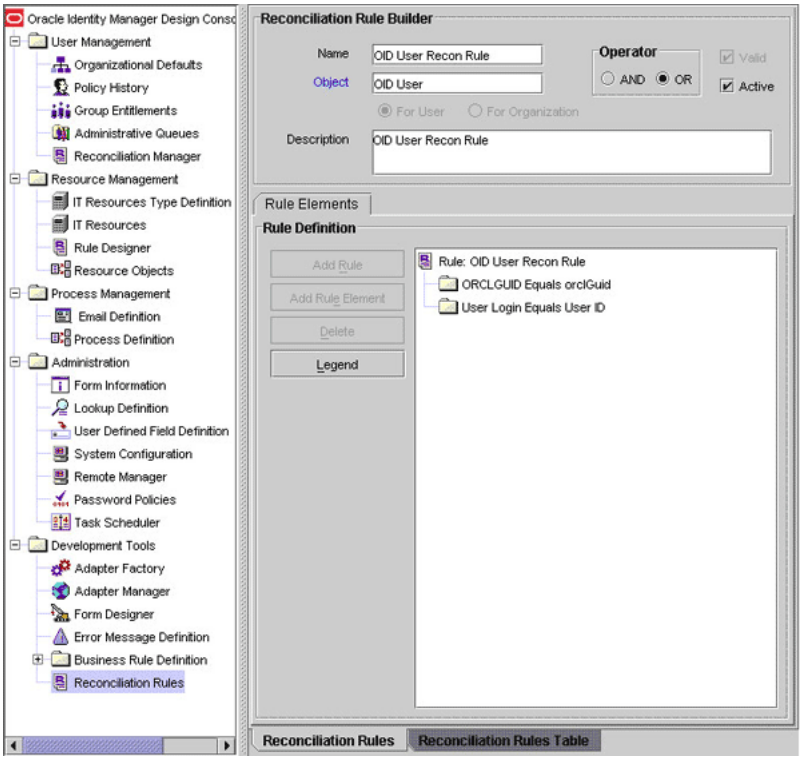
1.6.4.2 Viewing Reconciliation Rules for Target Resource Reconciliation in the Design Console

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

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

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

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

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

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

- Section 1.6.5.1, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.5.2, "Viewing Reconciliation Action Rules for Target Resource Reconciliation in the Design Console"

1.6.5.1 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

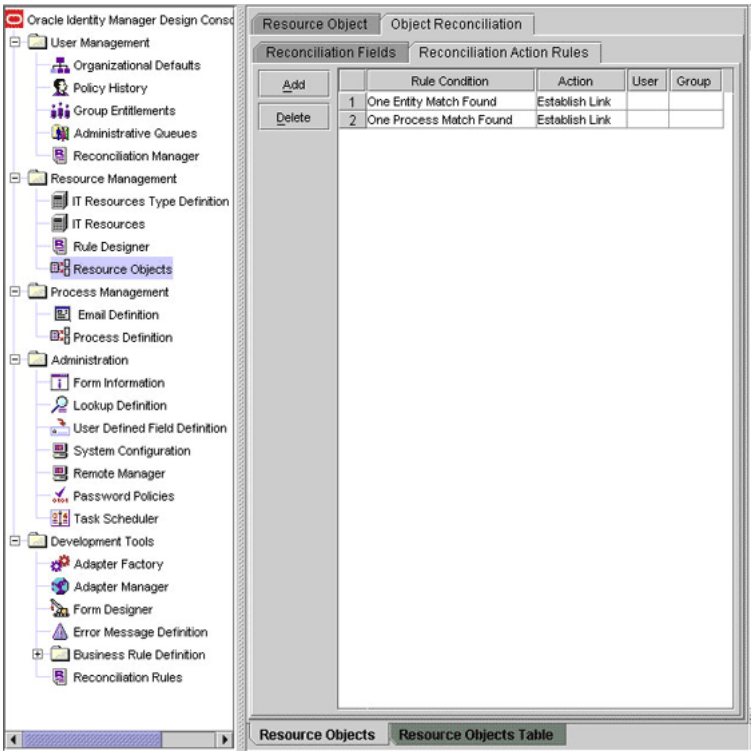
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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

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

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

Figure 1–3 Action Rules for Target Resource Reconciliation



1.7 Connector Objects Used During Trusted Source Reconciliation

This section discusses the following topics:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"

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

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–7 provides information about user attribute mappings for trusted source reconciliation.

Table 1–7 User Attributes for Trusted Source Reconciliation

Field on the Xellerate User Resource Object	Target System Attribute	Description
User ID	uid	User's logon name
First Name	givenname	First name
Last Name	sn	Last name
Middle Name	middleName	Middle name
Organization	ou	Name of the organization on the target system to which a user account belongs
User Type	NA	Default value: `End-User Administrator`
Employee Type	NA	Default value: `Consultant`
Start Date	orclActiveStartDate	Start date for the user account on the target system
End Date	orclActiveEndDate	End date for the user account on the target system
Email	mail	E-mail address
Status	orclisEnabled	This field stores the status of a user account on the target system.
manager	manager	Distinguished name (DN) of the user's manager.

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for generic information about reconciliation matching and action rules

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

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

1.7.2.1 Reconciliation Rule for Trusted Source Reconciliation

The following is the process-matching rule:

Rule name: Trusted Source Recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is the User ID field on the OIM User form.
- User ID is the user ID of the OID account.

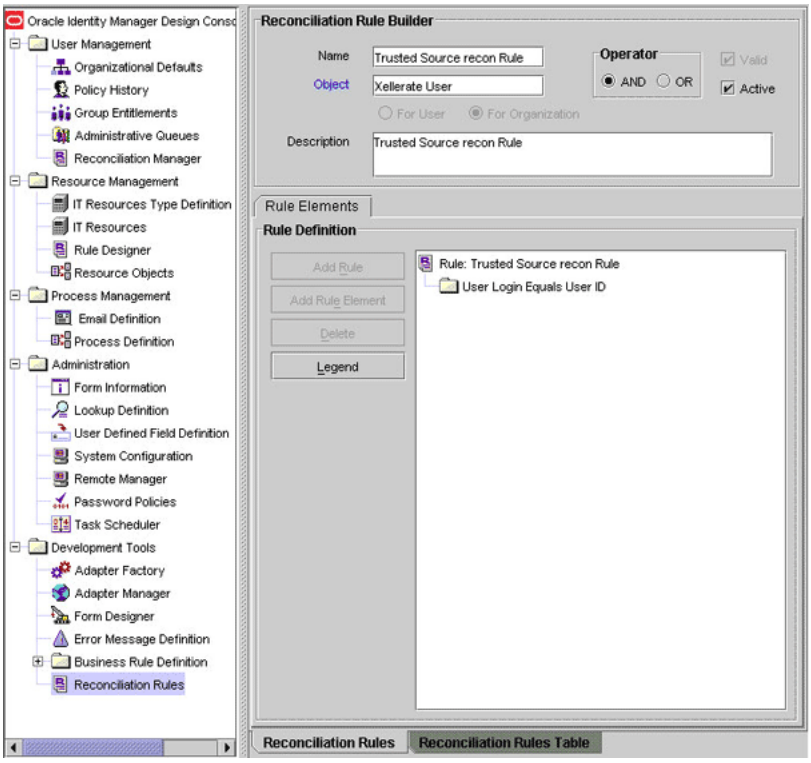
1.7.2.2 Viewing Reconciliation Rules for Trusted Source Reconciliation in the Design Console

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

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

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

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

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

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

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

1.7.3.1 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–8 lists the action rules for reconciliation.

Table 1–8 Action Rules for Trusted Source Reconciliation

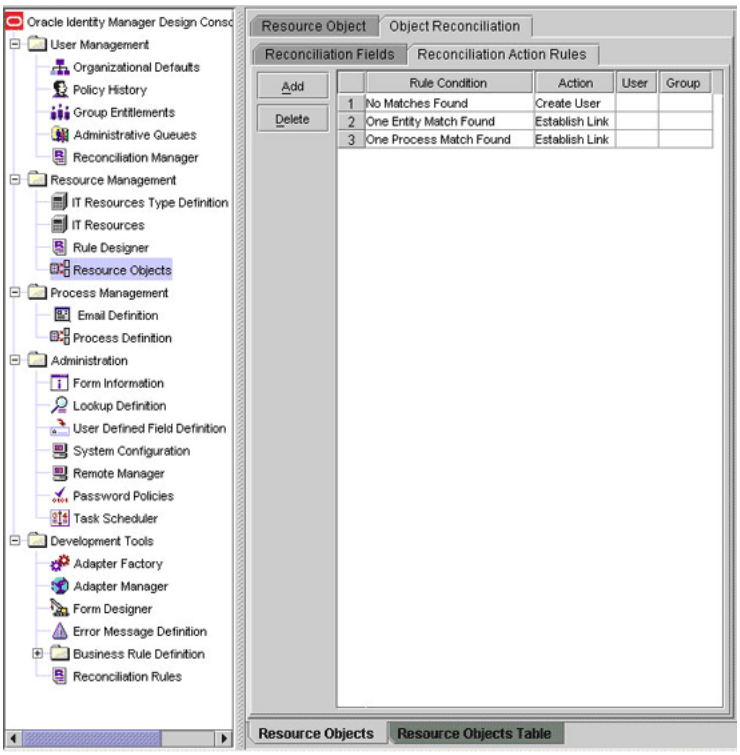
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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

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

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

Figure 1–5 Action Rules for Trusted Source Reconciliation



1.8 Connector Objects Used During Provisioning

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

> **See Also:** The "Provisioning" section in *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for conceptual information about provisioning

This section discusses the following topics:

- Section 1.8.1, "User Provisioning Functions"
- Section 1.8.2, "User Attributes for Provisioning"
- Section 1.8.3, "Group Attributes for Provisioning"
- Section 1.8.4, "Role Attributes for Provisioning"

1.8.1 User Provisioning Functions

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

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for generic information about process tasks and adapters

Table 1–9 User Provisioning Functions Supported by the Connector

Function	Description	Adapter
Create User	Creates a user in Oracle Internet Directory	OID Create User
Delete User	Deletes a user in Oracle Internet Directory	OID Delete User
Enable User	Enables a user in Oracle Internet Directory	OID Modify User
Disable User	Disables a user in Oracle Internet Directory	OID Modify User
Move User	Moves a user account from one container to another in Oracle Internet Directory.	OID Move User
Update Password	Updates the password of a user in Oracle Internet Directory	OID Modify User
Update First Name	Updates the first name of a user in Oracle Internet Directory	OID Modify User
Update Last Name	Updates the last name of a user in Oracle Internet Directory	OID Modify User
Update Department Name	Updates the department name of a user in Oracle Internet Directory	OID Modify User
Update E-mail Address	Updates the e-mail address of a user in Oracle Internet Directory	OID Modify User
Update Location	Updates the location of a user in Oracle Internet Directory	OID Modify User
Update the Middle Name	Updates the middle name of a user in Oracle Internet Directory	OID Modify User
Update Preferred Language	Updates the preferred language for a user in Oracle Internet Directory	OID Modify User
Update Telephone Number	Updates the telephone number of a user in Oracle Internet Directory	OID Modify User
Update Time Zone	Updates the time zone of a user in Oracle Internet Directory	OID Modify User
Update Title	Updates the title of a user in Oracle Internet Directory	OID Modify User
Update Container DN	Updates the container DN of a user in Oracle Internet Directory	OID Move User
Add User to Group	Adds a user to a group in Oracle Internet Directory	OID Add User to Group
Remove User from Group	Removes a user from a group in Oracle Internet Directory	OID Remove User from Group
Add User to Role	Adds a user to a role in Oracle Internet Directory	OID Add User to Role
Remove User from Role	Removes a user from a role in Oracle Internet Directory	OID Remove User from Role
Create OU	Creates an organizational unit	OID Create OU
Rename OU	Changes the name of an organizational unit	OID Change Org Name
Delete OU	Deletes an organizational unit	OID Delete OU
Move OU	Moves the organization sub unit to another parent organizational unit	OID Move OU
Create OID group	Creates an Oracle Internet Directory group	OID Create Group

Table 1–9 (Cont.) User Provisioning Functions Supported by the Connector

Function	Description	Adapter
Delete OID group	Deletes an Oracle Internet Directory group	OID Delete Group
Update Group Name	Updates a group name	Update OID Group Details
Create OID Role	Creates an Oracle Internet Directory role **Note:** In this guide, **OID Role** refers to an organizational role (object class organizationalRole) in the target system, not to an EUS role (object class orclDBEnterpriseRole) stored in the target system. An EUS role is an OID Group. However, you can change OID Role to refer to EUS roles by modifying the Lookup.OID.Role lookup definition appropriately.	OID Create Role
Delete OID Role	Deletes an Oracle Internet Directory role	OID Delete Role
Update Role Name	Updates a role name	Update OID Role Details

1.8.2 User Attributes for Provisioning

Table 1–10 lists the process form fields for which you can specify or modify values during provisioning operations.

Table 1–10 User Attributes for Provisioning

Process Form Field	Target System Attribute	Description	Adapter
User ID	uid	Unique ID of a user account	OID Modify User
First Name	givenname	First name	OID Modify User
Last Name	sn	Last name	OID Modify User
Middle Name	middleName	Middle name	OID Modify User
Common Name	cn	Common name on the target system	OID Modify User
Department	departmentNumber	Department	OID Modify User
Location	l	Location	OID Modify User
Telephone	telephoneNumber	Telephone number	OID Modify User
Email	mail	E-mail address	OID Modify User
Communication Language	PreferredLanguage	Preferred language for communication	OID Modify User
Title	title	Designation	OID Modify User
Container DN	NA	Container in which the user is present on the target system For example: `o=abc,dc=Company`	OID Move User
Time Zone	orclTimeZone	Timezone	OID Modify User
Start Date	orclActiveStartDate	Date from which the user account is active	OID Modify User
End Date	orclActiveEndDate	Date up to which the user account is active	OID Modify User

Table 1–10 (Cont.) User Attributes for Provisioning

Process Form Field	Target System Attribute	Description	Adapter
manager	manager	Distinguished name (DN) of the user's manager.	OID Modify User
Group	groupOfUniqueNames	Name of the group to which a user account belongs	OID Add User to Group
Role	OrganizationalRole	Name of the role that is assigned to the user account	OID Add User to Role

Table 1–11 lists special characters that are supported in process form fields:

Table 1–11 Special Characters Supported in Process Form Fields

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

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

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

1.8.3 Group Attributes for Provisioning

Table 1–12 provides information about group attribute mappings for provisioning.

Table 1–12 Group Attributes for Provisioning

Process Form Field	Target System Attribute	Description	Adapter
Group Name	cn	Group name	Update OID Group Details

1.8.4 Role Attributes for Provisioning

Table 1–13 provides information about role attribute mappings for provisioning.

Table 1–13 Role Attributes for Provisioning

Process Form Field	Target System Attribute	Description	Adapter
Role Name	cn	Role name	Update OID Role Details

1.9 Roadmap for Deploying and Using the Connector

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

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

2

Deploying the Connector

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

- Section 2.1, "Preinstallation"
- Section 2.2, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

Preinstallation information is divided across the following sections:

- 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"

2.1.1.1 Files and Directories on the Installation Media

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

Table 2–1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
configuration/OracleInternetDirectory-CI.xml	This XML file contains configuration information that is used during connector installation.
lib/OIDProv.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/OIDRecon.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.
Files in the test/troubleshoot directory	These files are used to perform basic tests on the connector, even before Oracle Identity Manager is installed.
xml/oimOIDUser.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ Process form ■ Process task and adapters (along with their mappings) ■ Resource object ■ Xellerate User (OIM User) ■ Provisioning process ■ Pre-populate rules ■ Reconciliation process ■ Lookup definitions
xml/OIDXLuser.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the test/troubleshoot 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 9.1.0.*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/OIDProv.jar

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

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

2.1.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the procedure described in the following sections:

- Section 2.1.2.1, "Creating a Target System User Account for Connector Operations"
- Section 2.1.2.2, "Using External Code Files"

2.1.2.1 Creating a Target System User Account for Connector Operations

You can create a target system user account for connector operations by performing the procedure described in one of the following sections:

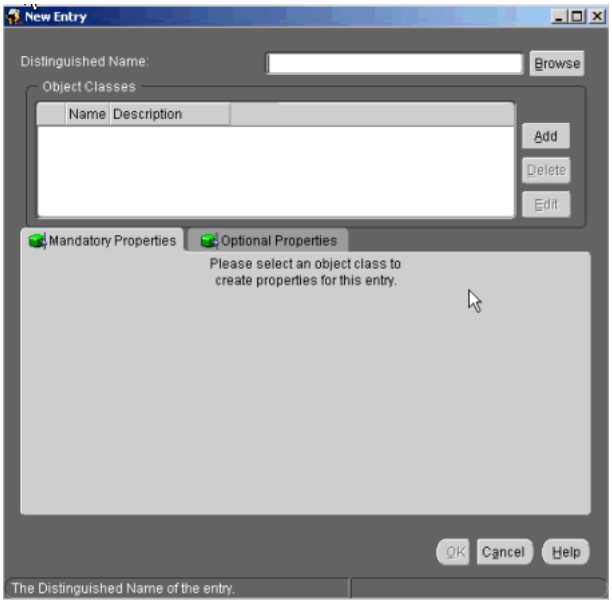
- If you are using Oracle Internet Directory release 10.1.*x*, see Section 2.1.2.1.1, "Creating a Target System User account for Connector Operations using Oracle Directory Manager."
- If you are using Oracle Internet Directory release 10.1.*x* or 11gR1, see Section 2.1.2.1.2, "Creating a Target System User Account for Connector Operations using Oracle Internet Directory Command-Line Utilities."

2.1.2.1.1 Creating a Target System User account for Connector Operations using Oracle Directory Manager

The connector uses a target system account to connect to the target system during reconciliation.To create a target system user account with the minimum permissions required to perform connector operations:

1. To create a user account on the target system:
   a. Log in to Oracle Directory Manager as an administrator.
   b. In the left pane, under Oracle Internet Directory Server, expand the directory server instance that you want to access, and then expand **Entry Management**.
   c. Navigate to and right-click the context under which you want to create the user. Then, click **Create**.

      The New Entry window is displayed as shown in the following screenshot:

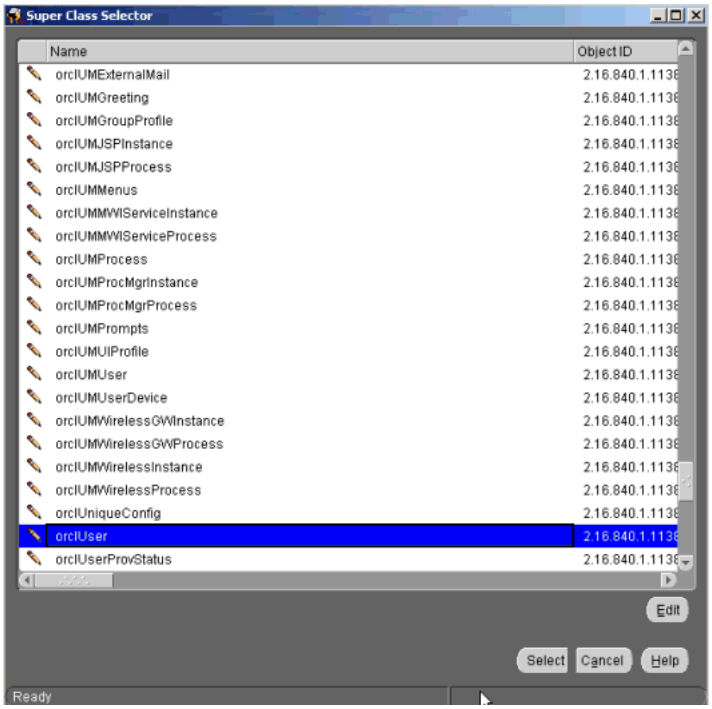


d. In the **Distinguished Name** field, enter the DN in which you want to create the user. Alternatively, you can click **Browse** and find the DN.

e. To add an object class to the user:

- In the Object Classes section, click **Add**.
- In the Super Class Selector dialog box, select the **top** object class, and then click **Select**.

  The following screenshot shown the Super Class Selector window in which the orclUser object class has been selected:



f. Repeat Step e to add each of the following object classes:

- person
- organizationalPerson
- inetOrgPerson
- orclUser
- orclUserV2

g. On the Mandatory Properties tab, enter values for all attributes. For example, in the text field for the sn attribute, enter the last name or surname of user being created.

h. If required, on the Optional Properties tab, enter values for the required attributes.

i. Click **OK**.

The user is created and is displayed in the left pane under the appropriate content.

2. To grant the user (that you created in Step 1) access rights to perform connector operations:

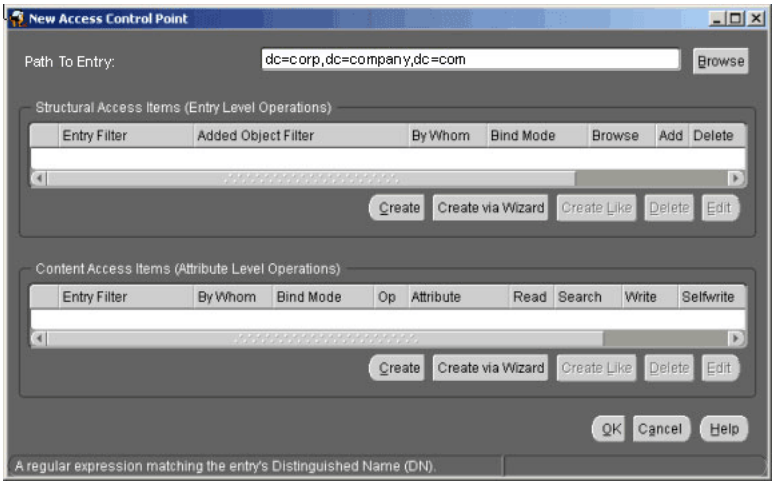
a. In the left pane, under Oracle Internet Directory Server, expand the directory server instance that you want to access, and then expand **Access Control Management**.

b. Right-click **Access Control Management** and select **Create**.

The New Access Control Point window is displayed.

c. In the **Path to Entry Field**, enter the DN that the user should be granted access to. Alternatively, you can click **Browse** to find the DN.

The following screenshot shows the New Access Control Point window in which a sample value for the Path to Entry Field has been entered:

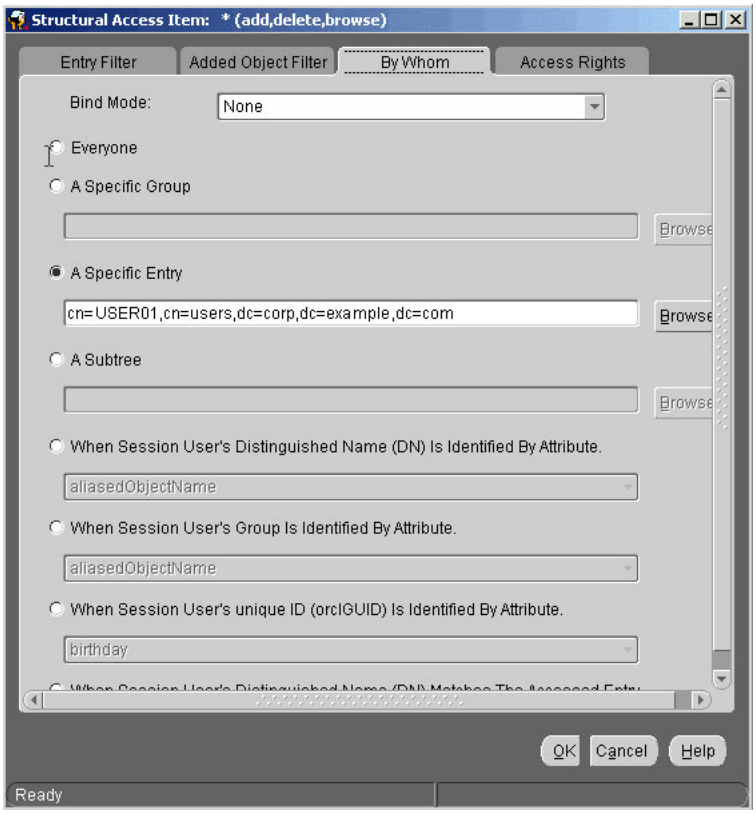


d. In the Structural Access Items section, click **Create**.

The Structural Access Item window is displayed.

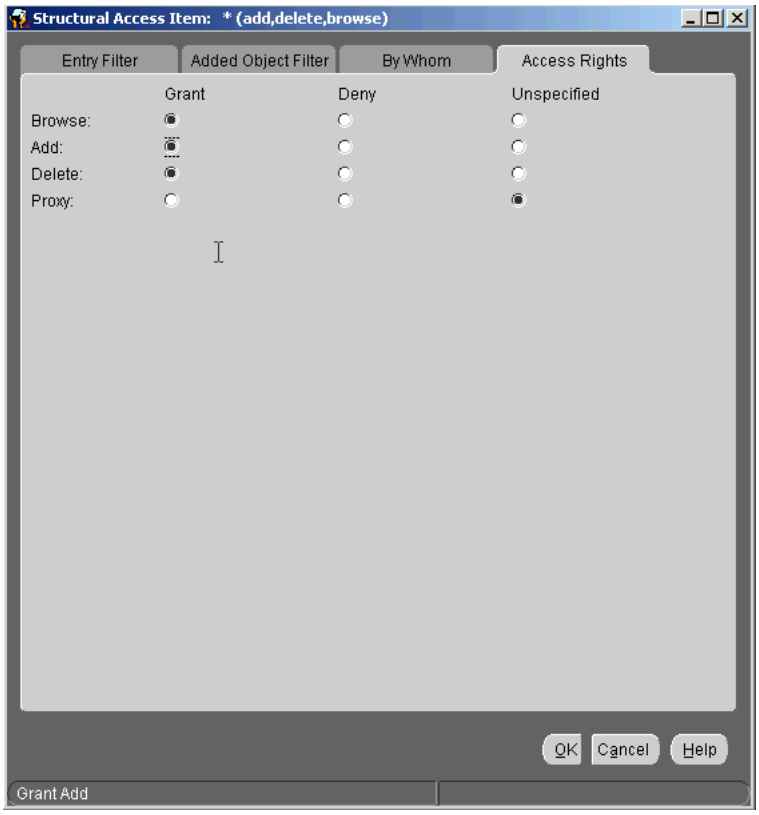
e. On the By Whom tab, select **A Specific Entry**, and then in the corresponding field, enter the DN in which the user (created in Step 1) exists.

The following screenshot shows the By Whom tab on which a sample value for the A Specific Entry field has been entered:



f. On the Access Rights tab, select the **Browse, Add,** and **Delete** access rights under the Grant column. Under the Unspecified column, select **Proxy**.

The following screenshot shows the Access Rights tab on which access rights have been selected:



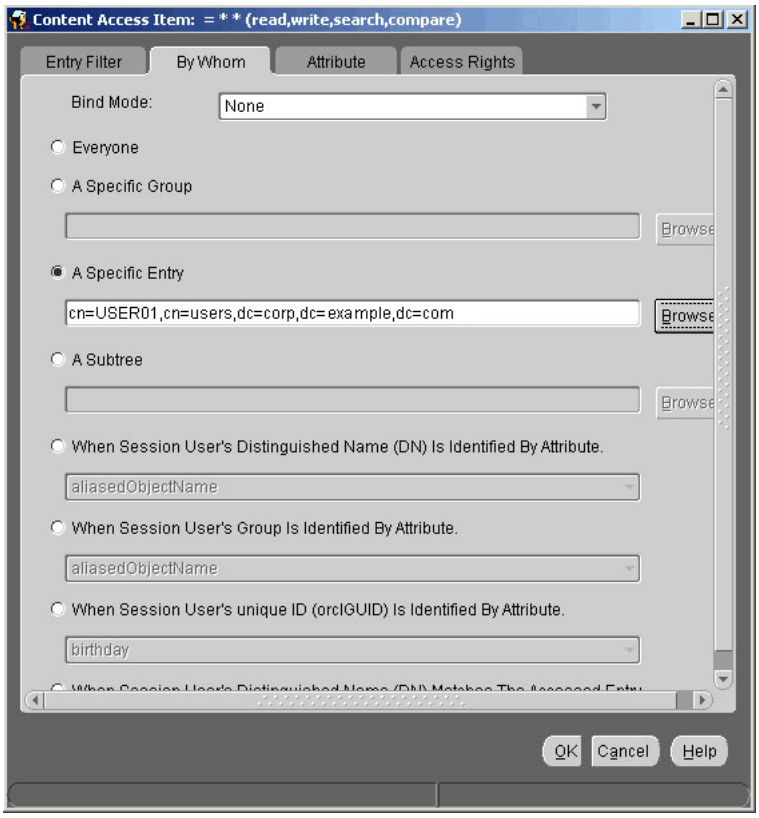
g. Click **OK**.

h. In the Content Access Items section, click **Create**.

The Content Access Item window is displayed.

i. On the By Whom tab, select **A Specific Entry**, and then in the corresponding field, enter the DN in which the user (created in Step 1) exists.

The following screenshot shows the By Whom tab on which a sample value for the A Specific Entry field has been entered:



j. On the Attribute tab, from the Attribute list on the right side, select *, which specifies that the user is granted access to all attributes.

On left hand side, select **EQ**, which is the matching operation to be performed against the attribute.

For example, if you select EQ and *, then the access rights that you grant apply to all attributes. The following screenshot shows the values used in the example:

k. On the Access Rights tab, select the **Read, Search, Write,** and **Compare** permissions under the Grant column. Under the Unspecified column, select **Selfwrite**.

The following screenshot shows the Access Rights tab on which permissions have been selected:

l. Click **OK**.

m. In the New Access Control Point window, click **OK**.

The access control point is created.

3. To verify whether the access control point (created in Step 2) was created properly:

a. Log in to Oracle Directory Server with the complete DN of the user (created in Step 1).

b. If the following error message is displayed, then the access control point is not created properly.

```
Bind of request to LDAP Server failed.
```

Otherwise, the access control point is created successfully.

Note: After creating the user you will be able to login to OID via that user, but you will not able to create user on the target system as it shows insufficient rights and throws LDAP error code 50. To overcome this error, you need to add the new administrator to a group REALM ADMINISTRATORS in groups in ORACLE CONTEXT on the target system.

2.1.2.1.2 Creating a Target System User Account for Connector Operations using Oracle Internet Directory Command-Line Utilities

The following procedure creates an admin user, admin group, and ACIs using the Oracle Internet Directory command-line utilities.

To use this procedure, you must be an administrator on the OID target system who is familiar with command-line utilities such as ldapsearch and ldapmodify. Alternatively, you can also use Oracle Directory Services Manager to perform these functions.

For more information, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory.*

Note: In this procedure, replace:

- `dc=example`, `dc=com` with the root suffix.
- `cn=MyAccounts,dc=example,dc=com` with the base location of the users and groups that will be managed by the connector.
- `admin user name` with the administrator user name. For example, oimAdminUser.
- `password` with the administrator user password.
- `admin group name` with the name of the group that the administror belongs to. For example, oimAdminGroup.
- *`OID-Server`* with the hostname or IP address of the computer that is running OID.
- *`OID-Port`* with the port at which the OID server is listening.

To create the admin user, group, and ACIs for connector operations:

1. Create a new file name oidadmin.ldif and add the following entries:

```
dn: cn=systemids,dc=example,dc=com
changetype: add
objectclass: orclContainer
objectclass: top
cn: systemids


dn: cn=oimAdminUser,cn=systemids,dc=example,dc=com
changetype: add
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: oimAdminUser
givenname: oimAdminUser
sn: oimAdminUser
cn: oimAdminUser
uid: oimAdminUser
userPassword: welcome1


dn: cn=oimAdminGroup,cn=systemids,dc=example,dc=com
changetype: add
objectclass: groupOfUniqueNames
objectclass: orclPrivilegeGroup
objectclass: top
cn: oimAdminGroup
description: OIM administrator role
```

```
uniquemember: cn=oimAdminUser,cn=systemids,dc=example,dc=com


dn: cn=oracleAccounts,dc=example,dc=com
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=oimAdminGroup,cn=systemids,dc=example,dc=com" (add,browse,delete) by
* (none)
orclaci: access to attr=(*) by
group="cn=oimAdminGroup,cn=systemids,dc=example,dc=com"
(read,search,write,compare) by * (none)


dn: cn=changelog
changetype: modify
add: orclaci
orclaci: access to entry by
group="cn=oimAdminGroup,cn=systemids,dc=example,dc=com" (browse) by * (none)
orclaci: access to attr=(*) by
group="cn=oimAdminGroup,cn=systemids,dc=example,dc=com" (read,search,compare)
by * (none)
```

2. Run the following command to load the oidadmin.ldif file:

   ```
   ./ldapmodify -h OID-Server -p OID-port -D OID-Admin-ID -w OID-Admin-password
   -c-v-f oidadmin.ldif
   ```

3. Run the following command to check if the ACI is added:

   ```
   /ldapsearch -h OID-Server -p OID-Port -D "cn=orcladmin" -w OID-Admin-password
   -b "dc=example,dc=com" -s one "objectclass=*" orclaci
   ```

4. Run the following command to check if the proxy user is working against OID. Before running this command ensure that the changenumber is catalogued.

   ```
   ./ldapsearch -h OID-Server -p OID-Port -D
   "cn=oimAdminUser,cn=systemids,dc=example,dc=com" -w OID-Admin-password -b
   "cn=changelog" -s sub "changenumber>=0"
   ```

   If the above command returns an error, run the following command:

   ```
   ./ldapsearch -h OID-Server -p OID-Port -D
   "cn=oimAdminUser,cn=systemids,dc=example,dc=com" -w OID-Admin-password -b
   "cn=changelog" -s sub "changenumber>=0"
   ```

2.1.2.2 Using External Code Files

The ldap.jar file contains APIs that are used to connect to the target system. 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 file from the Sun Web site and copy it into the ThirdParty directory as follows:

1. Log on to the JNDI Downloads section of the Sun Web site at

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

2. On the JNDI Downloads page, click **Download JNDI 1.2.1 & More**.
3. Select the **I agree to the Software License Agreement** check box, and then click **Continue**.
4. Select **LDAP Service Provider, 1.2.4**.
5. Click **jndi-1_2_4.zip**.
6. Specify the temporary directory into which you want to download the ldap-1_2_4.zip file.

7. Extract the contents of the ldap-1_2_4.zip file.
8. From the lib directory inside the ldap-1_2_4.zip file, copy the ldap.jar and ldapbp.jar files into one of the following directories:

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

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

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

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

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

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

- Section 2.2.1, "Running the Connector Installer"
- Section 2.2.2, "Configuring the IT Resource"

2.2.1 Running the Connector Installer

To run the Connector Installer:

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

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

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

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

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

  Oracle Fusion Middleware Administrator'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 **Oracle Internet 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 **Oracle Internet 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 XML files (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 2.3.1.1, "Configuring Trusted Source Reconciliation."

   c. Compilation of adapters.

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

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

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

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

   Note: At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

   There are no prerequisites for some predefined connectors.

b. Configuring the IT resource for the connector

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

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

---

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

See *Oracle Fusion Middleware 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 server.

2.2.2 Configuring the IT Resource

Note: The "modifytimestamp" code key and decode entry is newly added to the AttrName.Recon.Map.OID lookup definition. This entry holds the timestamp of the last successfully reconciled user record from the target system. This timestamp value is retrieved from the target system and is saved as the value of the Last Target Recon TimeStamp IT resource parameter.

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

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration section, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter OID Server and then click **Search**.

5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Description
Admin Id	DN value of the user who has administrator rights on the Oracle Internet Directory server Sample value: `cn=Admin,ou=People, o=xyz`
Admin Password	Password of the user who has administrator rights on the target Oracle Internet Directory server
Server Address	IP address of the Oracle Internet Directory server
Port	Port number to connect to the Oracle Internet Directory server Sample value: `389`

Root DN	Base DN on which all the user operations are to be carried out
	Sample value:
	`dc=`*`host_name`*`, dc=com`
	If the domain name is different from the host name, then specify the domain name as the value of this parameter.
	For example:
	If the host name is myhost.example.com and domain name is mydomain.example.com, then specify the following as the value of this parameter:
	`dc=mydomain, dc=example, dc=com`

SSL	If this parameter is set to `true`, then SSL is used to secure communication between Oracle Identity Manager and the Oracle Internet Directory server. In this case, the authentication certificate of the Oracle Internet Directory server must be imported into the Oracle Identity Manager server. If this parameter is set to `false`, then SSL is not used to secure communication between Oracle Identity Manager and the Oracle Internet Directory server. **Note:** It is recommended that you enable SSL to secure communication with the target system.
Prov Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning a user. The value must be `AttrName.Prov.Map.OID`.
Prov Group Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning a group. The value must be `AttrName.Group.Prov.Map.OID`.
Prov Role Attribute Lookup Code	Name of the lookup definition that has the target attribute mappings required for provisioning a role. The value must be `AttrName.Role.Prov.Map.OID`.

Parameter	Description
Use XL Org Structure	If set to `true`, then the Oracle Identity Manager organization structure is used during provisioning and reconciliation. During provisioning, you can configure the users to be provisioned in a different organization instead of the default `Xellerate Users` in Oracle Identity Manager. Consider the following example. Suppose a custom organization `org1` exists in the target system: `ou=org1,dc=corp,dc=company,dc=com` In the preceding sample, you can choose `org1` from the lookup in the Xellerate form and provision the user to the target system. In the preceding sample, the lookup must be populated with specific organization values. Oracle recommends that you first run a full reconciliation with `Use XL Org Structure=true` and then provision a user. Once the full reconciliation is run, the data in the target system is replicated in Oracle Identity Manager. As a result lookup gets populated with the organization/organizational unit values automatically during the reconciliation. If you do not run a full reconciliation, then the organization must first be manually created and then the user should be provisioned. The name of the entity should be the same as that in the target system with identical casing. During reconciliation, if this attribute is set to `true`, then the users are reconciled in the respective organization as specified in the target system. Suppose, a user belongs to `ou=org2,dc=corp,dc=company,dc=com` in the target system. During reconciliation, the user gets updated in `org2` in Oracle Identity Manager. This helps in maintaining the same organization structure in the target system and Oracle Identity Manager. If set to `false`, then the value of the Organization field in the process form is used for provisioning and the organization or container in the target Oracle Internet Directory is used for reconciliation. If the value is set to `false`, then all the users are provisioned and reconciled in the default Oracle Identity Manager organization, `Xellerate Users`.
Last Trusted Recon TimeStamp	For the first trusted user reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the timestamp of the last successfully reconciled user record is stored in this parameter. You do not need to provide a value for this parameter. Sample value: `20060524110907Z`
Last Target Recon TimeStamp	For the first target user reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the timestamp of the last successfully reconciled user record is stored in this parameter. You do not need to provide a value for this parameter. Sample value: `20060524110907Z`
Last Trusted Delete Recon TimeStamp	For the first trusted delete user reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the timestamp of the last successfully reconciled deleted user record is stored in this parameter. You do not need to provide a value for this parameter. Sample value: `20060524110907Z`
Last Target Delete Recon TimeStamp	For the first target delete user reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the timestamp of the last successfully reconciled deleted user record is stored in this parameter You do not need to provide a value for this parameter. Sample value: `20060524110907Z`

Parameter	Description
Group Reconciliation Time Stamp	For the first group reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of group reconciliation was completed is stored in this parameter. You do not need to provide a value for this parameter. Sample value: `20060524110907Z`
Role Reconciliation Time Stamp	For the first role reconciliation run, the timestamp value is not set. For subsequent rounds of reconciliation, the time at which the previous round of role reconciliation was completed is stored in this parameter. You do not need to provide a value for this parameter. Sample value: `20060524110907Z`

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

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

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

2.3.1 Postinstallation on Oracle Identity Manager Server

Postinstallation on Oracle Identity Manager involves performing the procedure described in the following sections:

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

- Section 2.3.1.1, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.2, "Changing to the Required Input Locale"
- Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.4, "Enabling Logging"
- Section 2.3.1.5, "Modifying the Value of the checkouttime Attribute"
- Section 2.3.1.6, "Setting Up Lookup Definitions in Oracle Identity Manager"
- Section 2.3.1.7, "Configuring High Availability of the Target System"
- Section 2.3.1.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 2.3.2.1, "Configuring the Target System"

2.3.1.1 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, OIDXLuser.xml, by using the Deployment Manager. Section 2.3.1.1.1, "Importing the XML File for Trusted Source Reconciliation" describes the procedure to import the XML file.

Note: Only one target system can be designated as a trusted source. If you import the OIDXLuser.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

---

2. Add the default password policy to the Xellerate User resource object. Section 2.3.1.1.2, "Adding the Default Password Policy for Xellerate User Resource Object" describes the procedure to add the default password policy.
3. Use the OID User Trusted Recon scheduled task to run trusted reconciliation.

Note: The OID Trusted Delete User Recon task is run with the DN value, which is the value for the `SearchBase` attribute in the User Reconciliation scheduled task. The value of this attribute specifies the organizational unit from where users are reconciled from the target system into Oracle Identity Manager. When you run the `OID Trusted Delete User Recon` task, all of the users in the other organizational units are deleted in Oracle Identity Manager.

2.3.1.1.1 Importing the XML File for Trusted Source Reconciliation

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.

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

4. Locate and open the OIDXLuser.xml file located in the following directory:

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

     OIM_HOME/xellerate/ConnectorDefaultDirectory/OID_904140/xml

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/OID_904140/xml

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

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

After you import the XML file for trusted source reconciliation, you must add the default password policy to the Xellerate User resource object.

2.3.1.1.2 Adding the Default Password Policy for Xellerate User Resource Object

To add the default password policy to the Xellerate User resource object:

1. Log in to Design Console.
2. Expand **Resource Management,** then double-click **Resorce Objects.**
3. Search for and open the **Xellerate User** resource object.
4. On the Password Policies Rule tab, click **Add.**
5. From the row that is displayed, double-click the **Rule** lookup field.
6. From the Lookup dialog box, select **Default,** and assign it to the resource object.
7. Click **OK.**
8. In the adjacent column, double-click the **Policy** lookup field.
9. From the Lookup dialog box, select **Default Policy,** and assign it to the resource object.
10. Click **OK.**
11. In the Priority field, enter the numeric value `1` .
12. Click **Save.**

After you add the default password policy to the resource object, you must specify values for the attributes of the OID User Trusted Recon scheduled task. This procedure is described in Section 3.4, "Configuring Scheduled Tasks."

2.3.1.2 Changing to the Required Input Locale

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

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

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

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager 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 9.1.0.*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 9.1.0.*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 9.1.0.*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.

2.3.1.4 Enabling Logging

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

- Section 2.3.1.4.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.1.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.4.1 Enabling Logging on Oracle Identity Manager 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:

- **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.OID=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.OID=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.OID">
        <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.OID">
   <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.OID=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.OID=INFO
     ```

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

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

- **Oracle WebLogic Server**

  To enable logging:

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

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

  After you enable logging, log information is displayed on the server console.

2.3.1.4.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

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

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

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

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

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

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

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

```
   </log_handler>

<logger name="XL_INTG.OID" level="[LOG_LEVEL]" useParentHandlers="false">
     <handler name="oid-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 2–2 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='oid-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.OID" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="oid-handler"/>
     <handler name="console-handler"/>
   </logger>
```

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

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

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

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

2.3.1.5 Modifying the Value of the checkouttime Attribute

To ensure that the connector XML files are correctly imported, you must provide a higher value, 50000 or more, for the checkouttimeout attribute in the following file:

- For Oracle Identity Manager release 9.1.0.*x*

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1

  /db/oim-config.xml

  The oim-config.xml file is in the metadata store (MDS).

To modify the xlconfig.xml file:

1. In a text editor, open the *OIM_HOME*/xellerate/config/xlconfig.xml file for editing.
2. Search for and set the value of the checkouttime attribute to value greater than 50000.
3. Save and close the file.

To modify the oim-config.xml file:

1. Export the /db/oim-config.xml file from MDS to a temporary location on the Oracle Identity Manager host computer as follows:
   a. Ensure that you have set the environment for running the Oracle Identity Manager MDS Export utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.
   b. In a command window, change to the *OIM_HOME*\server\bin directory.
   c. Run one of the following commands:
      – On Microsoft Windows

        ```
        weblogicExportMetadata.bat
        ```

      – On UNIX

        ```
        weblogicExportMetadata.sh
        ```

2. In a text editor, open the oim-config.xml file for editing.
3. Search for and set the value of the checkouttime attribute to value greater than 50000.
4. Save and close the file.
5. Import the oim-config.xml file into the db directory in MDS as follows:
   a. Ensure that you have set the environment for running the Oracle Identity Manager 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.
   b. In a command window, change to the *OIM_HOME*\server\bin directory.
   c. Run one of the following commands:
      – On Microsoft Windows

        ```
        weblogicImportMetadata.bat
        ```

      – On UNIX

        ```
        weblogicImportMetadata.sh
        ```

d. When prompted, enter value for the following:

   – `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 oim-config file is imported into MDS.

2.3.1.6 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.

The following sections discuss lookup definitions that you must manually configure in Oracle Identity Manager:

- Section 2.3.1.6.1, "Setting Up the Lookup.OID.Configuration Lookup Definition"
- Section 2.3.1.6.2, "Setting Up the Lookup.OID.PrefLang Lookup Definition"

2.3.1.6.1 Setting Up the Lookup.OID.Configuration Lookup Definition You can specify values for the following entries in the Lookup.OID.Configuration lookup definition:

- specialcharacter

  Use the specialcharacter parameter to specify the special characters that must not be allowed in the User ID and Common Name fields during reconciliation and provisioning operations. To add a special character to the default value, append the character to the default value without adding a space or any other delimiter.

  Default value: `~`!@#%^&*_-+=:,.?|`

- ldapConnectTimeOut

  Enter the timeout interval (in milliseconds) after which the connector must start trying to establish a connection with the backup target system installations.

  Default value: `3000`

2.3.1.6.2 Setting Up the Lookup.OID.PrefLang Lookup Definition You use the Lookup.OID.PrefLang lookup definition to specify a language for the user during a provisioning operation.

Note: If you want to add entries in this lookup definition, then ensure that the entries are in the format used for the default values.

Table 2–3 Entries in the Lookup.OID.PrefLang Lookup Definition

Code Key	Decode
BrazilianPortuguese	BrazilianPortuguese
English	English
French	French
German	German
Italian	Italian
Japanese	Japanese
SimplifiedChinese	SimplifiedChinese
Spanish	Spanish
TraditionalChinese	TraditionalChinese

2.3.1.7 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.OID.Backup server 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.OID.Backup server 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.OID.Backup server 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 Fusion Middleware User's Guide for Oracle Identity Manager* for information about working with lookup definitions

Table 2–4 shows samples entries for the Lookup.OID.Backup server lookup definition.

Table 2–4 Samples Entries for the Lookup.OID.Backup server Lookup Definition

Code Key	Decode
172.20.55.64	172.20.55.65:389
172.20.55.64	172.20.55.66:390
172.20.55.97	172.20.55.98:440

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.

2.3.1.8 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 Oracle Internet Directory 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 2.3.1.8.1, "Copying Predefined Request Datasets"
- Section 2.3.1.8.2, "Importing Request Datasets into MDS"
- Section 2.3.1.8.3, "Enabling the Auto Save Form Feature"
- Section 2.3.1.8.4, "Running the PurgeCache Utility"

2.3.1.8.1 Copying Predefined Request Datasets

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

ProvisionResourceOID User.xml

Copy the file from the DataSets directory on the installation media to the *OIM_HOME*/DataSet/file directory.

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.

2.3.1.8.2 Importing Request Datasets into MDS

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

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

To import a request dataset definition into MDS:

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

2.3.1.8.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

2.3.1.8.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.3.2 Postinstallation on the Target System

Postinstallation on the target system consists of the following procedure.

2.3.2.1 Configuring the Target System

You must configure incremental and role reconciliation by making the modifytimestamp and roleoccupant attributes, respectively, searchable attributes.

Similarly, you must configure full reconciliation by making both the modifytimestamp and roleoccupant attributes searchable.

To configure the target system for incremental, role, or full reconciliation:

1. If you want to configure incremental reconciliation, then make modifytimestamp a searchable attribute. To do so, use the catalog.sh file to index modifytimestamp.

   See *Oracle Identity Management User Reference Release 10g (10.1.4.0.1)* for information about the procedure.

2. If you want to configure role reconciliation, then make roleoccupant a searchable attribute. To do so, use the catalog.sh file to index roleoccupant.

   See *Oracle Identity Management User Reference Release 10g (10.1.4.0.1)* for information about the procedure.

3. If you want to configure full reconciliation, then make modifytimestamp and roleoccupant searchable attributes. To do so, use the catalog.sh file to index both modifytimestamp and roleoccupant.

   See *Oracle Identity Management User Reference Release 10g (10.1.4.0.1)* for information about the procedure.

4. Restart Oracle Internet Directory for the change to take effect.

2.3.3 Configuring SSL

Note:

This is an optional step of the deployment procedure.

The connector supports only Mode 1 secure connections to Oracle Internet Directory.

To set up SSL connectivity between Oracle Identity Manager and the Oracle Internet Directory server:

1. Configure SSL on Oracle Internet Directory and then export the Oracle Internet Directory server certificate using Wallet Manager.

   See the "Secure Sockets Layer and the Directory" chapter of *Oracle Internet Directory Administrator's Guide* for detailed instructions.

Note: For Mode 1 secure connection, you must select SSL Server Authentication as the SSL Authentication.

The default non-SSL port is 389. The default SSL port is 636. When you create a configuration set of Oracle Internet Directory, it is recommended that you select a different port (for example, 1636) for SSL communication with Oracle Identity Manager.

2. Check if the Oracle Internet Directory server is listening at the SSL port. If it is not, then set it to the SSL port (typically, the default SSL port is 636). Then, restart the server.
3. Import the certificate from the target system into the JSDK (the JSDK that is used during installation of Oracle Identity Manager) `cacerts` keystore as follows:

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

4. If you are using Oracle Identity Manager release 11.1.1, then import the target system 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. Restart the Oracle Identity Manager server.
6. In the OID Server IT resource definition:
   - Set the `SSL` parameter value to `true`.
   - Set the `Port` parameter value to the SSL port number. Typically, this number is 636.

3

Using the Connector

This chapter is divided into the following sections:

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

3.1 Performing First-Time Reconciliation

First-time 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 3.2, "Scheduled Tasks for Lookup Field Synchronization" for information about the attributes of the scheduled tasks for lookup field synchronization.

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

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

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

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

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

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

See Also: Section 2.2, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" 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.

3.2 Scheduled Tasks for Lookup Field Synchronization

The following scheduled tasks are used for lookup fields synchronization:

- Organization Lookup Reconciliation
- Role Lookup Reconciliation
- 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 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

Note:

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

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

Attribute	Description

LookupCodeName	This attribute holds the name of the lookup definition with which the values are to be synchronized.
	■ Default value for groups:
	`Lookup.OID.Group`
	■ Default value for roles:
	`Lookup.OID.Role`
	■ Default value for organizational units and organizations:
	`Lookup.OID.Organization`

ITResourceName	This attribute holds the name of the IT resource that contains connection information to connect to Oracle Internet Directory Default value: `OID Server`
SearchContext	Enter the search context (DN of the root that holds the group or role) to be used for fetching lookup field values from the target system Default value: `dc=corp,dc=company,dc=com`

ObjectClass	This attribute holds the name of the object class.
	The following are sample values:
	■ Default value for groups:
	`groupOfUniqueNames`
	■ Default value for roles:
	`OrganizationalRole`
	■ Default value for organizations:
	`Organization`
	■ Default value for organizational units:
	`OrganizationalUnit`

CodeKeyLTrimStr	The default value of this attribute is `[None]`. Do not change this value.
CodeKeyRTrimStr	Enter the string value that must be right-trimmed from each value returned by the scheduled task. Sample value: `,dc=corp,dc=company,dc=com` If there is nothing to be trimmed, then specify the value `[NONE]`.
ReconMode	Enter `REFRESH` if you want to completely refresh the existing lookup. Existing values in the lookup definition are deleted and then new values are added. Enter `UPDATE` if you want to update the lookup definition with new values. Existing values in the lookup definition are left untouched.

Table 3–1 (Cont.) Attributes of the Scheduled Tasks for Lookup Field Synchronization

Attribute	Description

AttrType	This attribute holds the naming attribute of the object on the target system.
	■ Default value for roles:
	`cn`
	■ Default value for groups:
	`cn`
	■ Default value for organizations:
	`ou`

ConfigurationLookup	This attribute holds the name of the configuration lookup definition, which contains values that are used during connector operations. Default value: `Lookup.OID.Configuration`

3.3 Configuring Reconciliation

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

- Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Paged Reconciliation"
- Section 3.3.4, "Reconciliation Scheduled Tasks"

3.3.1 Full Reconciliation vs. Incremental Reconciliation

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

If you set the time-stamp parameter to `0`, then full reconciliation is performed. In full reconciliation, all existing target system records are fetched into Oracle Identity Manager for reconciliation.

You can switch from incremental to full reconciliation at any time by setting the time-stamp parameter to `0`.

3.3.2 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 a reconciliation filter.

For this connector, you create a filter by specifying a query condition as the value of the SearchFilter attribute while configuring the scheduled task for user, group, or role reconciliation. The query condition must be in the LDAP format, as shown in the following sample value:

```
(objectclass=inetOrgPerson)
```

Note: You must enclose the query condition in parentheses as shown in the sample value.

With this query condition, only records for users whose objectclass is inetOrgPerson are considered for reconciliation.

You can add multiple query conditions by using the logical operators:

- The AND operator represented by the ampersand (&)
- The OR operator represented by the vertical bar (|)
- The EQUAL operator represented by the equal sign (=)

For example, the following query condition is used to limit reconciliation to records of those users whose first name is John and objectclass is inetOrgPerson:

```
(&(objectClass=inetOrgPerson)(givenname=John))
```

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))
```

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.

While specifying a value for the SearchFilter attribute, ensure that you do 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.

3.3.3 Paged Reconciliation

Note: This feature is supported only on Oracle Internet Directory 10.1.4.0.1 or later.

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

You can configure paged reconciliation to avoid these problems.

To configure paged reconciliation, you must specify a value for the PageSize attribute of the user reconciliation scheduled task while performing the procedure described in Section 3.4, "Configuring Scheduled Tasks."

3.3.4 Reconciliation Scheduled Tasks

When you run the Connector Installer or import the connector XML file, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- Section 3.3.4.1, "Scheduled Tasks for User Reconciliation"
- Section 3.3.4.2, "Scheduled Tasks for Group and Role Reconciliation"

3.3.4.1 Scheduled Tasks for User Reconciliation

The following scheduled tasks are used for user reconciliation:

Note: The procedure to configure these scheduled tasks is described later in the guide.

- OID User Target Recon Task
- OID Target Delete Recon Task
- OID User Trusted Recon Task
- OID Trusted Delete Recon Task

You must specify values for the set of scheduled tasks that are used for the mode (target resource or trusted source) in which you are using the connector. Table 3–2 describes the attributes of these scheduled tasks.

Note: This table describes the attributes of all the scheduled tasks for user reconciliation. Some of these attributes are not common to all the scheduled tasks.

Section 3.4, "Configuring Scheduled Tasks" describes the procedure to configure scheduled tasks.

Table 3–2 Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
ITResourceName	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `OID IT Resource`
TrustedResourceObjectName	This attribute holds the name of the resource object that is used in trusted reconciliation. Default value: `Xellerate User`
TargetResourceObjectName	This attribute holds the name of the resource object that is used in target reconciliation. Default value: `OID User`
SearchBase	Enter the DN value of the user container from which users must be reconciled into Oracle Identity Manager. Default value: `dc=corp,dc=company,dc=com`
ConfigurationLookup	This attribute holds the name of the lookup definition that stores the configurable attributes used for connector operations. Default value: `Lookup.OID.Configuration`
SearchFilter	Enter the search filter in LDAP format for fetching records from the target system during the reconciliation run. Default value: `(objectclass=inetOrgPerson)` See Section 3.3.2, "Limited Reconciliation" for more information.
Recon Attribute Lookup Code	This attribute holds the name of the lookup definition that holds mapping between the OID User resource object and target system attributes. Default value: `AttrName.Recon.Map.OID`
Organization	This attribute holds the name of the Oracle Identity Manager organization in which reconciled users must be created. Default value: `Xellerate Users`
Xellerate Type	This attribute holds the default employee type for the OIM User. Default value: `End-User Administrator`
Role	This attribute holds the default role for the OIM User. Default value: `Consultant`
PageSize	This attribute is used for paged reconciliation. During a reconciliation run, the total set of records to be reconciled is divided into pages and the PageSize attribute specifies the number of records that must constitute one page. It is recommended that you set a page size between 100 and 1000. Default value: `100` See Section 3.3.3, "Paged Reconciliation" for more information.
SearchScope	This attribute determines the search scope of users within the DN specified as the value of the SearchBase attribute. Enter `onelevel` if you want the connector to fetch records only from the same level of the DN. The DN is specified as the value of the SearchBase attribute. Enter `subtree` if you want the connector to fetch records from the of the DN (specified as the value of the SearchBase attribute) and all its subtrees.

3.3.4.2 Scheduled Tasks for Group and Role Reconciliation

The following scheduled tasks are used for reconciling groups or roles:

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."

- OID Group Recon Task
- OID Role Recon Task

You must specify values for the scheduled tasks that are used for group or role reconciliation. Table 3–3 describes the attributes of these scheduled tasks.

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

Attribute	Description
ConfigurationLookup	This attribute holds the name of the lookup definition that stores the configurable attributes used for connector operations. Default value: `Lookup.OID.Configuration`
Field Lookup Code	This attribute holds the name of the lookup definition that stores reconciliation field mappings for group or role connector operations. Provide the corresponding reconciliation lookup mappings. Default value: For group reconciliation: `Lookup.OIDGroupReconciliation.FieldMap` For role reconciliation: `Lookup.OIDRoleReconciliation.FieldMap`
isRoleRecon	Enter `yes` if you want role reconciliation to be performed. Enter `no` if you want group reconciliation to be performed. Default value: `yes`
ITResourceName	This attribute holds the name of the IT resource that contains connection information to connect to Oracle Internet Directory. Default value: `OID IT Resource`
MultiValued Attributes	Enter the list of multivalued attributes that you add for reconciliation and provisioning. The default value of this attribute is `[NONE]`. Sample value: `owner|description` See the following sections for information about adding multivalued attributes: Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation" Section 4.7, "Adding New Multivalued Attributes for Provisioning"

Table 3–3 (Cont.) Attributes of the Group and Role Reconciliation Scheduled Tasks

Attribute	Description
ResourceObjectName	Enter the name of the resource object into which groups or roles are to be reconciled. The value can be one of the following: ■ For group reconciliation: `OID Group` ■ For role reconciliation: `OID Role`
SearchBase	Enter the DN value of the user container from which users must be reconciled into Oracle Identity Manager. Sample value: `cn=users,dc=hostname,dc=com` In this value, *`users`* is the name of the user container and *`hostname`* is the host name under which the `oracle` context is created.
SearchFilter	Enter the search filter in LDAP format for fetching records from the target system during the reconciliation run. Default value: `(objectclass=inetOrgPerson)` See Section 3.3.2, "Limited Reconciliation" for more information.

3.4 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
Organization Lookup Reconciliation	This scheduled task is used for organization lookup field synchronization. See Section 3.2, "Scheduled Tasks for Lookup Field Synchronization" for information about this scheduled task.
Role Lookup Reconciliation	This scheduled task is used for role lookup field synchronization. See Section 3.2, "Scheduled Tasks for Lookup Field Synchronization" for information about this scheduled task.
Group Lookup Reconciliation	This scheduled task is used for group lookup field synchronization. See Section 3.2, "Scheduled Tasks for Lookup Field Synchronization" for information about this scheduled task.
OID User Trusted Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
OID User Target Recon Task	This scheduled task is used for user reconciliation when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
OID Trusted Delete Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.

Table 3–4 (Cont.) Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
OID Target Delete Recon Task	This scheduled task is used for reconciliation of deleted users when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
OID Group Recon Task	This scheduled task is used for reconciliation of groups from the target system. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
OID Role Recon Task	This scheduled task is used for reconciliation of roles from the target system. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.

To configure a scheduled task:

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.**
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 section, 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.
- Attributes of the scheduled task are discussed in Section 3.3.4, "Reconciliation Scheduled Tasks."

- 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.

3.5 Performing Provisioning Operations

This section discusses the following topics:

- Section 3.5.1, "Provisioning Users"
- Section 3.5.2, "Provisioning Organizational Units, Groups, and Roles"
- Section 3.5.3, "Enabling Provisioning of Users in Organizations and Organizational Units"

3.5.1 Provisioning Users

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create an Oracle Internet Directory 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 configure 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 procedure described in Section 3.6, "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 Fusion Middleware User's Guide for Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Section 3.5.1.1, "Direct Provisioning"
- Section 3.5.1.2, "Request-Based Provisioning"

3.5.1.1 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 9.1.0.*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 9.1.0.*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 Search list on the left pane.

Alternatively, in the Users region, click **Advanced Search - User,** provide a search criterion, and then click **Search.**

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 9.1.0.*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 **OID 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 OID 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 OID 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 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
- If you are using Oracle Identity Manager release 11.1.1, then:
  a. Close the window displaying the "Provisioning has been initiated" message.
  b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.1.2 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 3.5.1.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.5.1.2.2, "Approver's Role in Request-Based Provisioning"

3.5.1.2.1 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 **OID 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

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

3.5.1.2.2 Approver's Role in Request-Based Provisioning

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

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.

3.5.2 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 9.1.0.*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 9.1.0.*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 9.1.0.*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 9.1.0.*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 9.1.0.*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 AttrName.Group.Prov.Map.OID lookup definition are listed in the following table:

Code Key	Decode
Group Name	cn

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

     The default settings to enable provisioning of Roles in organizational units in the AttrName.Role.Prov.Map.OID lookup definition are listed in the following table:

Code Key	Decode
Role Name	cn

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 9.1.0.*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.

3.5.3 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 Lookup.OID.Configuration lookup definition, the following are default settings for enabling provisioning of users in organizational units:

- ldapOrgDNPrefix=ou
- ldapOrgUnitObjectClass=OrganizationalUnit

See Also: Appendix A, "Attribute Mappings Between Oracle Identity Manager and Oracle Internet Directory" for information about attribute mappings between Oracle Identity Manager and Oracle Internet Directory

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

Note: It is assumed that you have performed the procedure described in Section 2.3.1.8, "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 **OID 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 **OID 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 **OID 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 **OID User** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

4

Extending the Functionality of the Connector

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

4.1 Adding New Attributes for Target Resource Reconciliation

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

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

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

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

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

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

c. Search for and open the **OID User**.

d. Click **Create New Version**.

e. In the **Label** field, enter the version name. For example, `version#1`.

f. Click the **Save** icon.

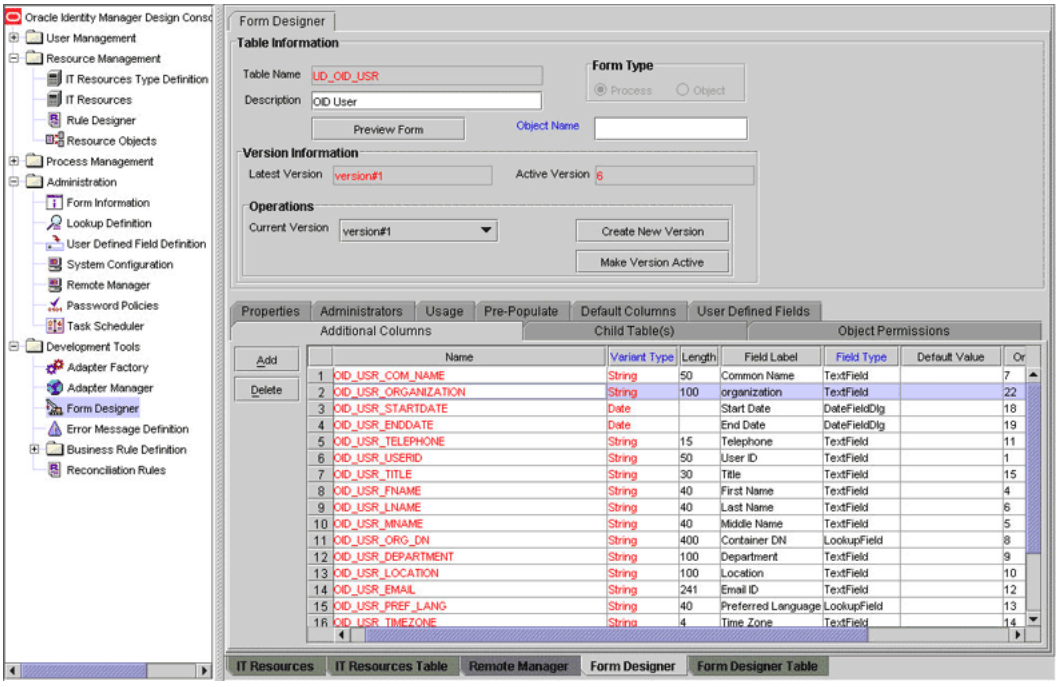
g. Select the current version created in Step e from the **Current Version** list.

h. Click **Add** to create a new attribute, and provide the values for that attribute.

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

Field	Value
Name	organization
Variant Type	String
Length	100
Field Label	organization
Order	20

The following screenshot shows this form:



i. Click the **Save** icon.

j. Click **Make Version Active**.

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

a. Expand **Resource Management.**

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

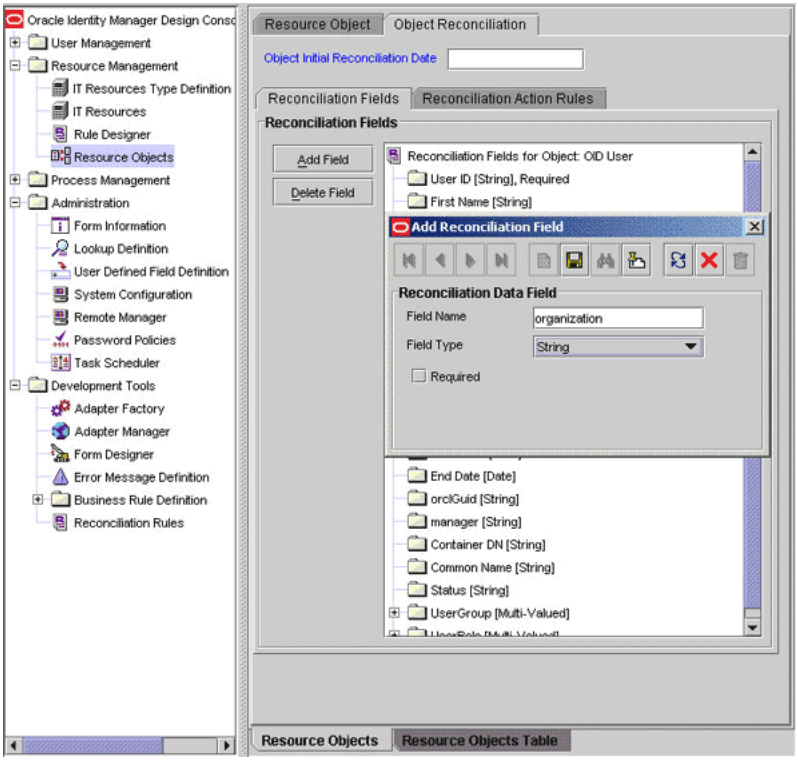
c. Search for and open the **OID User** resource object.

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

Field Name: `Organization`

Field Type: `String`

The following screenshot shows this form:



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

f. Click the **Save** icon.

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

a. Expand **Process Management.**

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

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

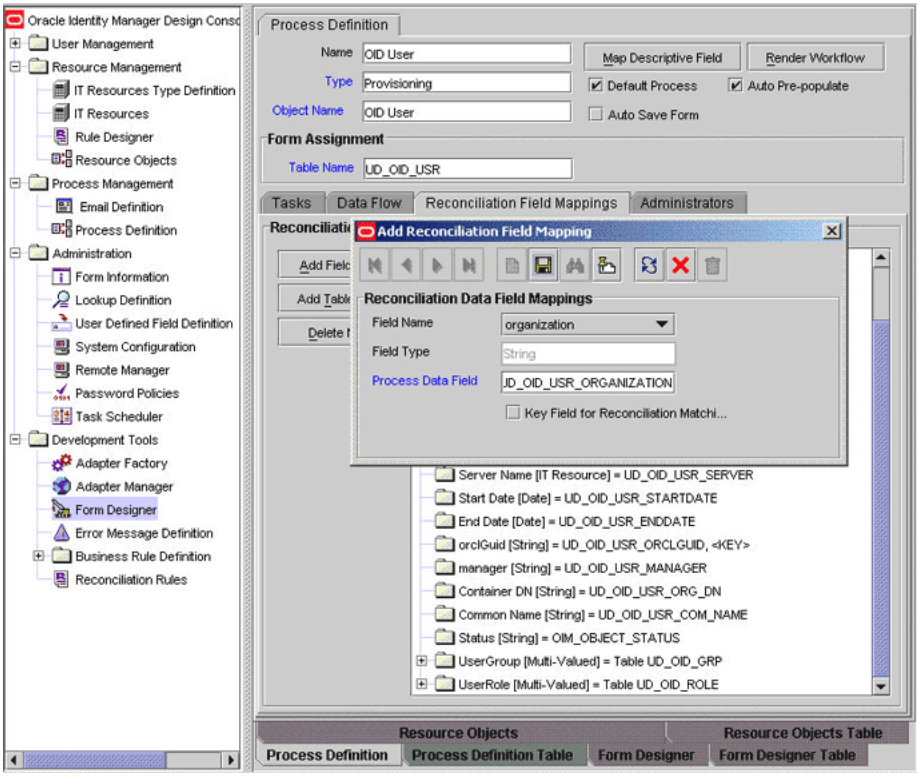
d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

Field Name: `Organization`

Field Type: `String`

Process Data Field: `Organization`

The following screenshot shows this form:



e. Click the **Save** icon.

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

   a. Expand **Administration**.

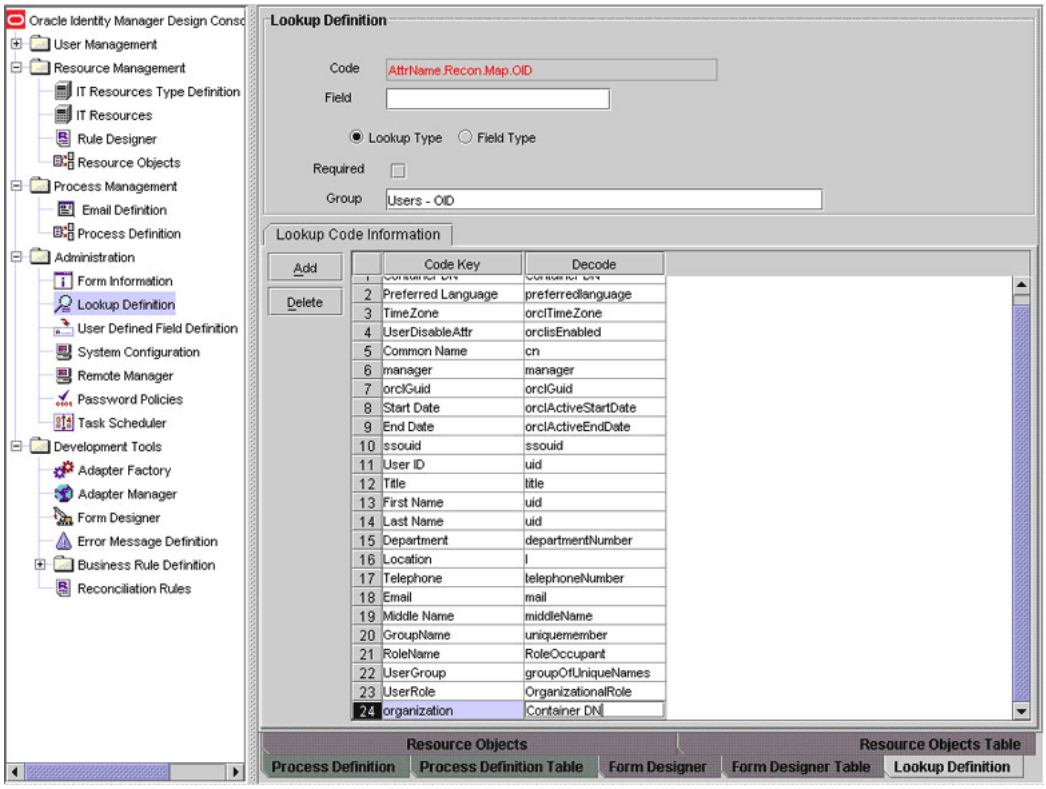
   b. Double-click **Lookup Definition**.

   c. Search for and open the **AttrName.Recon.Map.OID** lookup definition.

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

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

   The following screenshot shows this form:



e. Click the **Save** icon.

4.2 Adding New Multivalued Attributes for Target Resource Reconciliation

Note: This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for reconciliation. This procedure can be applied to add either user, group, or role attributes.

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, only the UserGroup and UserRole multivalued attributes (listed in Section 1.6.1, "User Attributes for Target Resource Reconciliation") are mapped for user reconciliation between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for target system reconciliation.

By default, no multivalued attributes are mapped for reconciliation between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation of groups or roles.

To add a new multivalued attribute for target resource reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.

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

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

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

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

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

a. Perform one of the following steps:

– For users, search for and open the **UD_OID_USR** process form.

– For groups, Search for and open the **UD_OID_GR** process form.

– For roles, search for and open the **UD_OID_RL** process form.

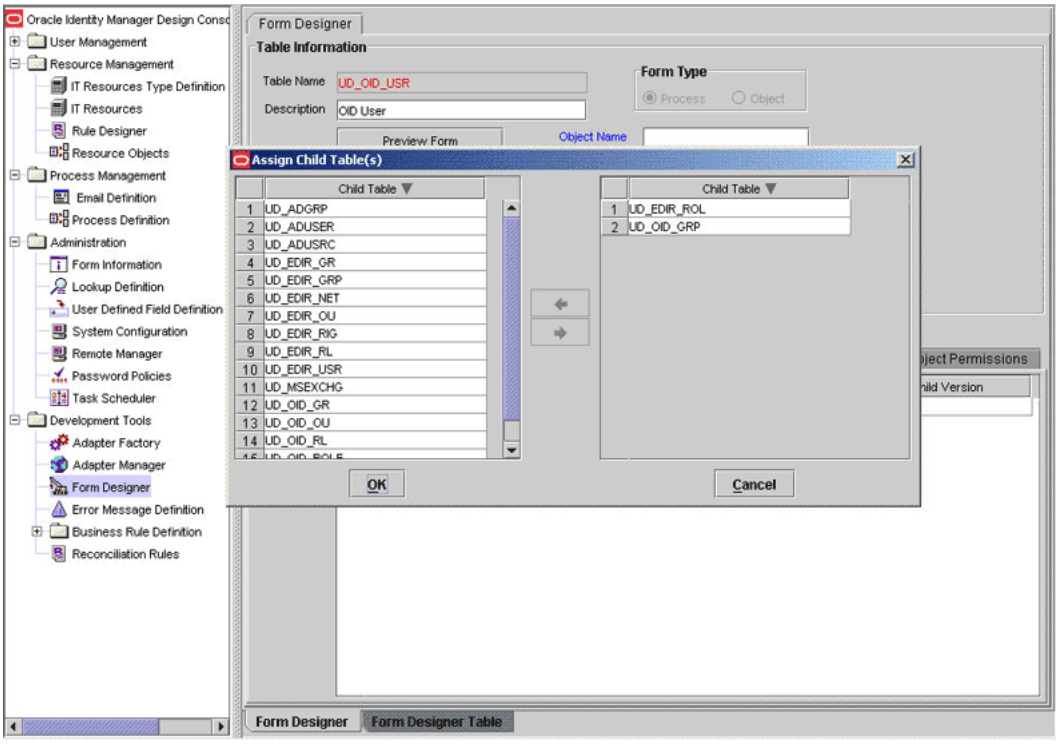
b. Click **Create New Version**.

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**.

The following screenshot shows this form:



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. Perform one of the following steps:

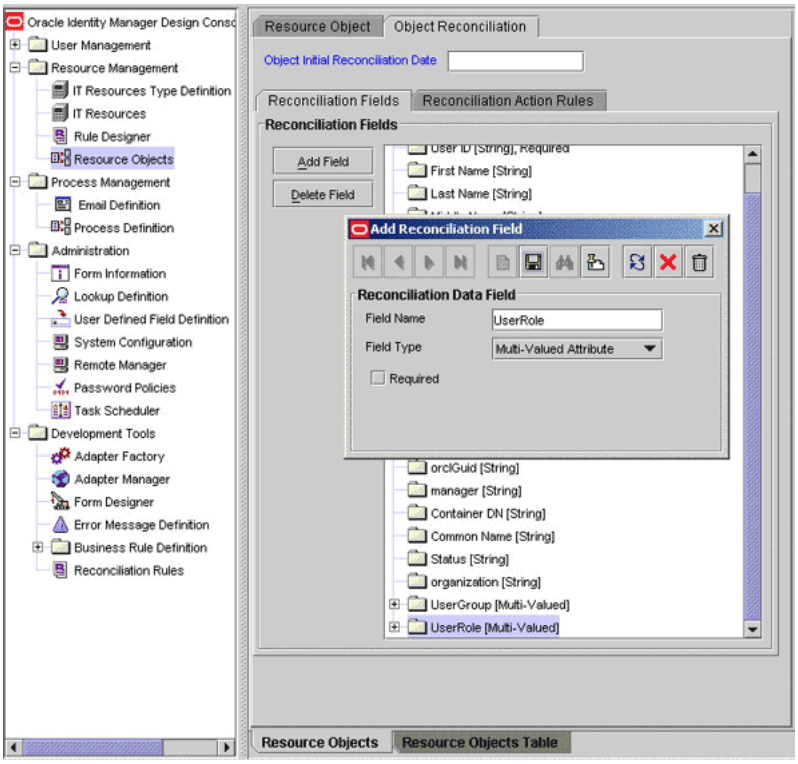
- For users, search for and open the **OID User** resource object.
- For groups, search for and open the **OID Group** resource object.
- For roles, search for and open the **OID Role** resource object.

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 `Address` in the **Field Name** field and select **Multi Valued Attribute** from the Field Type list.

The following screenshot shows this form:



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

g. Right-click the newly created attribute.

h. Select **Define Property Fields**.

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

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

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

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. Perform one of the following steps:

   – For users, search for and open the **OID User** process form.

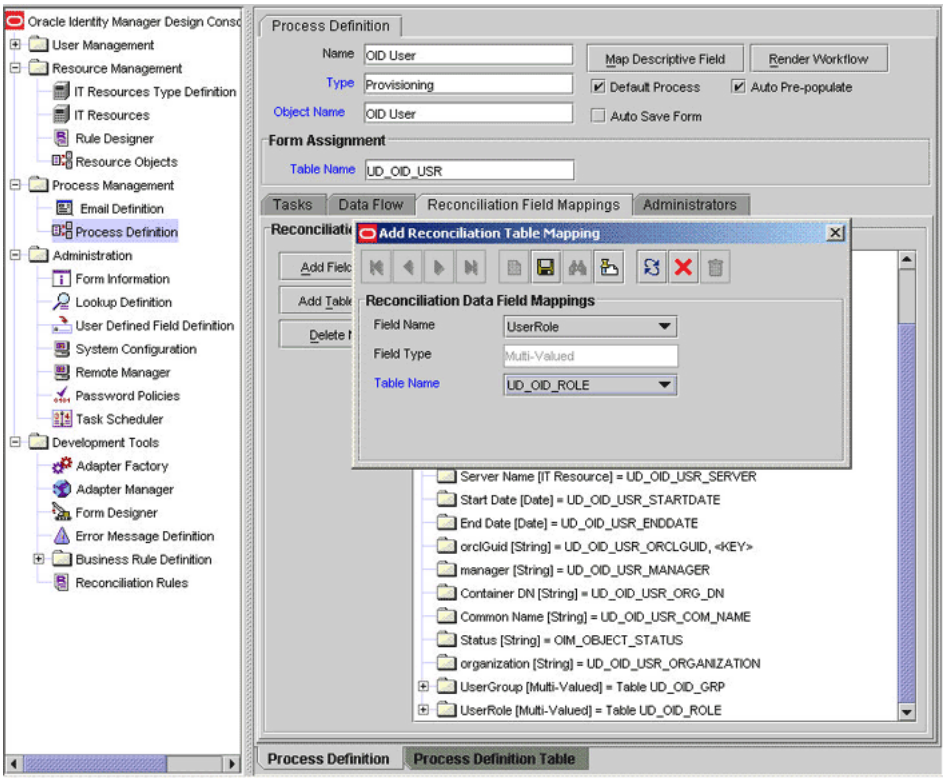
   – For groups, search for and open the **OID Group** process form.

   – For roles, search for and open the **OID Role** process form.

d. On the Reconciliation Field Mappings tab of the 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.

   The following screenshot shows this form:



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 the required data field.

i. Select the **Key Field for Reconciliation Mapping** check box, and then 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. For a user attribute, search for and open the **Lookup.OID.Configuration** lookup definition. Then, search for the `ldapUserMultiValAttr` Code Key value.

If you do not want to reconcile multivalued attributes, then accept the default Decode value `[NONE]`.

If you want to reconcile a multivalued attribute, then enter a value in the following format:

RECONCILIATION FIELD NAME OF ATTRIBUTE,PROPERTY NAME OF THE RECONCILIATION FIELD

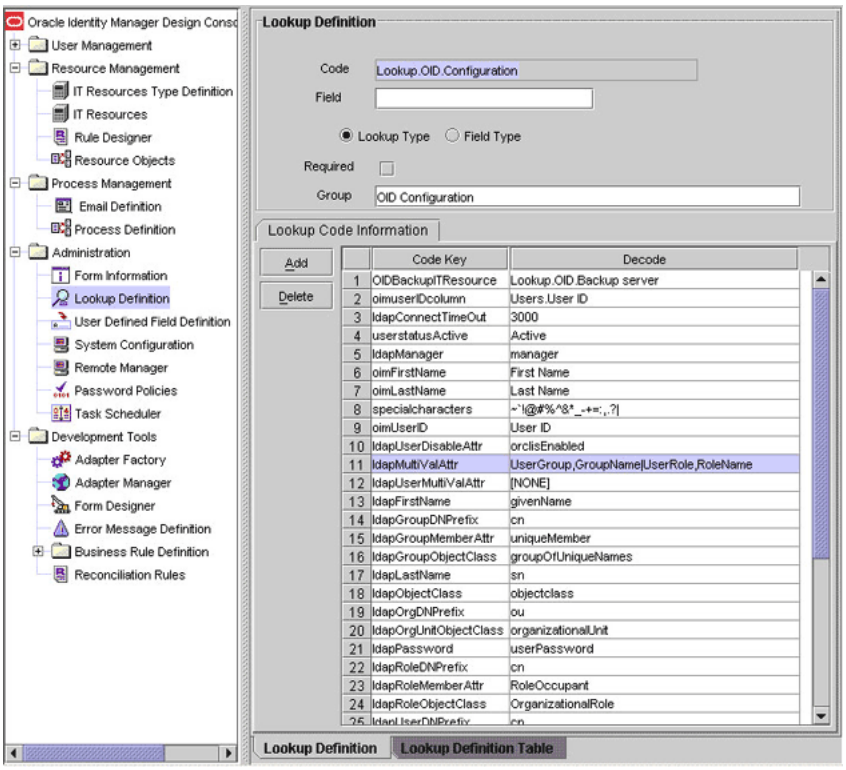
For example: `Address,MailingAddress`

If you want to reconcile more than one multivalued attribute, then enter values in the following format:

RECONCILIATION FIELD NAME OF ATTRIBUTE 1,PROPERTY NAME OF THE RECONCILIATION FIELD 1| RECONCILIATION FIELD NAME OF ATTRIBUTE 2,PROPERTY NAME OF THE RECONCILIATION FIELD 2| . . .

For example: `Address,MailingAddress|group,groupname`

The following screenshot shows this form:



d. Perform one of the following steps:

- For groups, search for and open the **Lookup.OIDGroupReconciliation.FieldMap** lookup definition.
- For roles, search for and open the **Lookup.OIDRoleReconciliation.FieldMap** lookup definition.

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

- Code Key: Enter the name of the attribute that you add on the process form.
- Decode Key: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

f. Perform one of the following steps:

   - For users, search for and open the **Attrname.Prov.Map.OID** lookup definition.
   - For groups, search for and open the **AttrName.Group.Prov.Map.OID** lookup definition.
   - For roles, search for and open the **AttrName.Role.Prov.Map.OID** lookup definition.

g. 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. The value that you enter must be in the same case (uppercase and lowercase) as the attribute name on the process form.
   - Decode Key: Enter the name of the attribute displayed on the target system, which you recorded earlier in this procedure.

If you have added new multivalued for groups or roles, then you must specify the decode key values of the newly added attributes as a value of the `Multivalue Attribute` attribute that is discussed in Section 3.3.4.2, "Scheduled Tasks for Group and Role Reconciliation."

4.3 Adding New Attributes for Reconciliation of Groups or Roles

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

By default, the attributes listed in Section 1.6.2, "Group Attributes for Target Resource Reconciliation" are mapped for group reconciliation between Oracle Identity Manager and the target system. Similarly, the attributes listed in the Section 1.6.3, "Role Attributes for Target Resource Reconciliation" are mapped for role reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for group or role reconciliation.

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 group or role reconciliation:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Expand **Development Tools.**
   b. Double-click **Form Designer.**
   c. Perform one of the following steps:
      - If you want to add new attributes for group reconciliation, then search for and open the **UD_OID_GR** form.
      - If you want to add new attributes for role reconciliation, then search for and open the **UD_OID_RL** form.

d. Click **Create New Version**.

e. In the **Label** field, enter the version name. For example, `version#1`.

f. Click the **Save** icon.

g. Select the current version created in Step e from the **Current Version** list.

h. Click **Add** to create a new attribute, and provide the values for that attribute.

i. Click the Save icon.

j. Click **Make Version Active**.

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

   a. Expand **Administration**.

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

   c. If you are adding new attributes for group reconciliation, then search for and open the **Lookup.OIDGroupReconciliation.FieldMap** lookup definition.

   d. If you are adding new attributes for role reconciliation, then search for and open the **Lookup.OIDRoleReconciliation.FieldMap** lookup definition.

   e. In the lookup definition, create an entry for the attribute that you want to add by clicking **Add,** and then enter the **Code Key** and **Decode** values for the attribute.

      The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name of the attribute in the target system.

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

   f. Click the **Save** icon.

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

   a. Expand **Resource Management.**

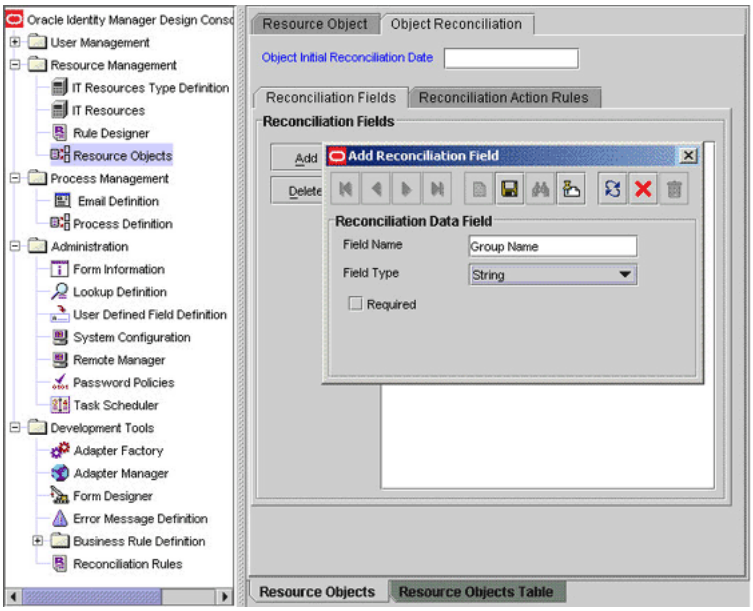
   b. Double-click **Resource Objects**.

   c. If you are adding a new attribute for group reconciliation, then search for and open the **OID Group** resource object.

   d. If you are adding a new attribute for role reconciliation, then search for and open the **OID Role** resource object

   e. On the **Object Reconciliation** tab, click **Add Field**, and then enter the appropriate values for the Field Name and Field Type fields.

      The following screenshot shows this dialog box:



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 the **Save** icon.

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

a. Expand **Process Management.**

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

c. If you are adding a new attribute for group reconciliation, then search for and open the **OID Group** process definition.

d. If you are adding a new attribute for group reconciliation, then search for and open the **OID Role** process definition.

e. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then specify the appropriate values for the **Field Name, Field Type,** and **Process Data Field** fields.

The following screenshot shows this dialog box:

f. Click the **Save** icon.

4.4 Adding New Attributes for Trusted Source Reconciliation

Note:

This section describes an optional procedure. Perform the procedure described in this section only if both the following conditions are true

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

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

To add a new attribute for trusted source reconciliation:

> **See Also:** One of the following guides for detailed information about these steps:
>
> - For Oracle Identity Manager release 9.1.0.*x: Oracle Identity Manager Design Console Guide*
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the Users process form as follows:
   - For Oracle Identity Manager releases prior to 11.1.1.5.4 (including release 9.1.0.*x*):
     a. Expand **Administration**.
     b. Double-click **User Defined Field Definition.**
     c. Search for and open the **Users** process form.
     d. Click **Add**.
     e. In the User Defined Fields dialog box, enter the details of the attribute.

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

        - In the **Label** field, enter `Employee ID`.

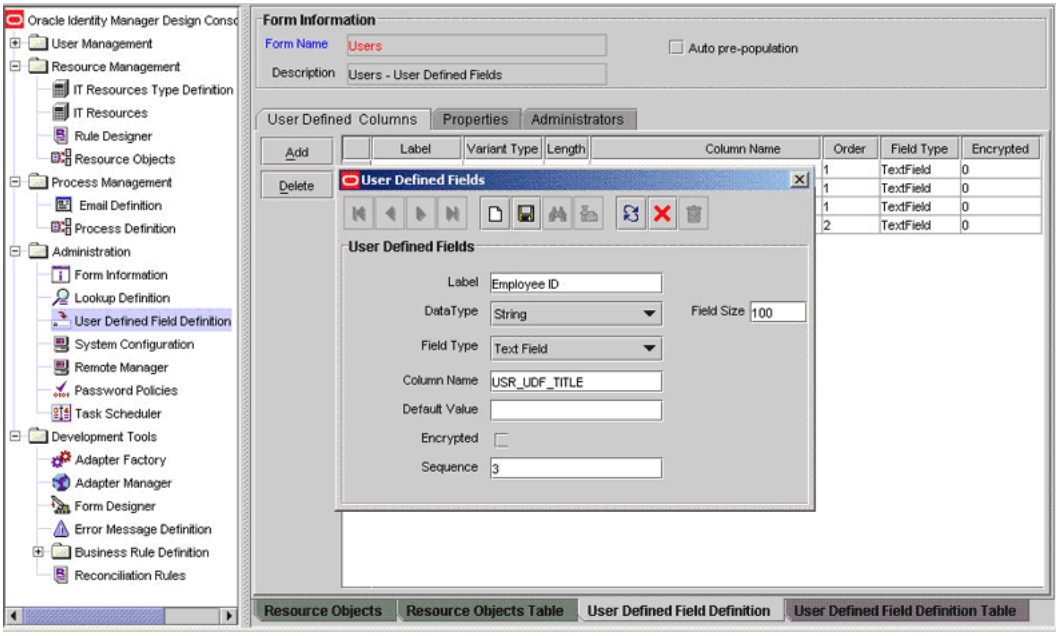
        - From the Data Type list, select **String**.

        - From the Field Type list, select **TextField**.

        - In the **Column Name** field, enter `USR_UDF_TITLE`.

        - In the **Field Size** field, enter `100` (for example).

        The following screenshot shows this form:



f. Click **Save.**

- For Oracle Identity Manager release 11.1.1.5.4 or later:

  See the "Configuring User Attributes" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager.*

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.

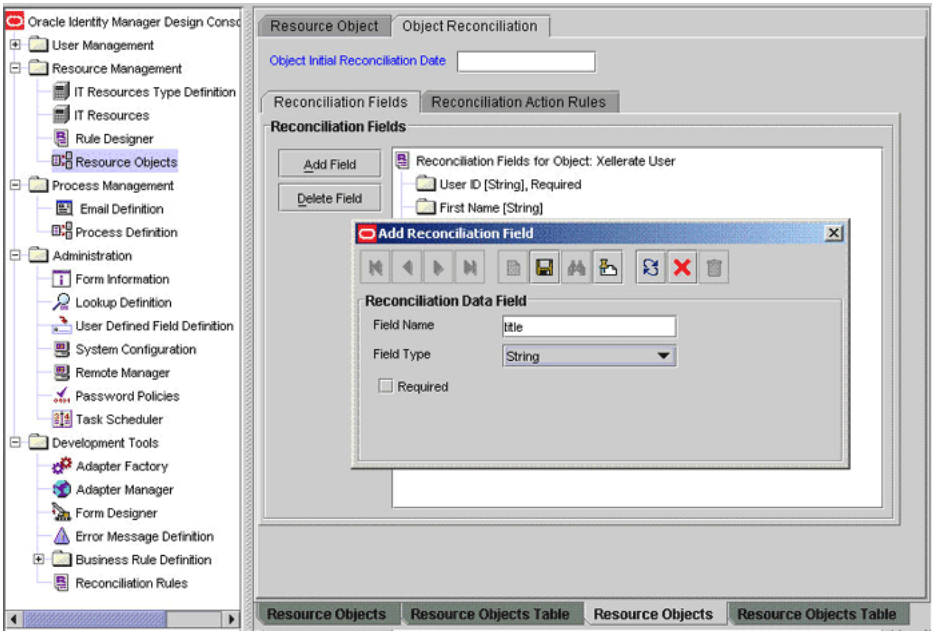
d. On the Object Reconciliation tab, click **Add Field**.

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.

The following screenshot shows the Add Reconciliation dialog box in which sample values have been entered:



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**.

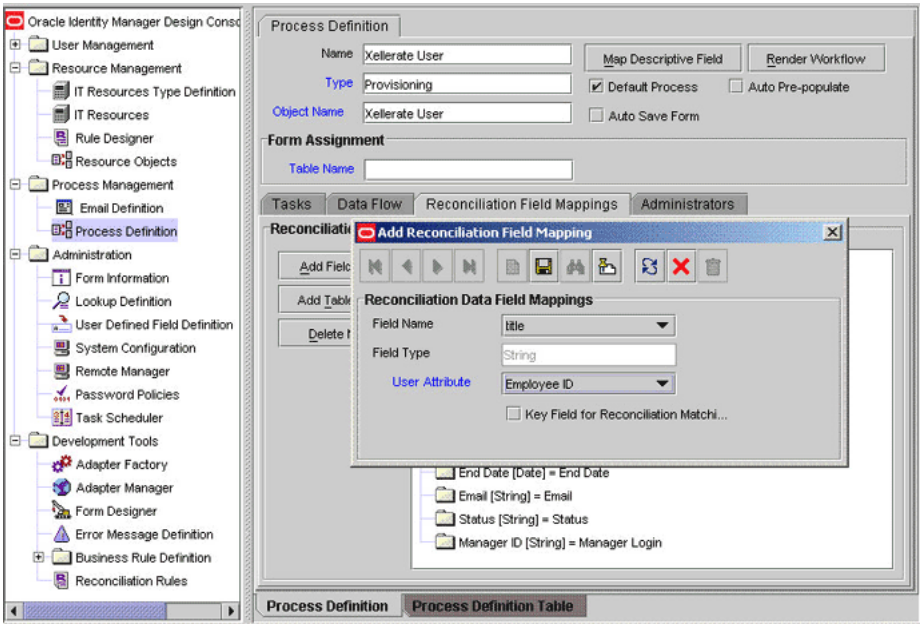
c. Search for and open the **Xellerate User** process definition.

d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**.

e. In the Field Name field, select the value for the attribute that you want to add.

For example, select `Title = Title`.

The following screenshot shows this form:



f. Click **Save**.

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

a. Expand **Administration**.

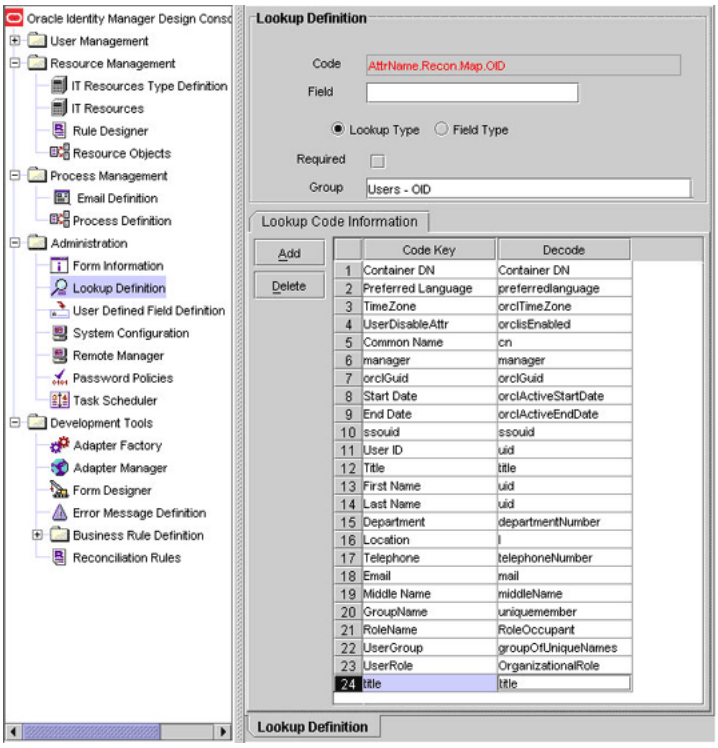
b. Double-click **Lookup Definition.**

c. Search for and open the **AttrName.Recon.Map.OID** 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.

The following screenshot shows this form:



e. Click **Save**.

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

4.5 Adding New Attributes for Provisioning Users

Note:

- This section describes an optional procedure. You need not perform this procedure if you do not want to add new user attributes for provisioning.
- Before starting the following procedure, perform Steps 1 and 2 as described in Section 4.1, "Adding New Attributes for Target Resource Reconciliation." If these steps have been performed while adding new attributes for target resource reconciliation, then you need not repeat the steps.

By default, the attributes listed in Section 1.8.2, "User Attributes for Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

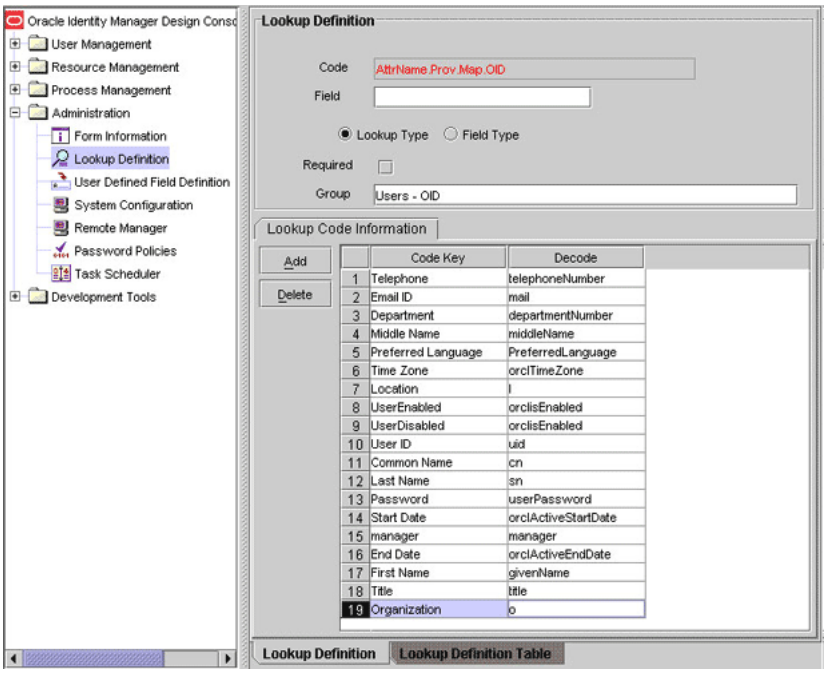
To add a new attribute for provisioning users, create an entry for the attribute in the lookup definition for provisioning as follows:

1. Expand **Administration.**
2. Double-click **Lookup Definition.**
3. Search for and open the **AttrName.Prov.Map.OID** lookup definition.
4. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The

Decode value is the name of the attribute in the target system. The value that you enter in the Code Key column must be in the same case (uppercase and lowercase) as the attribute name in the resource object.

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

The following screenshot shows this form:



5. Click the Save icon.

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, if you add organization as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "organization"
attr-ref = "organization"
type = "String"
```

```
widget = "text"
length = "100"
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 OID_USR_ORGANIZATION is the value in the Name column of the process form, then you must specify `organization` 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.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form.
- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute that you add.

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 2.3.1.8.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

4.5.1 Enabling Update of New Attributes for Provisioning Users

After you add an attribute for provisioning users, 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 attribute for provisioning a user:

1. Expand **Process Management.**

2. Double-click **Process Definition** and open the **OID User** process definition.

3. In the process definition, add a new task for updating the field as follows:

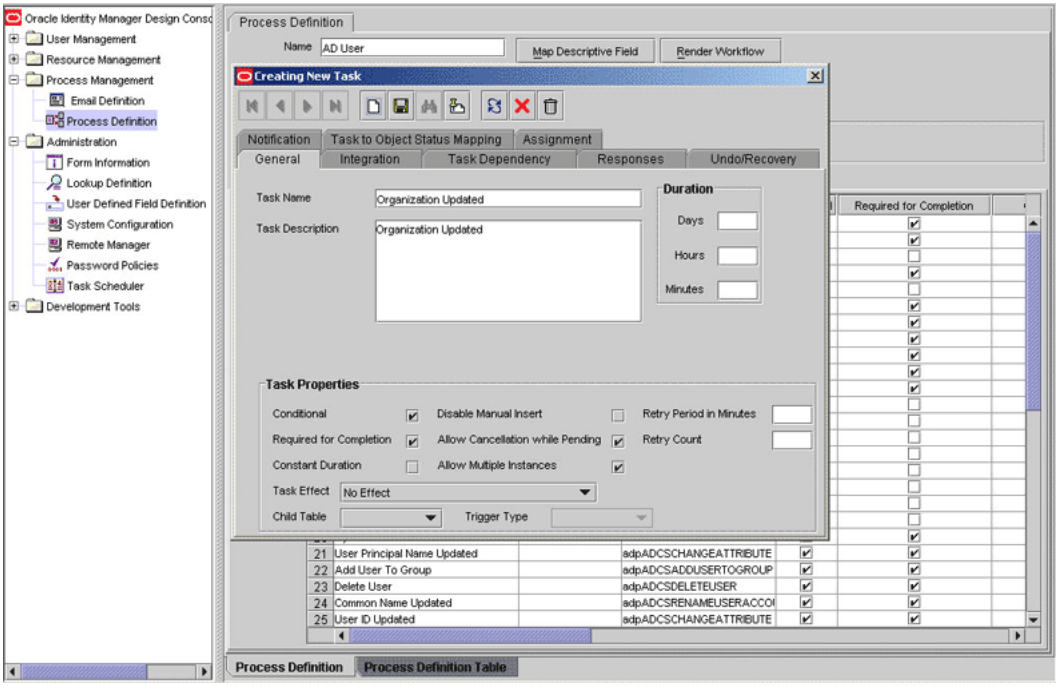
a. Click **Add** and enter the task name, for example, `organization Updated` and the task description.

b. In the Task Properties section, select the following fields:

- Conditional

- Required for Completion
- Allow Cancellation while Pending
- Allow Multiple Instances

The following screenshot shows this form:



c. Click on the Save icon.

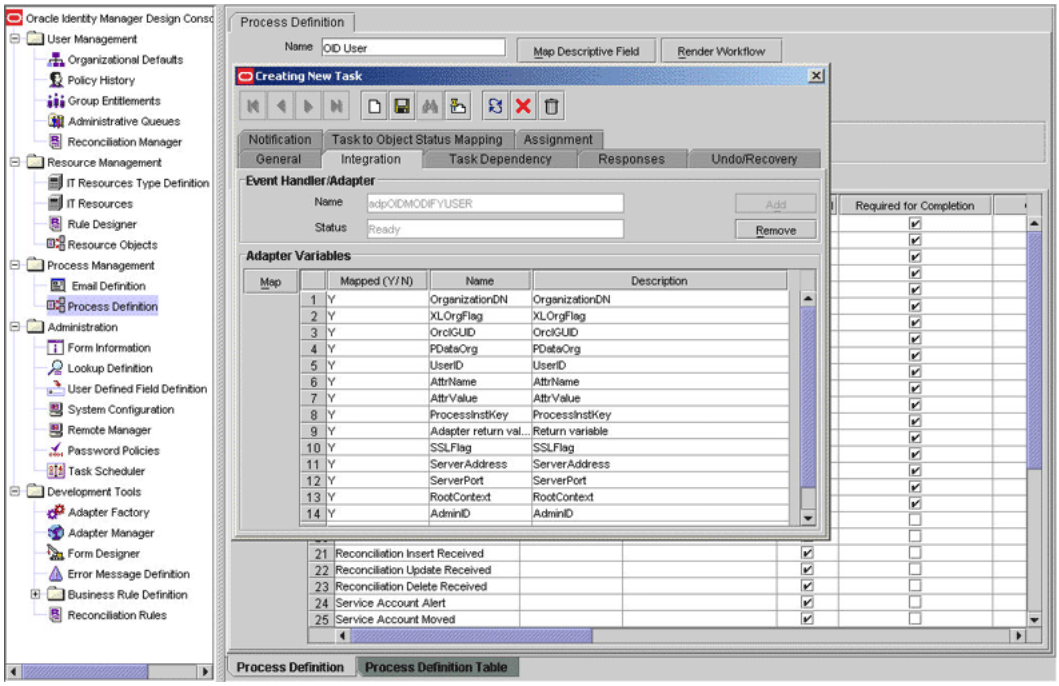
4. On the Integration tab, click **Add,** and then click **Adapter.**
5. Select the **adpOIDMODIFYUSER** adapter, click **Save,** and then click **OK** in the message that is displayed.
6. To map the adapter variables listed in this table, select the adapter, click **Map,** and then specify the data given in the following table:

Note: Some of the values in this table are specific to Organization (o value in OID target). These values must be replaced with values relevant to the attributes that you require.

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
PDataOrg	String	Process Data	Organization DN	NA	NA
User ID	String	Process Data	User ID	NA	NA
AttrName	String	Literal	String	Literal value :Organization	NA
AttrValue	String	Process Data	Organization Note: The name of the attribute in process form	NA	NA
ProcessInstKey	String	Process Data	Process Instance	NA	NA

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
Adapter return value	Object	Response Code	NA	NA	NA
SSL FLag	String	IT Resources	Server	OID Server	SSL
Server Address	String	IT Resources	Server	OID Server	Server Address
Server Port	String	IT Resources	Server	OID Server	Port
RootContext	String	IT Resources	Server	OID Server	Root DN
AdminID	String	IT Resources	Server	OID Server	Admin ID
AdminPwd	String	IT Resources	Server	OID Server	Admin Password
AttrLookupCode	String	IT Resources	Server	OID Server	Prov Attribute Lookup Code
OrganizationDN	String	Literal	String	Literal Value:Note: don't specify any value here	NA
XLOrgFlag	String	IT Resources	Server	OID Server	Use XL Org Structure

The following screenshot shows this form:



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

4.6 Adding New Attributes for Provisioning Groups or Roles

Note: This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning groups or roles.

By default, the attributes listed in Section 1.8.3, "Group Attributes for Provisioning" are mapped for provisioning of groups between Oracle Identity Manager and the target system. Similarly, by default, the attributes listed in Section 1.8.4, "Role Attributes for Provisioning" are mapped for provisioning of roles between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning groups or roles.

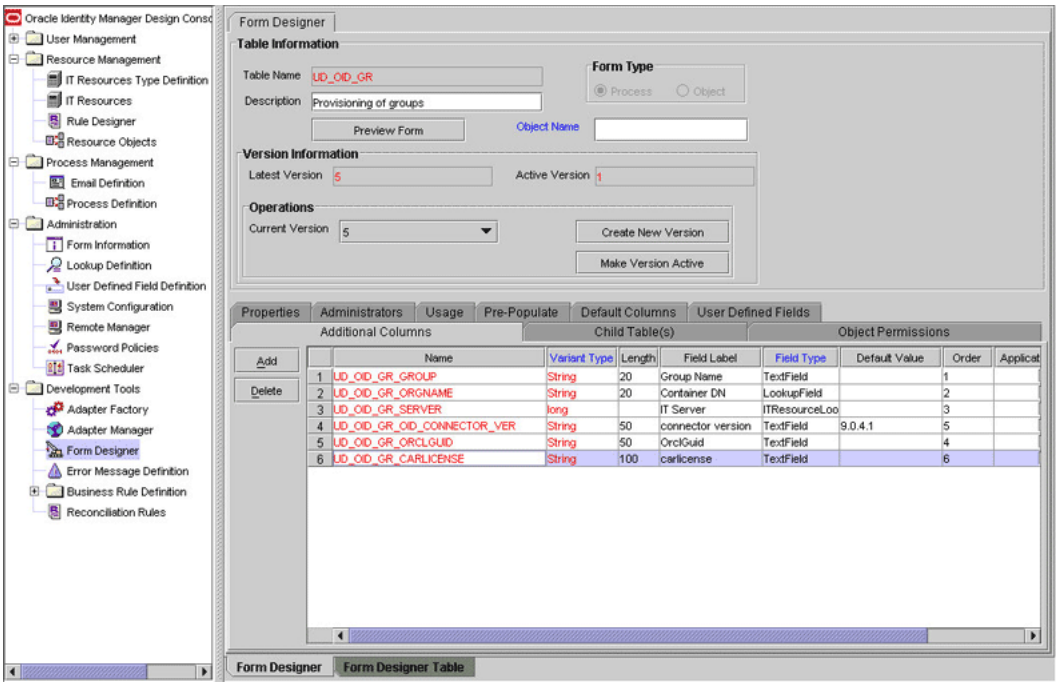
To add a new attribute for provisioning a group or role:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:
   a. Open the Form Designer form.
   b. Perform one of the following steps:

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

      Search for and open the **UD_OID_RL** form.
   c. Create a new version of the form.
   d. Add the new attribute on the form.

      The following screenshot shows this form:



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

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

   a. Open the Lookup Definition form.

   b. Do one of the following:

      – Search for and open the **AttrName.Group.Prov.Map.OID** lookup definition.

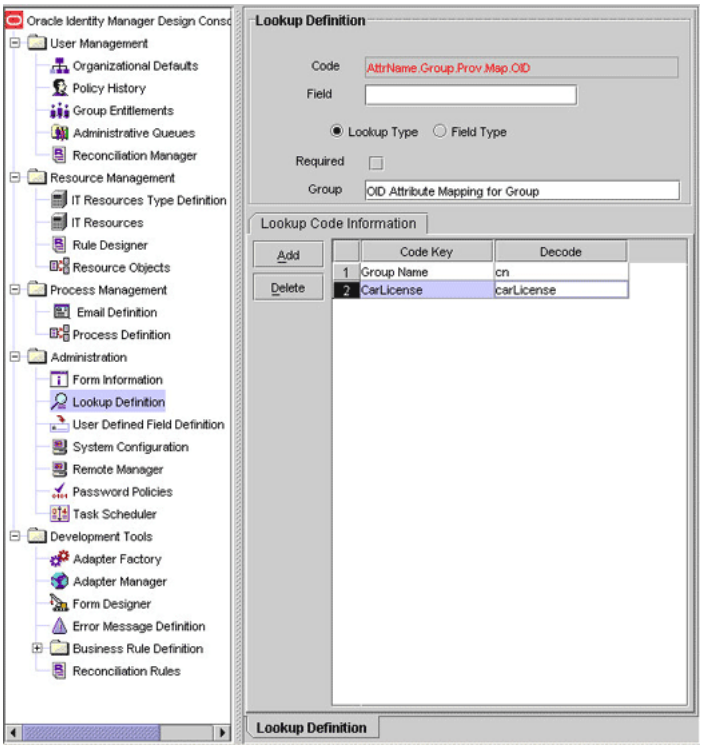
      – Search for and open the **AttrName.Role.Prov.Map.OID** lookup definition.

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

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

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

      The following screenshot shows this form:



Note: Perform steps 4 through 6 only if you want to perform request-based provisioning.

4. 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 2 of this procedure, if you added GroupDesc as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "GroupDesc"
attr-ref = "GroupDesc"
type = "String"
widget = "text"
length = "100"
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_OID_GR_GRPDESC is the value in the Name column of the process form, then you must specify `GroupDesc` 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 2.

- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.

- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 2.

- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.

- 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 2, 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.

5. 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.

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

See Section 2.3.1.8.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

7. 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.

4.6.1 Enabling Update of New Attributes for Provisioning Groups or Roles

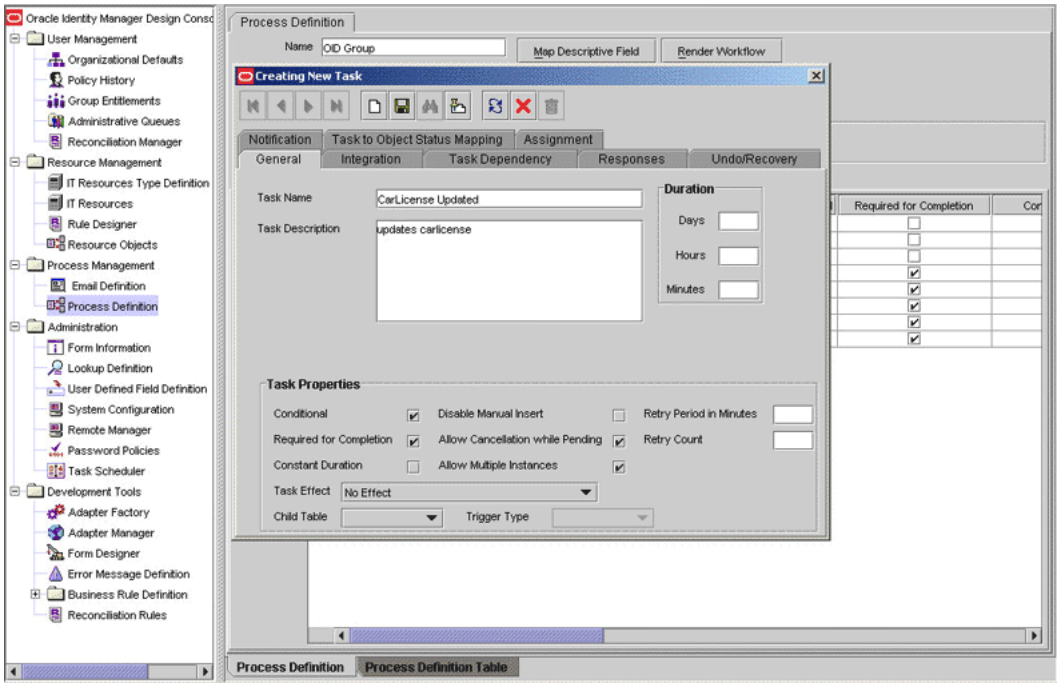
After you add an attribute for provisioning a Group or Role, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

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

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

        For the example described earlier, select **Mailing Address** from the list.

        The following screenshot shows this form:



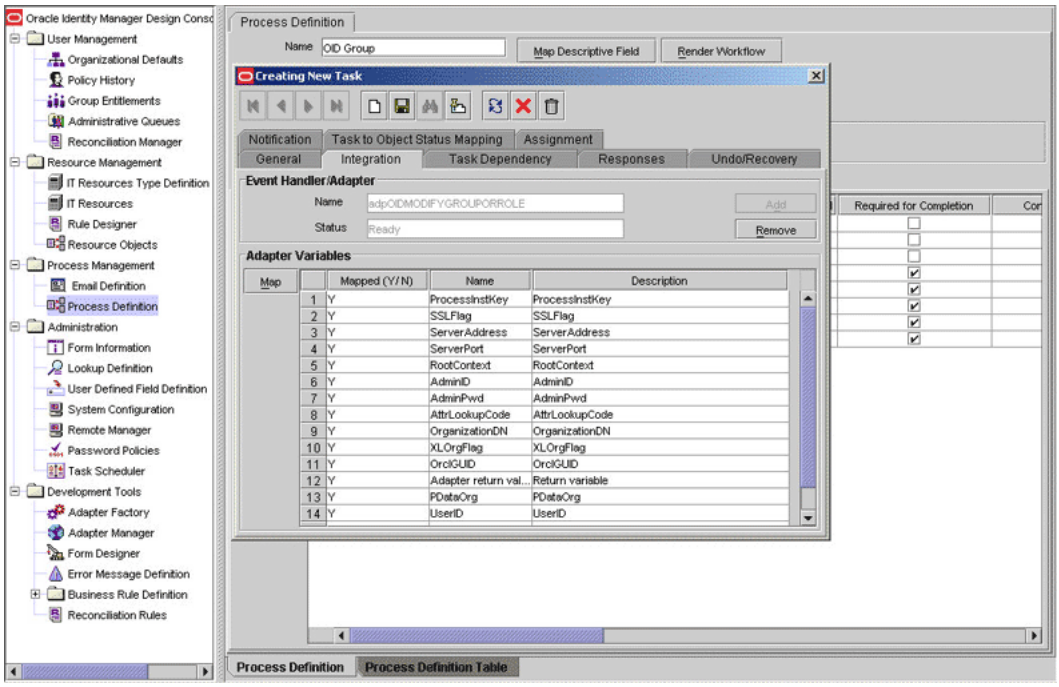
   c. On the **Integration** tab, click **Add**, and then click **Adapter**.

d. Select the **adpOIDMODIFYGROUPORROLE** 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
SSLFlag	String	IT Resource	Server	OID Server	SSL
Adapter return value	Object	Response Code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
userPassword	String	Process Data	Password	NA	NA
rootContext	String	IT Resources	Server	OID Server	Root DN
port	String	IT Resources	Server	OID Server	Port
LDAPServer	String	IT Resources	Server	OID Server	Server Address
AttrLookupCode	String	IT Resources	Server	OID Server	The value can be any one of the following: ■ For group: `AttrName.Group.Prov.Map.OID` ■ For Role: `AttrName.Role.Prov.Map.OID`
PropertyName	String	Literal	String	homePostalAddress **Note:** This is a sample (literal) value.	NA
PropertyValue	String	Select **Process Data** and then select (for example) **OID User Role**.	Address **Note:** This is a sample value.	NA	NA
Admin ID	String	IT Resources	Server	OID Server	Admin Id
AdminPwd	String	IT Resources	Server	OID Server	Admin Password
organizationDN	String	Literal	String	**Note:** Do not enter a value in the Literal field.	NA
ProcessInstKey	String	Process data	Process Instance	NA	NA
PDataOrg	String	Process data	Organization DN	NA	NA

The following screenshot shows this form:



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

4.7 Adding New Multivalued Attributes for Provisioning

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to add new multivalued fields for provisioning. This procedure can be applied to add either user, group, or role attributes.

By default, the user attributes Group and Role (listed in Section 1.8.2, "User Attributes for Provisioning") are the only multivalued attributes mapped for provisioning between Oracle Identity Manager and the target system. If required, you can add new multivalued attributes for provisioning users.

By default, no multivalued attributes are mapped for provisioning between Oracle Identity Manager and the target system for groups and roles. If required, you can add new multivalued attributes for reconciliation and provisioning of groups or roles.

To add a new multivalued attribute for provisioning:

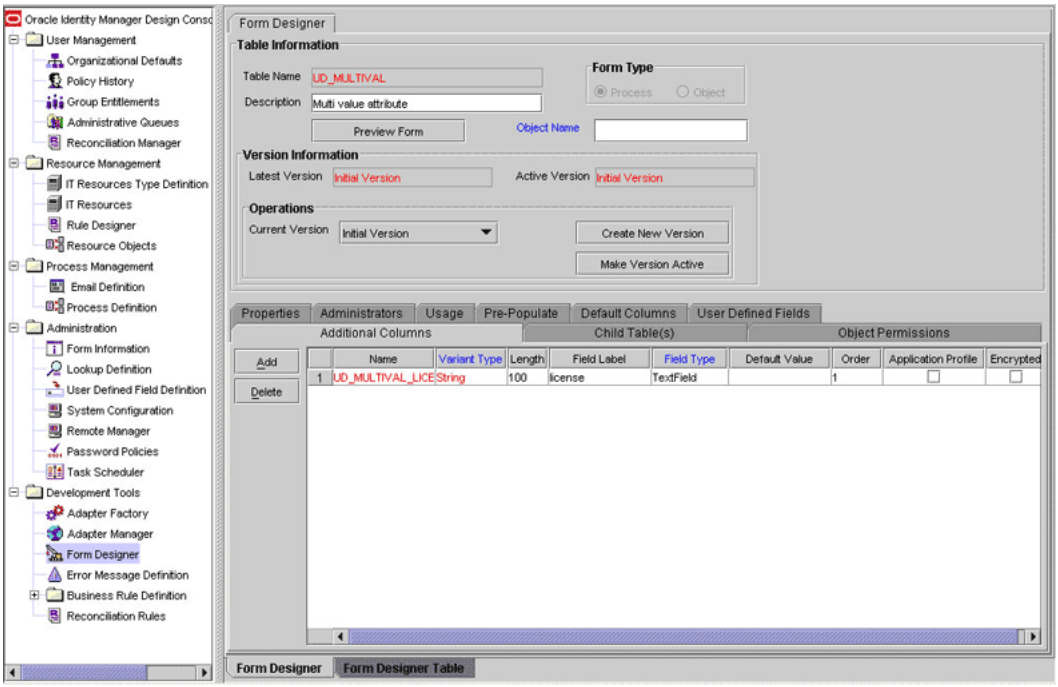
> **Note:** If you have already performed Steps 1 through 3 of the Section 4.2, "Adding New Multivalued Attributes for Target Resource Reconciliation," then you need not repeat the steps in the following procedure, and directly proceed to the Section 4.7.1, "Enabling Update of New Multivalued Attributes for Provisioning."

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued attribute as follows:
   a. Expand **Development Tools**.

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

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

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



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

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

a. Perform one of the following steps:

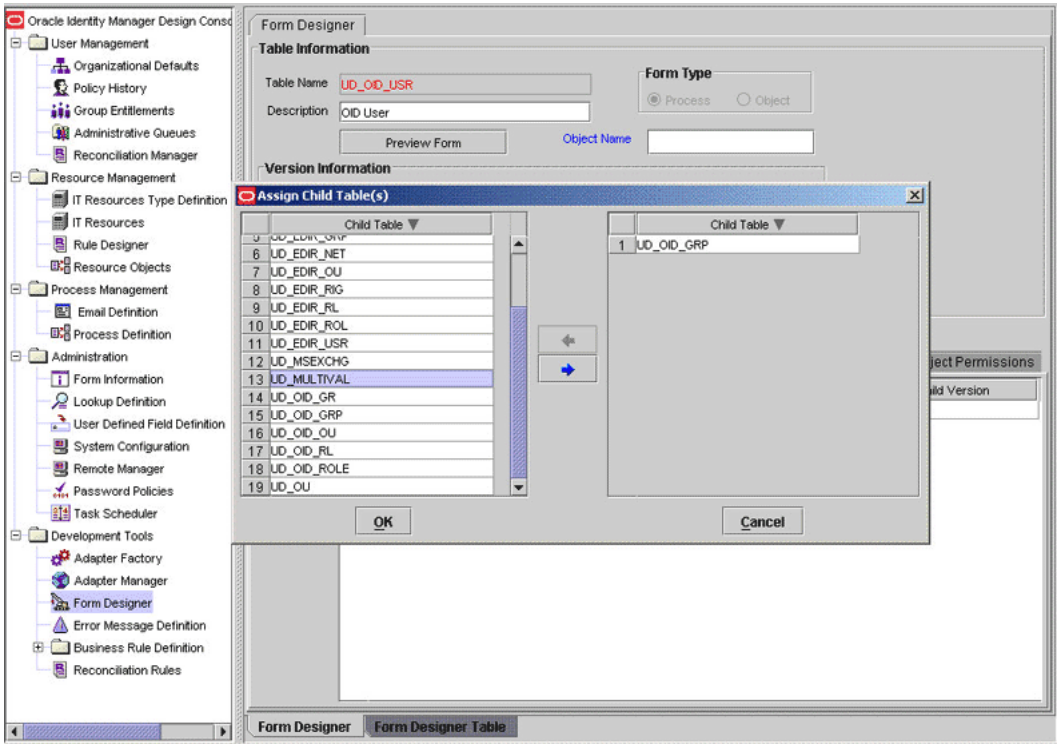
- For users, search for and open the **UD_OID_USR** process form.
- For groups, search for and open the **UD_OID_GR** process form.
- For roles, search for and open the **UD_OID_RL** process form.

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.**

Note: Perform steps 4 and 5 only if you want to perform request-based provisioning.

---

4. 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, if you added Address as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "Address"
attr-ref = "Address"
type = "String"
widget = "text"
length = "100"
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_MULTIVAL_ADDRESS is the value in the Name column of the process form, then you must specify `Address` 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.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form.
- For the length attribute, enter the value that you entered in the Length column of the process form.
- For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you add more than one attribute on the process form, then repeat this step for each attribute that you add.

c. Save and close the XML file.

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

See Section 2.3.1.8.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

4.7.1 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 provisioning operations.

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

> **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. Expand **Process Management**.

3. Double-click **Process Definition**, and then perform one of the following steps:

- For users, open the **OID User** process definition.
- For groups, open the **OID Group** process definition.
- For roles, open the **OID Role** process definition.

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

a. Click **Add**, enter the name of the task for adding multivalued attributes, and enter the task description.

b. In the Task Properties section, select the following fields:

- Conditional

- Required for Completion
- Allow Cancellation while Pending
- Allow Multiple Instances
- Select the child table from the list.

  For the example described earlier, select **Mailing Address** from the list.
- Select **Insert** as the trigger type for adding multivalued data. Alternatively, select **Delete** as the trigger type for removing multivalued data.

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

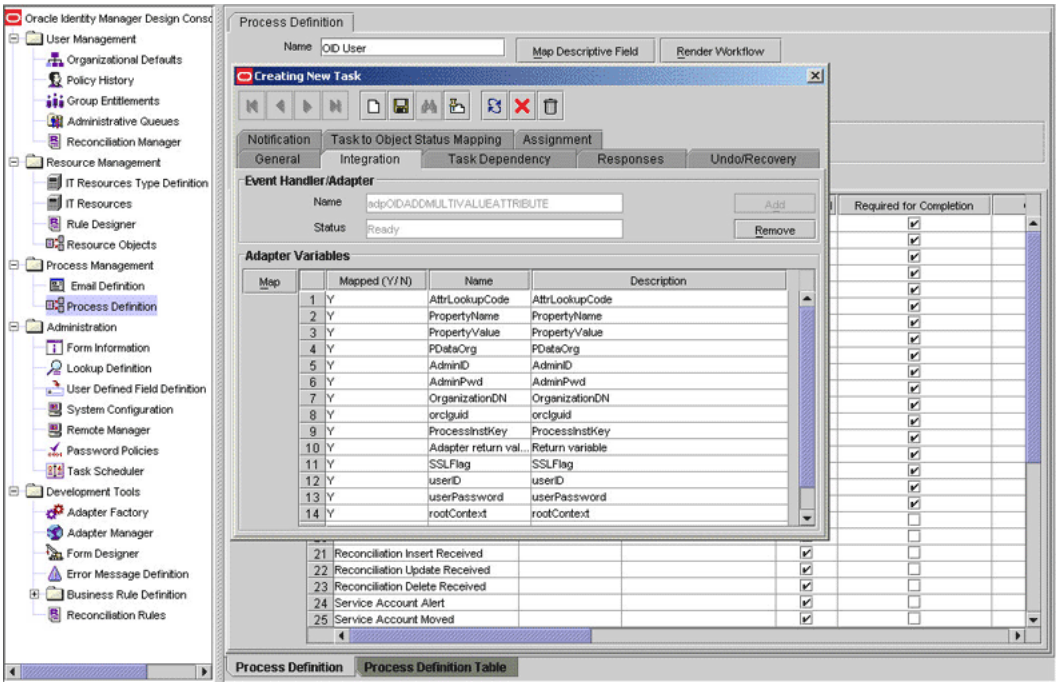
d. Select the **adpOIDADDMULTIVALUEATTRIBUTE** adapter, click **Save**, and then click **OK** in the message.

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
SSLFlag	String	IT Resource	Server	OID Server	SSL
Adapter return value	Object	Response Code	NA	NA	NA
UserID	String	Process Data	User ID	NA	NA
userPassword	String	Process Data	Password	NA	NA
rootContext	String	IT Resources	Server	OID Server	Root DN
port	String	IT Resources	Server	OID Server	Port
LDAPServer	String	IT Resources	Server	OID Server	Server Address
AttrLookupCode	String	IT Resources	Server	OID Server	Prov Attribute Lookup Code **Note:** While mapping for either group or role process definition, select the corresponding lookup definitions: ■ For group: `AttrName.Group.Prov.Map.OID` ■ For Role: `AttrName.Role.Prov.Map.OID`
PropertyName	String	Literal	String	homePostalAddress **Note:** This is a sample (literal) value.	NA

Variable Name	Data Type	Map To	Qualifier	IT Asset Type	IT Asset Property
PropertyValue	String	Select **Process Data** and then select (for example) **OID User Role**.	Address **Note:** This is a sample value.	NA	NA
Admin ID	String	IT Resources	Server	OID Server	Admin Id
AdminPwd	String	IT Resources	Server	OID Server	Admin Password
organizationDN	String	Literal	String	**Note:** Do not enter a value in the Literal field.	NA
ProcessInstKey	String	Process data	Process Instance	NA	NA
PDataOrg	String	Process data	Organization DN	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 **adpOIDREMOVEMULTIVALUEATTRIBUTE** adapter.

6. In the process definition, add a task for updating the value of the attribute by performing Step 4.

   While performing Step 4.d select the **adpOIDUPDATEMULTIVALUEATTRIBUTE** adapter. Map the Adapter return Value attribute for this update task by providing the values described in the preceding table.

4.8 Adding Custom Object Classes for Provisioning

Note: Perform the procedure described in this section only if you want to add custom object classes for provisioning organizational units, groups, or roles.

The `ldapUserObjectClassSecondary` field is one of the fields defined in the `Lookup.OID.Configuration` lookup definition.

By default, this field contains a value that you can change to the name of your object class. If required, you can modify the `ldapUserObjectClassSecondary` field and add more object classes. Use a vertical bar (`|`) to separate object classes whose names you enter. The following is a sample value that can be assigned to the `ldapUserObjectClassSecondary` field:

```
objclass1|objClass2
```

You must ensure that the attributes in the new object class are optional, and *not* mandatory attributes.

4.9 Adding New Object Classes for Provisioning and Reconciliation

To add a new object class for provisioning and reconciliation:

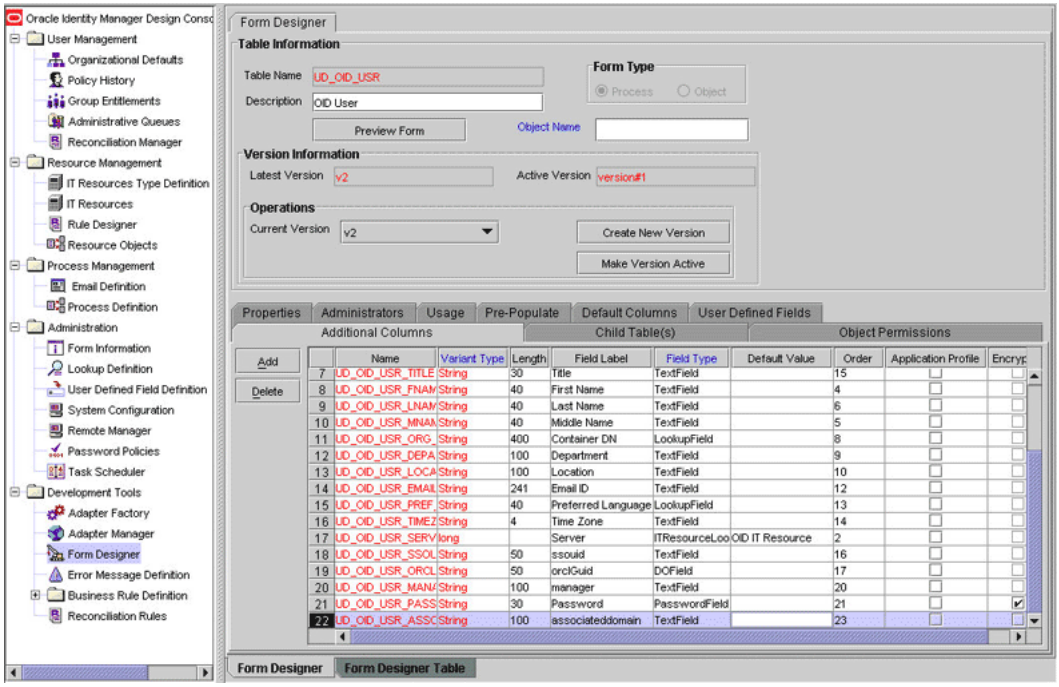
- Section 4.9.1, "Adding the Attributes of the Object Class to the Process Form"
- Section 4.9.2, "Adding the Object Class and its Attributes to the Lookup Definition for Provisioning"
- Section 4.9.3, "Adding the Attributes of the Object Class to the Resource Object"
- Section 4.9.4, "Adding Attributes of the Object Class to the Provisioning Process".

4.9.1 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_OID_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_OID_USR_ASSOCIATEDDOMAIN` in the **Name** field and then enter the other details of this attribute.



7. Click **Save,** and then click **Make Version Active.**

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

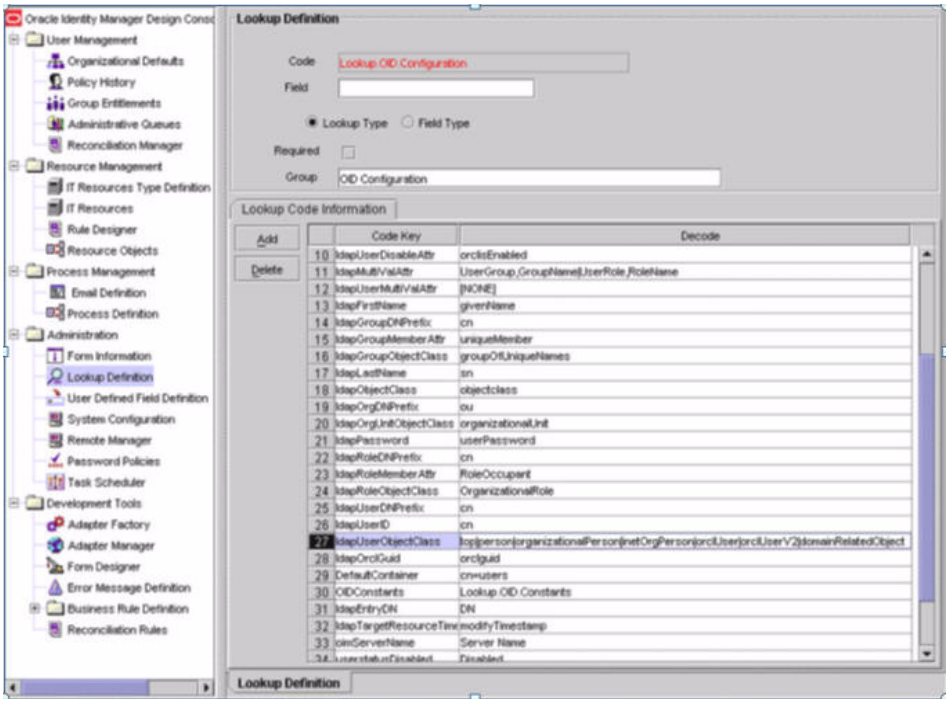
To add the object class and its attributes to the lookup definition for provisioning:

1. Expand the **Administration** folder.
2. Double-click **Lookup Definition.**
3. Search for and open the **Lookup.OID.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 `domainRelatedObject` in the Decode column then enter the value as follows:

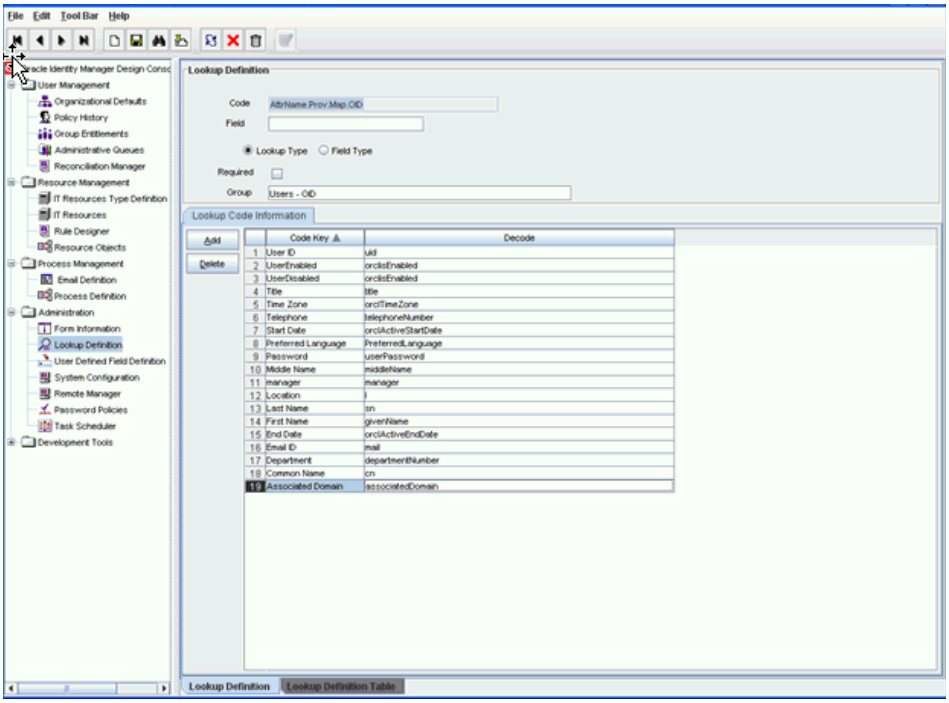
`top|person|organizationalPerson|inetOrgPerson|orclUser|orclUserV2|`**`domainRelated Object`**



5. Search for and open the **AttrName.Prov.Map.OID** 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.**

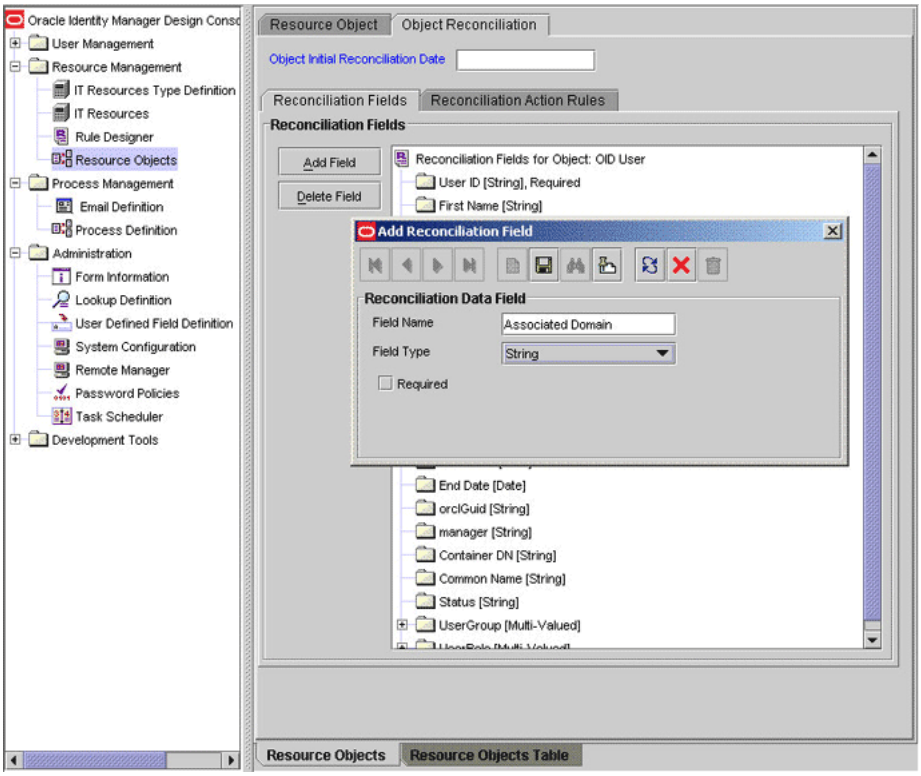
4.9.3 Adding the Attributes of the Object Class to the Resource Object

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 **OID 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.

4.9.4 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 **OID 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_OID_USR_ASSOCIATEDDOMAIN`
6. In the **Field Type** field, select the field type.
7. Click the save icon.

4.10 Configuring the Mapping of the User ID Field

Note: Perform this procedure only if you want to customize the mapping between the user ID fields of Oracle Internet Directory and Oracle Identity Manager.

While creating a user account on Oracle Internet Directory through Oracle Identity Manager, the user ID that you specify is assigned to the `uid` field of Oracle Internet Directory. If required, you can customize the mapping so that the user ID is assigned to the `cn` field of Oracle Internet Directory.

See Also: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about modifying lookup definitions

1. In the Design Console, open the AttrName.Prov.Map.OID lookup definition.
2. Change the decode value of the User ID code key to `cn`.
3. Save the changes.
4. In the Design Console, open the Lookup.OID.Configuration lookup definition.
5. Change the decode value of the ldapUserDNPrefix code key to `cn`. Do *not* change the case of `cn` to, for example, `CN`.
6. Save the changes.

Now, when you create a user account on Oracle Internet Directory through Oracle Identity Manager, the user ID assigned in Oracle Identity Manager will be assigned to the `cn` field of Oracle Internet Directory.

After you map for provisioning, the User ID field of Oracle Identity Manager to the `cn` field of the target system, you must customize the mapping for reconciliation. By default, during reconciliation, the uid field of Oracle Internet Directory is mapped to the User ID field of Oracle Identity Manager. To customize mapping so that the value in the `cn` field in Oracle Internet Directory is assigned to the User ID field in Oracle Identity Manager:

1. In the Design Console, open the AttrName.Recon.Map.OID lookup definition.
2. Change the decode value of the User ID code key to `cn`.
3. Save the changes.

5 Testing and Troubleshooting

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

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

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/troubleshoot 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 9.1.0.*x*:

     OIM_HOME/xellerate/test/troubleshoot

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/test/troubleshoot

2. Specify the required values in the config.properties file. This file is present in the following directory:

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

     OIM_HOME/xellerate/test/troubleshoot

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/test/troubleshoot

   The following table describes the sections of this file in which you must provide information for running the tests.

Section	Information
Oracle Internet Directory Connection Parameters	Connection parameters required to connect to the target system The values that you provide are the same as those provided for the IT resources parameters. The procedure to configure the IT resource is described earlier in this guide.
Create User Information	Values required to create a user
Modify User Information	Values 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 OIDProv.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. Depending on the Oracle Identity Manager version you are using, add one of the following to the CLASSPATH environment variable:
   - For Oracle Identity Manager release 9.1.0.*x*:

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

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/jars/OIDProv.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/client/oimclient.jar
     OIM_HOME/server/jars/OIDRecon.jar
     OIM_HOME/designconsole/ext/spring.jar
     OIM_HOME/designconsole/ext/commons-logging.jar
5. In the following files, set the value of the DXL.HomeDir attribute to the directory in which the Design Console is installed:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME\xellerate\test\troubleshoot\scripts\testcreate.bat

     OIM_HOME\xellerate\test\troubleshoot\scripts\testmodify.bat

     OIM_HOME\xellerate\test\troubleshoot\scripts\testdelete.bat

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME\server\test\troubleshoot\scripts\testcreate.bat

     OIM_HOME\server\test\troubleshoot\scripts\testmodify.bat

     OIM_HOME\server\test\troubleshoot\scripts\testdelete.bat
6. Perform the following tests:

Note: When you run a BAT file to perform the corresponding test, the global.properties file is automatically created in the same directory. You can view log details in the Troubleshoot.log file, which is created in the same directory when you run the tests.

- Create a user by running the testcreate.bat file.

  After you run the BAT file, check if the user is created in Oracle Internet Directory with the details given in the config.properties file. If you run the BAT file from a command window, then the `User_Creation_Successful` message is displayed.

- Modify the user by running the testmodify.bat file.

  After you run the BAT file, check if the user is modified in Oracle Internet Directory with the details given in the config.properties file. If you run the BAT file from a command window, the `User_Modification_Successful` message is displayed.

- Delete the user by running the testdelete.bat file.

  After you run the BAT file, check if the, specified user is deleted from Oracle Internet Directory. If you run the BAT file from a command window, the `User_Deletion_Successful` message is displayed.

5.2 Troubleshooting

This section provides instructions for identifying and resolving 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, "Delete User Errors"
- Section 5.2.4, "Modify User Errors"
- Section 5.2.5, "Child Data Errors"

5.2.1 Connection Errors

The following table provides solutions to some commonly encountered connection errors.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with Oracle Internet Directory. **Returned Error Message:** Connection error encountered **Returned Error Code:** `INVALID_CONNECTION_ERROR`	▪ Ensure that Oracle Internet Directory is running. ▪ Ensure that Oracle Identity Manager is running. ▪ Ensure that all the adapters have been compiled. ▪ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the 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 Oracle Internet Directory is running. ▪ Ensure that the specified Oracle Internet Directory connection values are correct.

Problem Description	Solution
Authentication error **Returned Error Message:** Invalid or incorrect administrator password **Returned Error Code:** AUTHENTICATION_ERROR	Ensure that the specified Oracle Internet Directory connection password is correct.

5.2.2 Create User Errors

The following table provides solutions to some commonly encountered Create User errors.

Problem Description	Solution
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.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Required information missing **Returned Error Code**: INSUFFICIENT_INFORMATION_PROVIDED	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_EXISTS	A user with the specified ID already exists in Oracle Internet Directory. Assign a new ID to the 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 user container value already exists in Oracle Internet Directory.
Oracle Identity Manager cannot create a user. **Returned Error Message:** Could not create user **Returned Error Code:** USER_CREATION_FAILED	The user cannot be created because one or more attribute values violate the schema definition. Check if the Oracle Internet Directory schema is correctly defined and contains all the object classes defined in the lookup definition.

5.2.3 Delete User Errors

The following table provides solutions to some commonly encountered Delete User errors.

Problem Description	Solution
Oracle Identity Manager cannot delete a user. **Returned Error Message:** Required information missing **Returned Error Code:** `INSUFFICIENT_INFORMATION_PROVIDED`	Ensure that the following information is provided: ■ User Container ■ User ID
Oracle Identity Manager cannot delete a user. **Returned Error Message:** User does not exist **Returned Error Code**: `USER_DOESNOT_EXIST`	The specified user ID does not exist in Oracle Internet Directory.

5.2.4 Modify User Errors

The following table provides solutions to some commonly encountered Modify User errors.

Problem Description	Solution
The Modify User operation failed because a value was being added to a nonexistent attribute. **Returned Error Message:** Attribute does not exist **Returned Error Code:** `ATTRIBUTE_DOESNOT_EXIST`	1. From the corresponding process task, get the value passed for `AttrName` of the connector. 2. Using the name obtained in the previous step, check in the `AttrName.Recon.Map.OID` lookup definition if the decode value is a valid attribute name in the target.
Oracle Identity Manager cannot modify an attribute of a user. **Returned Error Message:** Invalid attribute value or state **Returned Error Code:** `INVALID_ATTR_MODIFY_ERROR`	The attribute ID and value specified may be wrong. Check the specified values.
The Modify User operation failed because a value was being added to an attribute that does not exist in the `AttrName.Prov.Map.OID` 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 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.Prov.Map.OID` lookup definition.
Oracle Identity Manager cannot update information about a user. **Returned Error Message:** Could not update user **Returned Error Code**: `USER_UPDATE_FAILED`	Generic error. Review the log for more details.

Problem Description	Solution
Oracle Identity Manager cannot move a user from one container to another. **Returned Error Message:** Could not move user **Returned Error Code:** USER_MOVE_FAILED	Generic error. Review the log for more details.

5.2.5 Child Data Errors

The following table provides solutions to some commonly encountered Child Data errors.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Group does not exist **Returned Error Code:** GROUP_DOESNOT_EXIST	The specified user security group does not exist in Oracle Internet Directory. Check the group name.
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 does not exist in Oracle Internet Directory. Check the role name.
The operation failed because a duplicate value was being added to an attribute. **Returned Error Message:** Duplicate value encountered **Returned Error Code:** DUPLICATE_VALUE_ERROR	The user has already been added to the specified group or role.
Oracle Identity Manager cannot add a user to a group. **Returned Error Message:** Could not add user to group **Returned Error Code:** ADD_USER_TO_GROUP_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot remove a user from a group. **Returned Error Message:** Could not remove user from group **Returned Error Code:** REMOVE_USER_FROM_GROUP_FAILED	Generic error. Review the log for more details.

Problem Description	Solution
Oracle Identity Manager cannot add a user to a role. **Returned Error Message:** Add user to Role failed **Returned Error Code:** ADD_USER_TO_ROLE_FAILED	Generic error. Review the log for more details.
Oracle Identity Manager cannot remove a user from a role. **Returned Error Message:** Removing assigned role failed **Returned Error Code:** REMOVE_ROLE_FROM_USER_FAILED	Generic error. Review the log for more details.

6

Known Issues

This chapter lists and describes known issues associated with this release of the connector.

- **Bug 9799541**

  Reconciliation of group data and role data is not supported.

- **Bug 10229448**

  User groups are not getting reconciled during OID user target reconciliation.

A

Attribute Mappings Between Oracle Identity Manager and Oracle Internet Directory

The following table discusses attribute mappings between Oracle Identity Manager and Oracle Internet Directory:

Note: Apply the following guideline while performing provisioning operations:

Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you 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.

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
User ID	cn	Login ID
First Name	givenname	First name
Last Name	sn	Last name or surname
Organizational Unit	o	Organization to which the user belongs
Email	mail	E-mail address
ldapUserDisableAttr	orclisEnabled	This attribute specifies whether or not the user account is locked. If the value is `DISABLED`, then it means that the account is locked. If the value is `ENABLED`, then it means that the account is not locked.
ldapOrgDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapUserDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)

Oracle Identity Manager Attribute	Oracle Internet Directory attribute	Description
ldapUserUniqueAttr	cn	Common name of an entry (for example, organization, user, role, and group)
Middle Name	middleName	Middle name
ldapUserObjectClass	inetOrgPerson	Object class for the user (primary)
GroupName	uniquemember	Multivalued attribute for the group object, which shows the number of users in the group
RoleName	RoleOccupant	Multivalued attribute for the role object, which shows the number of users in the role
UserGroup	groupOfUniqueNames	Object class for the group
UserRole	OrganizationalRole	Object class for the role
ldapUserDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapObjectClass	objectclass	Object class
ldapGroupDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
Title	title	Designation
Location	l	City of office address
Telephone	telephoneNumber	Office telephone number
Department	departmentNumber	Department name
Preferred Language	PreferredLanguage	Preferred language for communication
ldapPassword	userPassword	Password
Time Zone	orclTimeZone	Time zone
ldapRoleDNPrefix	cn	Common name of an entry (for example, organization, user, role, and group)
ldapRoleMemberAttr	RoleOccupant	Custom object class for the role Section 4.8, "Adding Custom Object Classes for Provisioning" provides information about how to add a custom object class.
ldapUserObjectClassSecondary	orclUserV2	Object class for the user (secondary)
ldapOrgDNPrefix	cn	Common name of an entry (for example, organization, user, role, and Group)

Index

M

O

P

R

S

T

U

V

X