Oracle® Identity Manager

Administrative and User Console Guide

Release 9.1.0.2

E14765-02

August 2009

ORACLE®

Oracle Identity Manager Administrative and User Console Guide, Release 9.1.0.2

E14765-02

Primary Author: Lyju Vadassery

Contributing Author: Debapriya Datta

Contributor: Javed Beg

Contents

List of Figures

List of Tables

Preface

This guide describes the procedures that you can perform by using the Oracle Identity Manager Administrative and User Console.

Audience

This guide is intended for database administrators, system administrators, and developers, and end users of Oracle Identity Manager.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For more information, see the other documents in the Oracle Identity Manager documentation set for this release.

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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

Part I

General Features

Part I is divided into the following chapters:

1

Introduction to the Administrative and User Console

Oracle Identity Manager is an advanced, flexible provisioning system for automatically granting and revoking access to enterprise applications and managed systems. You use Oracle Identity Manager to provide access to enterprise resources to staff and partners, and to enforce access policies that are associated with these resources.

Oracle Identity Manager enables you to do the following:

- View your Oracle Identity Manager user account information such as group memberships and e-mail address.
- Modify your profile.
- Review the resources that you have permission to access.
- View requests that you made and requests made for you.
- Make requests for additional resources for yourself.
- Change your password.
- View and modify login challenge questions and answers.
- Set up your user proxy.
- View and manage your pending requests, if you are the authorized approver.

In addition, depending on your permissions in Oracle Identity Manager, you may also be able to do the following:

- Update passwords and user IDs for accounts on resources that you have been allocated (provisioned).
- Create requests for resources for any users you manage.
- Complete draft requests for resources for any users you manage.
- Approve the provisioning of resources for other users.
- Respond to requests for more information.

Oracle Identity Manager provides the Administrative and User Console to create requests for resources and approve the provisioning of resources of the users that you manage. Users can search for, edit, and delete account information in the Oracle Identity Manager database by using the Administrative and User Console.

The rest of this guide describes the actions you can perform in Oracle Identity Manager by using the Administrative and User Console. This chapter discusses the following topics:

Note: Not all functions are available to all users. The features you can view and use in Oracle Identity Manager depend on the permissions that you are assigned.

If you are the system administrator for the Oracle Identity Manager system, read Appendix A, "System Configuration Considerations for Administrators" in this guide before running your product in a production environment.

See Also:

- *Oracle Identity Manager Administrative and User Console Customization Guide* for information about customizing Oracle Identity Manager Administrative and User Console
- *Oracle Identity Manager Globalization Guide* for information about globalizing Oracle Identity Manager Administrative and User Console

1.1 Understanding User Roles and Capabilities

Table 1–1 lists important user roles associated with Oracle Identity Manager.

Table 1–1 User Roles

Role	Description
Administrator	A person who manages users, organizations, user groups, resources, and policies.
Approver	A person who approves and denies access to resources.
End user	A person who uses self-service features of Oracle Identity Manager and who is not an administrator.

1.2 Overview of the Resource Model

Oracle Identity Manager allows resources to be requested and allocated (provisioned) to enterprise users. The resource can be an application, access to a database, rights to a directory structure on a network, or other entities to which access is vital. The manner in which access to the resource is granted and the permissions given to a user on that resource are governed by provisioning processes that you define. Access to a resource may be provisioned uniformly for all users. Alternatively, access may be provisioned in a unique fashion, based on variables such as the following:

- Your role, for example, "administrator" and "accountant"
- Your location
- Your employment status, for example, "full time" and "consultant"
- Your group or department designation
- Other criteria that are deemed relevant by the resource-specific and Oracle Identity Manager administrators

Once a resource is successfully provisioned to you, you can access that resource without further interaction with Oracle Identity Manager. For example, if you request access to a Microsoft Exchange application and that resource is successfully provisioned to you, then you can log in to that application by using the user ID and password provided by Oracle Identity Manager.

Oracle Identity Manager controls the provisioning of resources by using processes and tasks that comprise them. It also uses a specific kind of process, called an approval process, to govern the approvals that must be obtained before the provisioning of a resource may occur. Oracle Identity Manager has two different types of resource-related processes: approval processes and provisioning processes.

1.2.1 Approval Processes

An **approval process** determines whether or not a resource is to be approved for provisioning to one or more users or organizations for whom it is requested. Approval processes consist of a series of tasks that require responses from the users responsible for approving the provisioning of the resource. Because these responses are manually provided, these are assigned to an approver or a group of approvers.

Approvers can act upon all tasks in an approval process that are assigned to them. If an approver is assigned to a task in a request, then the approver can view all tasks in the request. If you are an approver for a request, the request ID is displayed when you click **Pending Approvals** under the **To-Do List** menu in the Administrative and User Console.

Note: Approval processes are optional. As an Oracle Identity Manager administrator, you can configure some resources to be provisioned without requiring approval. In this case, access to the resource is granted as soon as the request is submitted.

1.2.2 Provisioning Processes

A provisioning process is the process used to allocate (provision) the resource to one or more users or organizations for whom it is requested. Provisioning processes consist of a series of automated tasks that perform the steps necessary to grant access to a given resource. The provisioning process cannot be initiated until the approval process is complete, except in cases where an approval process has not been defined for the resource. The provisioning process can also use a special form to prompt users for, and capture, data required to grant access to a resource.

Oracle Identity Manager's exception capabilities allow you to handle problems that may occur during the provisioning process. For example, you can add business logic to a provisioning process that prevents the transaction from stopping or failing if a resource is unavailable. Oracle Identity Manager also includes a state engine that allows the system to roll back to the last known consistent state in the event that a provisioning transaction fails. The state engine also rolls back the system to its original state if a provisioning request is rejected.

2

Self-Registration Using the Administrative and User Console

In Oracle Identity Manager, user accounts are created in two ways. As an administrator, you can create an account in the Administrative and User Console for a user. A user can also self-register in the Administrative and User Console to create an account.

This chapter describes how to create an account in Oracle Identity Manager, and how to log in and out of Oracle Identity Manager by using that account.

This chapter discusses the following topics:

2.1 Creating Oracle Identity Manager Accounts

In Oracle Identity Manager, a user ID cannot include the following characters:

; # / % = | +, \ " < >

Depending on how the system is configured, users might want to contact their managers to have them create an account for the users.

Also, depending on how your system is configured, requests for self-registration may require approvals. If approvals are not required, your account is created and available for use as soon as Oracle Identity Manager has processed your self-registration request. If your system administrator has set Oracle Identity Manager to require approvals for self-registration requests, you can track the status of that request. When the required approvals are obtained, your account is ready for use.

Note: If approval is required for your request, then record the request ID after submitting your request. You need the request ID to track the status of your request.

To create an account by self-registering:

1. Access your corporate portal link to the Administrative and User Console. The Oracle Identity Manager Welcome page is displayed.

2. Under the Self-Register menu item in the left navigation pane, click **Create Request**. The User Self-Registration page is displayed.
3. Enter the information required to create the user account.

   Required information is marked with an asterisk (*). Ensure that you select and specify answers to password challenge questions if your system requires them. Depending on how Oracle Identity Manager is configured, you might be required to specify answers to challenge questions to reset your password.

   Note: During self-registration, the password policy attached to the Default rule is applied. If no password policy is attached to the Default rule, then the password specified during self-registration would not be evaluated against any password policy. See "Adding a Password Policy Rule to a Resource Object" in *Oracle Identity Manager Design Console Guide* for more information.

4. Click **Submit Request**.

   Oracle Identity Manager informs you that the request has been submitted and displays the numeric ID of the request so that you can track it. Record the request ID after submitting your request. You need the request ID to track the status of your request.

   A link to the request is displayed.
5. If your request requires an approval, then click **Track Request** under the Self-Register menu in the left navigation pane. The Track Self-Registration request page is displayed. You can check the status of your request on this page by entering the request ID.

2.2 Changing Passwords

If you forget your Oracle Identity Manager password, then you can contact your system administrator to have your account unlocked or you can reset your password from a page where you are prompted to answer challenge questions. If you provide the correct answers to these questions, Oracle Identity Manager lets you change your password.

You can also reset your password if your Oracle Identity Manager account had been locked after logon retry attempts exceed the maximum number of attempts allowed. However, if you exceed the maximum number of attempts to correctly answer your challenge questions, then your account is locked and can be unlocked only by an Oracle Identity Manager system administrator.

Note: If you have forgotten your Oracle Identity Manager user ID, then contact your Oracle Identity Manager system administrator.

If a password policy is attached to the Xellerate User resource object, then the View Password Policy link is displayed on all pages of the Administrative and User Console in which a password field is present, except for the Create User and User Self-Registration pages. Clicking this link shows the password policy that is applicable for specifying a password.

To reset a password:

1. Log in to the Administrative and User Console.
2. On the left navigation pane, click **Forgot Password**.
3. On the Verify User Id page, enter your user ID in the **User ID** field, and then click **OK**.
4. On the Change Password page, answer the challenge questions.

   These questions and the answers that you set are part of your account options. You select these questions and answers the first time you log in to the Oracle Identity Manager Administrative and User Console.

   a. Provide the correct answers to the password challenge questions.

   b. Enter your new password in both of the password fields.
5. Click **Submit**.

2.3 Tracking Self-Registration Requests

Depending on how Oracle Identity Manager has been configured, requests for self-registration may require approval. If approvals are required, you can track the status of that approval and self-registration process.

To track the status of a self-registration request:

1. Access your corporate portal link to the Administrative and User Console. The Welcome page is displayed.
2. In the left navigation pane, click **Track Request** under Self-Register. The Track Self-Registration Request page is displayed.
3. Enter the ID of the request associated with your self-registration in the **Request ID** field.
4. Click **Track Request**. The details about the self-registration request status are displayed.

2.4 Logging In to the Administrative and User Console

Before logging in to the Administrative and User Console, ensure that you have an account in that application. If you do not currently have an account, create an account as described in "Creating Oracle Identity Manager Accounts" on page 2-1, or contact your manager to have an account created for you.

To log in to the Administrative and User Console:

1. Access your corporate portal's URL to the Administrative and User Console.
2. Enter your user ID and password.
3. Click **Login**.

2.5 Logging Out of the Administrative and User Console

You may be automatically logged out of the Administrative and User Console after a specific period of time because of inactivity in the console. You can also log out if you are not working in a single sign-on environment.

To log out of the Administrative and User Console when you are not in a single sign-on environment:

1. Click **Logout**. A confirmation message is displayed.
2. Click **Logout** or **Cancel**.

3

Using the Administrative and User Console

This chapter describes how to use the main features of the Administrative and User Console. It discusses the following topics:

- Searching in the Administrative and User Console
- Customizing the Display of Data in the Administrative and User Console

3.1 Searching in the Administrative and User Console

Many fields in the Administrative and User Console pages have lookup capabilities. You use these capabilities to locate a record, for example, to find a particular user account, to assign a particular entity to a record, or to add users to requests. Some fields have predefined menu choices. Other fields provide full search capabilities, also referred to as a query function.

This section discusses the following topics:

- Constructing a Search (or Query)
- Using Wildcards
- Understanding How Search Works

3.1.1 Constructing a Search (or Query)

To search for a particular record, you can enter information in one or more fields and click **Search**. Enter as much information as possible about the record you are trying to locate. For example, if you remember a user's first name only, enter that and leave the other fields blank. All user records that have the same first name as the one you entered are displayed.

In a search page, if you leave all the fields blank and click **Search**, then all the records are displayed. To restart a search, click **Clear**. Some pages also provide a **Cancel** button that you can click to cancel a search.

Note: Searches in the Administrative and User Console are not case-sensitive. For example, you can enter `JOHN` or `john` to search for a user named `John`.

3.1.2 Using Wildcards

In addition to entering values in the fields to limit the records retrieved by the search, you can enter wildcard characters in a particular search field. The wildcard characters help further refine the search.

The asterisk (*) wildcard character represents unspecified portions of field values in a search. You can use the asterisk at the beginning, middle, or end of a value that you enter in a field. For example, if you enter `j*` in the **User ID** field and perform a search, all users whose user ID begins with the letter `j`, such as `John` and `Jane`, are displayed. If the asterisk is placed in the middle of a search value, as in `j*n`, then all records that begin with `j` and end with `n`, for example, `john` and `joan`, are displayed. If you place the asterisk at the beginning of the search value, as in `*d`, then all records that end with the letter `d`, such as `Richard`, are displayed.

Note: You cannot include wildcard characters when you specify search criteria for a user-defined field (UDF) of a numeric type. In this context, numeric types include INTEGER, LONG, DOUBLE, and so on.

3.1.3 Understanding How Search Works

The manner in which the search is constructed and run depends on the type of search you perform. The results you retrieve are based on the context in which you are conducting the search.

If you search for a user record when creating or tracking a request, only the user records are displayed for whom you are the manager or administrator. The search parameters you enter are combined to retrieve results. For example, if you enter `John` in the **First Name** field and **NYoffice** in the **Organization** field, all the users with the first name of John, who work in the NY office and are managed by you, are displayed.

If you are performing a request record search, for example, while tracking requests, you must select which data element of the request you want to search. For example, you can search for requests by entering the request ID or a target user's ID, but not both.

3.2 Customizing the Display of Data in the Administrative and User Console

This section describes how you can configure the Administrative and User Console to meet your data display requirements. This section discusses the following topics:

- Truncating Text Entries
- Displaying Process Forms with Child Tables

3.2.1 Truncating Text Entries

By default, the Administrative and User Console displays entire text entries, irrespective of the length of the entry. You can configure the Administrative and User Console so that it truncates long text entries by using a series of three dots (...).

To customize a field to show the entire entry name:

- If you are using JBoss Application Server, then:
  1. Copy the `XellerateFull.ear` file from the following directory to a temporary directory and extract its contents in the temporary directory:
     - For JBoss Application Server in nonclustered environments:

       JBOSS_HOME`/server/default/deploy/`

– For JBoss Application Server in clustered environments (the following directory on each node):

JBOSS_HOME/server/all/deploy/

2. In the extracted contents of the `XellerateFull.ear` file, locate the `xlWebApp.war` file and extract its contents in the same directory.
3. Locate the `xlWebAdmin.properties` file in the following directory inside the extracted contents of the file:

WEB-INF/classes/

4. In the `xlWebAdmin.properties` file, modify the value of the `global.property.tableColumnSize` property for all the nodes in the cluster.

   The default value is `-1`, which displays entire text entries. To display text entries with three dots, change the value of the `global.property.tableColumnSize` property to a positive integer that indicates the number of characters to display. For example, assigning a value of `10` to the `global.property.tableColumnSize` property displays the first 10 characters of each text entry and truncates any additional characters with three dots.
5. In the temporary directory, re-create the `xlWebApp.war` file with the newly modified `xlWebAdmin.properties` file included in it.
6. In the temporary directory, re-create the `XellerateFull.ear` file with the newly created `xlWebApp.war` file included in it.
7. Delete the old `XellerateFull.ear` file from the following directory, and then copy the newly created `XellerateFull.ear` file into the directory:

   – For JBoss Application Server in nonclustered environments:

   JBOSS_HOME/server/default/deploy/

   – For JBoss Application Server in clustered environments (the following directory on each node):

   JBOSS_HOME/server/all/deploy/

8. Restart the application server for the changes to take effect.

- If you are using Oracle WebLogic Server, IBM WebSphere Application Server, or Oracle Application Server, then:

1. Locate the `xlWebAdmin.properties` file in the following directory, and open it in a text editor:

   – For Oracle WebLogic Server in nonclustered environments:

   BEA_HOME/user_projects/domains/*DOMAIN_NAME*/XLApplications/WLXellerateFull.ear/xlWebApp.war/WEB-INF/classes/

   For Oracle WebLogic Server in clustered environments, the following directory on each node:

   BEA_HOME/user_projects/domains/*DOMAIN_NAME*/XLApplications/WLXellerateFull.ear/xlWebApp.war/WEB-INF/classes/

   BEA_HOME/weblogic81/common/nodemanager/*MANAGED_SERVER_NAME*/stage/Xellerate/xlWebApp.war/WEB-INF/classes/

– For IBM WebSphere Application Server in nonclustered environments:

WEBSPHERE_HOME/profiles/*PROFILE_NAME*/installedApps/*node_name*/Xellerate.ear/xlWebApp.war/WEB-INF/classes/

For IBM WebSphere Application Server in clustered environments, the following directory on each node:

WEBSPHERE_HOME/profiles/*PROFILE_NAME*/installedApps/*XL_NODE_PROFILE*/Xellerate.ear/xlWebApp.war/WEB-INF/classes/

– For Oracle Application Server in both nonclustered and clustered environments (the following directory on each node in the cluster):

OAS_HOME/j2ee/*OC4J_Instance_Name*/applications/Xellerate/xlWebApp/WEB-INF/classes/

2. In the `xlWebAdmin.properties` file, modify the value of the `global.property.tableColumnSize` property for all the nodes in the cluster.

   The default value is `-1`, which displays entire text entries. To display text entries with three dots, change the value of the `global.property.tableColumnSize` property to a positive integer that indicates the number of characters to display. For example, assigning a value of `10` to the `global.property.tableColumnSize` property displays the first 10 characters of each text entry and truncates any additional characters with three dots.

3. On a clustered environment, repeat Step 2 on each node of the cluster.

4. Restart the application server for the changes to take effect.

3.2.2 Displaying Process Forms with Child Tables

During the resource provisioning process, the Administrative and User Console by default displays any associated process form with a child table that has 10 or fewer columns.

The following are examples of Administrative and User Console pages that display child tables with 10 columns at a time:

- When you go to the User Detail page in the Resource Profile and click the **Edit** or **View** links for the resource and process forms.
- When you use the User Direct Provisioning Wizard, Step 3 through Step 6.
- When you navigate to the Organization Detail page in the Resource Profile and click the **Edit** or **View** links for the resource and process forms.
- When you use the Organization Direct Provisioning Wizard, Step 3 through Step 6.
- When you navigate to the Resource Detail page in the Organizations Associated with This Resource and click the **Edit** or **View** links for the resource and process forms.

To display a child table with more than 10 columns:

1. Open the `xlDefaultAdmin.properties` file from the following directory:

   OIM_HOME/xellerate/webapp/precompiled/jsp-temp/WEB-INF/classes

2. Modify the value of `global.property.NumberOfChildTableColumns`.

The default is 10 columns. You can change the value to any required number.

4

Managing Your Account

This chapter describes how to access and manage your Oracle Identity Manager user account and includes the following topics:

4.1 Viewing and Modifying Account Profiles

You can modify the basic information associated with your Oracle Identity Manager user account.

> **Note:** The fields you can edit in your user profile depend on how the system administrator has configured Oracle Identity Manager.

To view and edit your account:

1. Log in to the Administrative and User Console. The Welcome to Oracle Identity Manager Administrative and User Console page is displayed.
2. In the left navigation pane, click **My Account**, and then click **Account Profile**. The Account Profile page is displayed with information about your user account.
3. Click **Modify Account Profile**.
4. Make the desired changes and click **Save Profile**.

   If approvals are required for these changes, a request ID displayed. Record this ID and use it to track the request. Otherwise, the change takes effect as soon as your request is processed. Depending on the load on your system, this may take several minutes.

   Oracle Identity Manager stores the request for auditing purposes.

4.2 Changing Passwords

Depending on local system settings, you may be required to periodically change your password to maintain system security.

To change your password:

1. In the left navigation pane, click **My Account**, and then click **Change Password**. The **Change Password** page is displayed.
2. Enter your current password in the **Old Password** field, and then enter your new password in the New Password and Confirm Password fields.
3. Click **Save**.

If a password policy is attached to the Xellerate User resource object, then the **View Password Policy** link is displayed in all pages of the Administrative and User Console in which a password field is present. Clicking this link shows the password policy that is applicable for specifying a password.

> **See Also:** *Oracle Identity Manager Design Console Guide* for information about password policies

4.3 Specifying Questions and Answers for Password Change and Retrieval

You can select verification questions and the answers to these questions. You configure challenge questions and answers the first time you log in to the Administrative and User Console. These questions are used to verify your identity if you forget your password and want to reset it, or if you want to change your password.

The system administrator determines the number of questions you must answer and the list of potential questions from which you may select. From the available list of challenge questions and answers, you can select the questions for yourself.

To change the challenge questions and answers:

1. In the left navigation pane, click **My Account**.
2. Click **Challenge Q&A**. You are prompted to enter your password.
3. Enter the password, and click **Continue**. The Select Challenge Questions page is displayed.
4. Select the challenge questions, ensuring that you select at least the minimum number of questions, then click **Select**. The **Provide Challenge Answers** page is displayed.
5. Enter an answer for each question listed. You should supply answers that you can easily remember.
6. Click **Save**.
7. Click **OK** to confirm your answers.

   If you forget your password or want to reset it, then you are required to provide the answers to the questions that you selected in the preceding steps.

4.4 Delegating Responsibilities to a Proxy

You can delegate your task approval responsibilities to another user when you are unavailable, for example, due to illness or vacation. As an approver, you can select another user as a proxy for yourself. After selecting the user, any task that is assigned to you is routed to the delegated proxy user.

Note: A proxy assignment starts at 00:01 a.m. (one minute past midnight) on the start date and ends at 00:00 (midnight) at the start of the end date.

When the proxy user logs in to the Administrative and User Console, the welcome page displays the user for whom the logged-in user is a proxy. Tasks that would be assigned to the user are displayed in the proxy user's **Pending Request** list.

See Also: The "Reviewing Pending Approvals" section on page 7-1 for more information about pending requests

To designate a proxy user:

1. In the left navigation pane, click **My Account**, then click **My Proxy**. The Proxy Details page is displayed.
2. If no proxy is defined at this time, click **Assign** to delegate a user. The Assign Proxy page is displayed.
3. In the Proxy Name field, select **Your Manager** or **Other User**.

   By default, the **Your Manager** option is selected if a manager is defined for you. To look up other users, click the magnifying glass icon next to this field. The lookup form page is displayed with all the user names available for defining a proxy user.
4. Select a user ID to define your proxy user, then click **Select**. The selected user ID is displayed in the Assign Proxy page.
5. In the **Start Date** field, specify the date when you want to activate the proxy user.
6. In the **End Date** field, specify the date when you want the proxy user to be deactivated.
7. Click **Assign**. A confirmation page is displayed with the selected user ID as defined for the proxy user.
8. If information in the Confirmation page is correct, then click **Assign**. The Proxy Details page is displayed with the proxy user information that you defined.
9. To change the information for this proxy user, click **Modify**.

   To delete this user as a defined proxy user, click **Remove Proxy**.

5

Managing Your Resources

You can view resources that have been provisioned to you, and you can request access to resources for yourself and others.

This chapter discusses the following topics:

- Viewing Resources
- Viewing Resource Requests
- Requesting New Resources

5.1 Viewing Resources

To view the resources that have been provisioned to you:

1. In the left navigation pane, click **My Resources**, then click **My Resources**. The My Resources page is displayed. This page displays a table that consists of information about provisioned resources associated with the user. The information includes the resource name, the date when the resource is provisioned, and the status of the resource.
2. To request a new resource for yourself, click **Request New Resources**. The Step 1: Provide Resources page of the Create a Request to Provision Resources wizard is displayed.
3. To select the resources you want to request, select the resources, then click **Add** to add them to the Selected list.

   You can click **Remove** to delete the resource from the Selected list.

   When you are finished, click **Continue**.

   If a resource you are requesting has a resource form associated with it, then the Step 2: Provide Resource Data page is displayed. Otherwise, the Step 3: Verify Information page is displayed.
4. If the Step 2: Provide Resource Data page is displayed, enter the required data for the requested resource, and click **Continue**. The Step 3: Verify Information page is displayed.
5. Enter data as described in the fields listed in the following tables.

Field	Description
User ID	The login identification or user name
First Name	The first name of the user

Field	Description
Last Name	The last name of the user

The Resources Selected table consists of the following fields:

Field	Description
Resource Name	The name of the resource you are requesting or provisioning
Details	The additional detailed information about the resource

6. To add a comment, click **Add a comment**. The Add Request Comment page is displayed.
7. After entering your comment in the Comment field, click **Click here to add a comment** to insert a comment in your resource request.

   Click **Clear** to delete the text in the Comment field, or click **Close** to close this page without saving the data.

   After adding a comment, this page displays the added comment.
8. To modify this resource request, either click **Change** to change the resource or add another comment by clicking **Add**.
9. After verifying the information in the page that is displayed, click **Submit Now** to make the request active. The Request Submitted page is displayed.

   This Request Submitted page shows information in the fields listed in the following table:

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	The date when the request is executed

10. To activate this request at a later time, click **Schedule for Later**. The Schedule for Later page is displayed.

    If you click **Schedule for Later**, the request is created, the approval process is initiated, and approvers can approve the approval tasks and complete the approval process. However, the provisioning process will not be initiated and the resource will not be provisioned until the scheduled date.
11. Use the calendar icon to define a date to activate your request, and then click **Submit**.

> **Note:** If you are using a non-English operating system for the client, then install the appropriate language pack so that all the components of the Calendar window are displayed correctly. For example, you must install the language pack for East Asian languages when you are using an English operating system and you want the button label to be displayed in Japanese.

5.2 Viewing Resource Requests

You can view all resource requests that you have submitted for yourself and those made by other users for you.

To view all resource requests:

1. In the left navigation pane, click **My Resources**, then click **My Requests**. The My Requests page is displayed. In this page, the Raised by me option is selected by default. You can search for the request by using the search syntax for a specific target. Use the menu to select one of the following search criteria:

   - Request ID (default)
   - Request Type

   Enter a value to match the selected search criteria.

   The results table displays information in the fields listed in the following table:

Field	Description
Request ID	The identification number of the request
Request Type	The type of the request
Request Preview	The summary of the user and the associated resource for this request

2. To view the list of requests made by another user (a proxy user) for you, select the **Raised for me** option. The My Requests page is displayed.

   The table on this page is similar to the table that is displayed when you select the **Raised by me** option, but it displays resources that are raised on your behalf, including the name of the person who made the request.

   When you select the **Raised for me** option, you are the beneficiary of the request. By making a provisioning request as the administrator, your goal is to allocate resources to users or organizations. Users entitled to be provisioned with the resources view the request when they log in.

   When you select the **Raised by me** option, you are the requester. The Requester column is not displayed for this option. You will see all your requests under this option.

5.3 Requesting New Resources

The following procedure describes how to request provisioning of a new resource:

1. In the left navigation pane, click **My Resources**, then click **Request New Resources**. The Step 1: Provide resources page of the Create a Request To Provision Resources Wizard is displayed.
2. To select the resources you want to request, select **Resource Name**, and then click **Add** to add them to the Selected list.

   Alternatively, you can click **Remove** to delete the resource from the Selected list.
3. Click **Continue**. The Step 2: Provide Resource Data page of the Create a Request To Provision Resources Wizard is displayed. This page displays the resource object for the user.

4. If the resource you are requesting does not have a form for providing information, then you can skip this step.

   Click **Continue** to provide additional information about the resource object. Alternatively, click **Back** or **Exit**.

   The Step 2: Provide Resource Data page of the Create a Request To Provision Resources wizard is displayed. This page provides additional information about this resource object.

5. Enter the required additional information in the field, and click **Continue**. Alternatively, click **Back** or **Exit**. The Step 3: Verify Information page of the Create a Request To Provision Resources wizard is displayed.

   In this page, the Users Selected table displays information in the fields listed in the following table:

Field	Description
User ID	The login identification or user name
First Name	The first name of the user
Last Name	The last name of the user

   The Resources Selected table displays information in the fields listed in the following table:

Field	Description
Resource Name	The name of the resource you are requesting or provisioning
Details	The additional detailed information about the resource

6. To add a comment if required, click **Add a comment**. The Add Request Comment page is displayed.

7. After entering your comment in the Comment field, click **Click here to add a comment** to insert your comment with your resource request. Alternatively, you can click **Clear** to delete the text in the Comment field or click **Close** to close the page without saving the data.

8. To modify the information for this resource request, click **Change** to change the resource, or click **Add** to add another comment.

9. After verifying the information, click **Submit Now** to make the request active. The Request Submitted page is displayed. This page shows information in the fields as listed in the following table.

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	The date when the request is executed

10. To activate this request at a later time, click **Schedule for Later**. The Schedule for Later page is displayed.

Use the calendar icon to define a date to activate your request, and then click **Submit**.

6

Administering Requests

You can create and track requests for resources that you have requested for users and organizations. As an administrator, you can create requests to provision resources for the users you manage. If you are an approver, you can view and act on the tasks assigned to you. For example, you can approve or reject a task. If you are both an approver and an administrator, then you can perform the functions associated with both roles.

This chapter discusses the following topics:

- Creating and Managing Requests
- Tracking Requests

For a list of roles and their associated Oracle Identity Manager capabilities, see "Understanding User Roles and Capabilities" on page 1-2.

6.1 Creating and Managing Requests

You can use the Administrative and User Console to create and manage requests for provisioning resources to yourself, other users, and organizations.

As an administrator, you can create requests to provision other users with resources. Some resources may be configured to allow users to request the resource for themselves, as follows:

- If a resource allows self-service requests, then you do not have to be an administrator to request it for yourself.
- If the resource is configured as allowed for all users, then you must be an administrator to request it for another user.

If a resource is not set as allowable for *all* users, then only the users who are associated with departments or organizations for which the resource is allowed will be able to have the resource requested for them. To determine if a resource can be requested for you, contact your system administrator or the administrator for the resource.

To enable, disable, and revoke a resource instance, the resource must be configured for these tasks.

You can search for resources based on the following criteria:

- User ID
- Request ID
- Date the request was created
- Resource name

- Status of the request

In the left navigation pane, under the Requests menu item, when you click **Resources**, the following options are available to you:

- Grant Resource: Enables resources to be provisioned to a target.
- Disable Resource: Disables resources temporarily.
- Re-enable Resource: Allows you to reenable resources after the resources are disabled by the system administrator.
- Revoke Resource: Deletes resources permanently. You cannot reenable a resource after you have revoked it.

This section discusses the following topics:

6.1.1 Granting Resources

This section describes how to create requests for granting (or provisioning) resources. You can provision the same resource multiple times if the resource is configured for this usage.

> **Note:** Requesting resources for an organization is similar to requesting resources for a user. Therefore, the following procedure includes the steps for requesting resources for only a user.

To create a request for granting a resource:

1. In the left navigation pane, click **Requests**, then click **Resources**.

   The Make a Request page is displayed. In this page, the **Grant Resource** option is selected by default. You can use this option to grant a resource to a specific user or organization.

2. Click **Continue**. The Step 1: Select type page of the Create a Request To Provision Resources Wizard is displayed.

3. Click the **Users** option to assign a resource to one or many users.

   Alternatively, select the **Organization** option to provision a resource to one or many organizations.

   Click **Continue**.

   If you select the **Users** option, the Step 2: Select users page is displayed. In this page, the results table displays the following information:

Field	Description
User ID	The login identification or user name
First Name	The first name of the user
Last Name	The last name of the user

4. In the results table, select the options for the users, and then click **Add** to place the user names in the Selected list.

   You can click **Remove** to delete any user in the Selected list.

   To filter the list of users, select a key in the Filter By menu, enter selection criteria in the box next to this menu, and click **Go**.

   If the request system form has any user-defined fields, these fields are displayed on the STEP 2: Provide Additional Information page. These fields are created in the Design Console by using the User Defined Field Definition form "REQUESTS".

   See Also: *Oracle Identity Manager Design Console Guide* for information about the User Defined Field Definition form

   When you are finished, click **Continue**. The Step 3: Provide resources page is displayed.

5. Select the option for the resource, and then click **Add** to place the resource name in the Selected list.

   You can click **Remove** to delete any item from the Selected list.

   To filter the list, select a key in the **Filter By** menu, enter selection criteria in the box next to this menu, and click **Go**.

   When you are finished, click **Continue**. The Step 4: Provide Resource Data page is displayed. This page displays information about the resource and the user for this request.

6. If the information in the Step 4: Provide Resource Data page is correct, then click **Continue,** or click **Back** to make corrections.

   Any associated forms are displayed on the next page.

7. Enter the information requested in the **Forms** field and click **Continue**, or click **Back** to make corrections.

   If you click **Continue**, the Step 5: Verify Information page is displayed.

8. To add a comment, click **Click here to add a comment**.

   The Add Request Comment page is displayed.

9. Enter your comment in the **Comment** field, and click **Add comment** to insert your comment with your resource request.

   Otherwise, click **Clear** to delete the text in the Comment field, or click **Close** to cancel this page.

   After adding a comment, this page displays the added comment.

10. After verifying the information, click **Submit Now** to make the request active.

    The Request Submitted page is displayed.

    This page shows the following information:

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request

Field	Description
Date	The date when the request is executed

11. To activate this request at a later time, click **Schedule for Later** to define a date when the request becomes active.

    Specify a date that is later than today's date. The Schedule for Later page is displayed.

    The Schedule for Later option is often used for new employees who are starting on a future date. After you define a date, the request is created, the approval process is initiated, approvers can approve the tasks, and the approval process can be completed. However, the provisioning process is not initiated until the scheduled date.

12. Use the calendar icon to define a date to activate your request, and then click **Submit**.

> **Note:** When you use a single request to grant resources to multiple users, rule evaluation performed to determine the password policy to be applied is based on the last modified user from the selected group of users.

6.1.2 Disabling Resources

This section discusses how to create requests for disabling resources.

> **Note:** Disabling resources for an organization is similar to disabling resources for a user. Therefore, the following procedure includes the steps for disabling resources for only a user.

To create a request for disabling a resource:

1. In the left navigation pane, click **Requests**, then click **Resources**.

   The Make a Request page is displayed.

2. Select the **Disable Resource** option, and click **Continue**.

   The Step 1: Select type page of the Create a Request To Disable Resources Wizard is displayed.

   This page lets you select one of the following options:

   - **Users**: You can disable resources for one or many users.
   - **Organizations**: You can disable resources for one or many organizations.

     In this example, the Users option is selected.

3. Click **Continue**.

   The Step 2: Select users page is displayed.

4. Select the options for the users, and then click **Add** to place the user names in the Selected list.

   You can click **Remove** to delete any user in the Selected list.

To filter the list, select a key in the **Filter By** menu, enter selection criteria in the box next to this menu, and click **Go**.

When you are finished, click **Continue**.

The Step 3: Provide resources page is displayed.

5. Select the option for any resource that you want to disable from the user, and then click **Add** to place the resources in the Selected list.

   You can click **Remove** to delete any resources in the Selected list.

6. Click **Continue**.

   If multiple instances of a resource are provisioned for the user, the Step 4: Resolution page is displayed. Otherwise, the Step 5: Verify Information page is displayed.

7. If the Step 4: Resolution page is displayed, select the resource instance you want to disable, then click **Continue**.

   The Step 5: Verify Information page displays the following information.

Field	Description
User ID	The login identification or user name
First Name	The first name of the user
Last Name	The last name of the user
Resource Name	The name of the resource you are disabling
Details	The additional detailed information about the resource

8. To add a comment, click **Click here to add a comment**.

   The Add Request Comment page is displayed.

9. Enter a comment in the Comment field, and click **Add a comment** to insert the comment with your resource request.

   Click **Clear** to delete the text in the Comment field. Click **Close** to close this page.

   The Verify Information page displays any added comment.

   To modify the information for this resource request, click **Change**. Click the **Add** link to add another comment.

10. After verifying the information, click **Submit Now** to make the request active.

    The Request Submitted page is displayed.

    This page shows the following information:

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	The date when the request is executed

11. To activate this request at a later time, click **Schedule for Later**.

The Schedule for Later page is displayed. Use the calendar icon to define a date to activate your request, then click **Submit**.

6.1.3 Reenabling Resources

You can reenable a resource after you disable it. You cannot reenable a revoked resource. This section discusses how to create requests for reenabling resources.

> **Note:** Reenabling resources for an organization is similar to reenabling resources for a user. Therefore, the following procedure only includes the steps for reenabling resources for only a user.

To create a request for reenabling a resource:

1. In the left navigation pane, click **Requests**, then click **Resources**.

   The Make a Request page is displayed.

   The **Grant Resource** option is selected by default.

2. Select the **Reenable Resource** option to provide access to resources that are system administrator for this user, and click **Continue**.

   The Step 1: Select type page of the Create a Request To Reenable Resources wizard is displayed.

3. Click **Users** to reenable resources that are system administrator for one or many users.

   Otherwise, select **Organization** to reenable resources that are system administrator for one or many organizations. In this example, the **Users** option is selected.

4. Click **Continue**.

   The Step 2: Select users page is displayed.

   The results table displays the following information:

Field	Description
User ID	The login identification or user name
First Name	The first name of the user
Last Name	The last name of the user

5. Select the **Users** option, and then click **Add** to place the user name or names in the Selected list, or click **Remove** to delete users from the Selected list.

   When you are finished, click **Continue**.

   The Step 3: Provide resource page is displayed.

6. Select the Resource Name option, and then click **Add** to place the resource name in the Selected list, or click **Remove** to delete users from the Selected list. Then, click **Continue**.

   If multiple instances of a resource instance are provisioned for the user, the Step 4: Resolution page is displayed. Otherwise, the Step 5: Verify Information page is displayed.

7. If the Step 4: Resolution page is displayed. Select the resource instance you want to reenable, and then click **Continue**.

   The Step 5: Verify Information page is displayed.

8. To add a comment, click **Click here to add a comment**.

   The Add Request Comment page is displayed.

9. Enter your comment in the **Comment** field, and click **Add Comment** to insert your comment with your resource request.

   The page displays the added comment.

   Click **Clear** to delete the text in the Comment field, or click **Close** to cancel this page.

10. Verify the information on the Step 5: Verify Information page, then click **Submit Now** to make the request active.

    The Request Submitted page is displayed, which shows the following information:

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	The date when the request is executed

    If you want to view the details of this request, then click **Request ID**. The Request Details page is displayed. For more information about this page, see "Tracking Requests" on page 6-9.

11. To activate this request at a later time, click **Schedule for Later**.

    The Schedule for Later page is displayed.

12. Use the calendar icon to define a date to activate your request, and then click **Submit**.

6.1.4 Revoking Resources

Revoking requests is a permanent operation.

To create a request for revoking a resource:

1. In the left navigation pane, click **Requests**, then click **Resources**.

   The Make a Request page is displayed.

2. Select the **Revoke Resource** option, and then click **Continue**.

   The Step 1: Select type page of the Create a Request To Revoke Resources Wizard is displayed.

   This page lets you select one of the following options:

   - **Users**: You can revoke resources for one or many users.
   - **Organizations**: You can revoke resources for one or many organizations.

   In this example, the **Users** option is selected.

3. Click **Continue**.

The Step 2: Select users page is displayed.

4. Select the option for the users, and then click **Add** to place the user names in the Selected list.

   You can click **Remove** to delete any user names from the Selected list, and then click **Continue**.

   The Step 3: Provide resources page is displayed.

5. Select the option for each resource for which you want to revoke user access, then click **Add** to place the resources in the Selected list.

   You can click **Remove** to delete any resources from the Selected list, and then click **Continue**.

   If multiple instances of a resource are provisioned for the user, the Step 4: Resolution page is displayed. Otherwise, the Step 5: Verify Information page is displayed.

6. If the Step 4: Resolution page is displayed, select the resource instance you want to revoke, and then click **Continue**.

   The Step 5: Verify Information page is displayed.

7. The Step 5: Verify Information page displays the information described in the following tables.

   The Users Selected table displays the following information:

Field	Description
User ID	The login identification or user name
First Name	The first name of the user
Last Name	The last name of the user

   The Resources Selected table displays the following information:

Field	Description
Resource Name	The name of the resource you are requesting or provisioning
Details	The additional detailed information about the resource

8. To add a comment, click **Click here to add a comment**.

   The Add Request Comment page is displayed.

9. Enter your comment in the **Comment** field, and click **Add a comment** to insert your comment with your resource request.

   The Verify Information page displays the added comment.

   Otherwise, click **Clear** to delete the text in the **Comment** field, or click **Close** to cancel this page.

   To modify the information for this resource request, click **Change** to change the resource, or click **Add** to add another comment.

10. Verify the information and click **Submit Now** to make the request active.

    The Request Submitted page is displayed. This page shows the following information:

Field	Description
Status	The status of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	The date when the request is executed

11. To activate this request at a later time, click **Schedule for Later** to define a date when the request becomes active.

    The Schedule for Later page is displayed. Use the calendar icon to define a date to activate your request, and then click **Submit**.

6.2 Tracking Requests

Depending on the permissions that have been assigned to you in Oracle Identity Manager, you can view requests for resources. In addition, you can edit details or approve tasks within those requests. This is referred to as tracking a request. The requests that you can track fall into one of the following categories:

- Requests created by other users to provision you with resources
- Requests you created to provision other users with resources
- Requests you created to provision yourself with resources
- Requests you created through self-registration
- Requests you created by modifying your profile

The types of requests you can create, view, and edit are governed by characteristics of your account in Oracle Identity Manager. If you are assigned to approve a task within a request, you can approve any task assigned to you when tracking that request. For a list of the various roles and their associated capabilities, see "Understanding User Roles and Capabilities" on page 1-2.

The following topics describe how to perform tasks related to tracking requests:

- Searching for Requests
- Viewing Approval Details
- Viewing Provisioning Details
- Viewing Request Comments
- Viewing Request Status History

6.2.1 Searching for Requests

The following procedure describes how to search for a request.

1. In the left navigation pane, click **Requests**, then click **Track**.

   The Track Requests page is displayed. To locate the request you want to track, you can search for existing requests by using the options on this page. You can select only one of these options, for example, User ID or Request ID, not both. If you select a request ID or resource name and leave the fields associated with that option blank, all requests are displayed.

If you are unable to locate a request by using one of the search options, select a different option or widen your search criteria to retrieve more results. The following table lists the available search criteria.

Field	Description
User ID	Lets you track requests that are created for yourself or another user. Select Self or Other. If you select Other, then you must click Find User ID and specify the user associated with the requests that you want to track. You can use the asterisk (*) wildcard character to search for requests associated with user IDs beginning or ending with specific characters or numbers. You can also search by the organization to which the user belongs.
Request ID	Lets you track requests by the ID of the request. This is usually a numeric value. Select this option, and then enter the ID of the request. You can use the asterisk (*) wildcard character to search for requests beginning or ending with specific characters or numbers.
Creation Date	Lets you track requests by date of creation. Select this option, then enter the start and end dates for the range on which you want to query. All the requests created between those dates are displayed.
Resource Name	Lets you track requests according to the resources to be provisioned, which means, the resources specified on the request. Select this option, and then enter the name of the resource. You can use the asterisk (*) wildcard character to perform searches for requests containing a resource name that begins or ends with specific characters.
Status	Lets you track requests according to the status of the request, for example, Request Initialized, Request Received, Approved, Not Approved, Request Cancelled, Request Closed, Object Approval Complete, Request Complete, or Provide Information. Select this option, and then select the desired status from the menu. **Note:** You can specify multiple statuses for searching requests.

2. Click **Search**.

   All the requests that match the criteria you entered are displayed. If your query has retrieved several pages of requests, then use the First, Previous, and Next links to move through the result set.

3. To view the details of a request, click the **Request ID** link in the results table.

   The Request Details page is displayed.

   To cancel an entire request, select the option next to it, and click **Cancel Request**.

6.2.2 Viewing Approval Details

Approval details include all approvals for the request including process and pending tasks.

To view approval details:

1. Search for a resource request, as described in "Searching for Requests" on page 6-9.
2. Select **Approval Details** option from the Additional Details box.

   The **Approved Tasks** page is displayed. The **Approval Details** field shows all tasks associated with the approval processes. The Request ID number is an active

link to the Request Details page for this request. The Request Approval Task table displays the following fields:

Field	Description
Task	Name of the approval task.
Status	Current status of the request.
Assign To	Assignment of the request to the user or proxy user. The request can also be assigned to a user group or proxy group.
Action	The Action column has an option for each request. The last row contains **Approve**, **Deny**, and **Re-assign** buttons that you select to determine the action for the request. Select the requests and click **Approve** or **Deny**. A confirmation page is displayed with the tasks with **Confirm** and **Cancel** buttons. If you click **Re-assign**, then the console displays a list of all the users that you or the proxy user has permission to see to whom you can reassign the task. This page has an option that, when selected, lists all the groups to whom the task can be reassigned.

6.2.3 Viewing Provisioning Details

You can view provisioning tasks by user, organization, or resource depending on whether the request is created for a user, organization, or resource.

To view provisioning details:

1. Search for a resource request, as described in "Searching for Requests" on page 6-9.
2. Select the **Provisioning Details** option from the Additional Details box.

   The Provisioning Tasks page is displayed. The Provisioning Details field shows all the tasks associated with the provisioning processes.
3. Select the appropriate option to display the information you want.

6.2.3.1 Viewing Provisioning Details by User/Organization

When you select **User/Organization**, the page displays all the tasks for the users or organizations who will be provisioned. If a request has multiple users or organizations, then the page displays a corresponding table for each user or organization.

The information table shows the following:

Field	Description
Resource Name	The name of the resource object to be provisioned
Resource Status	The current status of the resource request
Process Instance Name	The name of either an approval process or a provisioning process
Description	A number that uniquely identifies the process or any identifier that maps the process to the Map Descriptive field
Process Status Details	The current status of the process

6.2.3.2 Viewing Provisioning Details by Resource

Select the **Resource** option to display all the resources and information related to this resource. If a request has multiple resources, then the page displays a corresponding table for each user or organization.

The information table shows the following:

Field	Description
User/Organization	The name of the user or organization that has been provisioned with this resource object
Resource Status	The current status of the resource request
Process Instance Name	The name of the provisioning process
Data	A number that uniquely identifies the process
Process Status Details	The current status of the process

6.2.4 Viewing Request Comments

A request is viewed by any user with view permissions. Comments enable other users to understand the request. Users, as well as the system administrator, can add comments to the request so that others can see how the request has been processed.

To view request comments:

1. Search for a resource request, as described in "Searching for Requests" on page 6-9.
2. Select the **Request Comments** option from the Additional Details box.
3. Click the Request ID number to go back to the Request Details page.

   You can add a comment on this page by clicking **Click here to add a comment**. If there is a comment added to this request, then the Request Comments page is displayed with the comment.

   This page displays a table with the following information:

Field	Description
Comment	The actual comment that is added
Date	The date when the comment is added
Add By	The user name logged in to the console

6.2.5 Viewing Request Status History

Request status history is a supplemental view that helps you understand the state of the current workflow. Users can make a request and a workflow is created. There are many steps and actions that must be taken, such as a manual action by the user or a system action, before the request is completed or rejected.

Whenever an action is executed, the status of the workflow is changed and it transitions to the next state.

To view status history:

1. Search for a resource request, as described in"Searching for Requests" on page 6-9.
2. Select the **Request Status History** option from the Additional Details box.

   The Request History page is displayed. This page shows a table that depicts the workflow of the request. This page displays the information listed in the following table.

Field	Description
Status	The current status of the resource request
Date	The date when the request is created
Create by	The name of the user who created this request

7

Managing Your To-Do List

A To-Do list is a list of tasks within a process. Tasks are the constituent elements of the processes for approving requests and their associated resources, and making the resources available for provisioning.

Before resources in a request can be provisioned to target users, other users who are assigned as approvers for tasks of the provisioning process must provide approval. If approvals are required for self-registration, then the approval tasks associated with user self-registration requests also require action by an assigned approver before the registration process can be completed.

Only users who are task approvers for provisioning tasks, or administrators of the organizations to which the target users belong, can view tasks in a request. If you are an approver for any task in a request, then you can view all the tasks in the request, but you can approve only the tasks that are assigned to you. You can also view pending requests for users whom you manage.

You define a process by using the Process Definition form in the Design Console. When defining the process, you specify whether the process is of the Provisioning or Approval type. By selecting the Provisioning type, the process becomes a provisioning process. Each resource is associated with one mandatory provisioning process. Tasks can then be assigned to the users.

This chapter discusses the following topics:

7.1 Reviewing Pending Approvals

You can use the Pending Approvals page to view and complete tasks that are assigned to you. In addition, you can view requests that are assigned to the users for whom you are the manager.

To review pending approvals:

1. In the left navigation pane, click **To-Do List**, and then click **Pending Approvals**.

   The Pending Approvals page is displayed, with a list of all the requests that contain one or more tasks for which you are an approver. By default, the page is displayed with pending requests that are assigned to you.

2. To view pending requests that are assigned to users that you manage, select the **Assigned to user(s) you manage** option.

The appropriate pending requests are displayed.

You can also query for specific requests by using the Search list, which provides the following search criteria:

- Request ID
- Requester
- Assigned To

The results table has a description of the search criteria. Enter the appropriate value in the corresponding field. For example, to use the Request Type criterion, select the corresponding value from the **Request Type** list. The results table displays the following fields:

Field	Description
Request ID	The unique and system-generated identification number of the request.
Request Type	The request type can be one of the following:: Add, revoke, enable, or disable resources for users or organizations **Note:** The following request types are not used in release 9.1.0.1 and later releases of Oracle Identity Manager: Enable, disable, delete, or modify entity
Requester	The user who created the request.
Request Preview	The summary of the request. The information being displayed includes the user ID or organization and the resource.
Assigned To	The user assigned to approve this request.
Status	The status of the request.
Approve/Deny	The request to either approve or deny it.
Reassign	The request to be reassigned to another user or user group.

3. To approve a pending request, select the appropriate option in the **Approve/Deny** column, and then click **Approve**.

   The request ID is removed from the results table.

   To deny a pending request, select the appropriate option in the **Approve/Deny** column, and then click **Deny**.

   The request ID is removed from the results table.

4. To reassign a pending request, select the appropriate option in the **Re-Assign** column, and then click **Re-Assign**.

   The Re-Assign Pending Approvals page is displayed.

5. Select the option for the user or group to which you want to reassign the request, and then click **Re-Assign**.

   The Confirm page is displayed.

7.1.1 Managing the Display of Pending Approvals

You can use the `Remove Open Tasks` scheduled task to manage the display of pending approvals. This is described in the "Managing the Display of Open Tasks" section on page 7-5.

7.2 Managing Open Tasks

The Open Tasks page lists open (pending or rejected) tasks that are defined for a provisioning process. The Open Tasks page displays all open provisioning tasks that are assigned to you or a user for whom you are the manager. Use the Open Tasks page to retry a task if the task has a `Rejected` status, reassign a provisioning task to another user, or specify a response for a provisioning task. This section describes the following tasks:

- Viewing Open Tasks
- Retrying Rejected Tasks
- Reassigning Open Tasks
- Setting Responses to Open Tasks
- Manually Completing Rejected Tasks
- Managing the Display of Open Tasks

7.2.1 Viewing Open Tasks

You can view all open provisioning tasks that are assigned to you, or the users and user groups that you manage.

To view open tasks:

1. In the left navigation pane, click **To-Do List** and then click **Open Tasks**.

   The Open Tasks page is displayed.

2. Use the **Filter By** search criteria to sort the tasks by the following categories:

   - Task Name
   - Resource Name
   - Organization Name
   - User ID
   - Assign Before (enter date – yyyy-MM-dd)
   - Assign After (enter date – yyyy-MM-dd)

   Enter the appropriate value in each field. To use the **Open Task Type** and **Object Type** criteria, select the corresponding value and then click **Go**. The results table displays the following information about the provisioning task:

Field	Description
Task Name	The name of the task that you have defined in the Process Definition form for this resource name.
Task Status	The current status of the resource task.
Resource Name	The name of the resource associated with this provisioning task.
Description	This is a description of the task.

Field	Description
Process Form	This is a link to the process form associated with the task.
Request ID	This number identifies the request with which the task is associated.
Organization Name	The organization with which the task is associated.
Target User	The user for whom the provisioning process was started.
Date Assigned	The date that the provisioning task was assigned.
Assigned To User	The user name of the user to whom the provisioning task is assigned.
Retry	If this check box is selected, then it indicates that the status of the provisioning task is `Rejected`. Use this check box to retry the provisioning task if it is in the `Rejected` state.
Reassign	Use this check box to assign this provisioning task to another user or user group.
Set Response	Use this check box to set a response for this provisioning task.
Complete Manually	Use this check box to manually complete the provisioning task if it is in the `Rejected` state

7.2.2 Retrying Rejected Tasks

You can retry tasks that are in the `Rejected` state. To perform this procedure:

1. Perform the procedure described in the "Viewing Open Tasks" section on page 7-3 to display the list of open tasks.
2. Select the **Retry** check box for the task that you want to retry, and then click **Retry**.

   If the task is completely successfully, then it is moved to the Completed state.

> **Note:** The number of times that you can retry a rejected task is defined in the Design Console. See *Oracle Identity Manager Design Console Guide* for more information.

7.2.3 Reassigning Open Tasks

You can assign open tasks to other users. To reassign open tasks:

1. Select the required tasks, and then click **Reassign**.

   The Re-Assign Open Tasks page is displayed
2. Select a user ID or group ID, and then click **Reassign**.

   Only one user ID or group ID can be selected.

   A Confirmation page is displayed. This page displays the user ID (first name and last name) in the first sentence and the provisioning task as a bulleted list item.
3. Click **Confirm Reassign Tasks**, or click **Cancel**.

   The Open Tasks page is displayed.The provisioning task that you have reassigned is no longer in the results table.

7.2.4 Setting Responses to Open Tasks

To set a response to an open task:

1. Select one or more provisioning tasks, and then click **Set Response.**

   The Specify Task Responses page is displayed.

2. Select a response for the provisioning task, and then click **Set Responses**.

   Otherwise, click **Cancel**.

   A Confirmation page displays the response for this provisioning task.

3. Click **Confirm Response for Tasks**, or click **Cancel**.

   The Open Tasks page is displayed. The provisioning task for which you set a response is no longer displayed in the results table.

7.2.5 Manually Completing Rejected Tasks

To manually complete tasks that are in the `Rejected` state:

> **Note:** You can perform this procedure only for open tasks that are in the `Rejected` state.

1. Perform the procedure described in the "Viewing Open Tasks" section on page 7-3 to display the list of open tasks according to your requirements.

2. Select **Complete Manually** for the task that you want to complete manually, and then click **Complete Manually**.

   The task is moved to the Completed state.

7.2.6 Managing the Display of Open Tasks

Along with information about tasks at various stages, information about open tasks and pending approvals is stored in the Oracle Identity Manager database. This information is distributed between two tables. In addition to these two tables, a single table stores a copy of information about open tasks and pending approvals. When a search for open tasks or pending approvals is performed, this table is queried for the required information. This feature reduces the time taken to fetch and display open tasks or pending approvals.

After a period of time, the number of open tasks and pending approvals may increase and cause a corresponding increase in the time taken to fetch and display information. To improve the performance of data fetch operations, from the single table that stores a copy of information about open tasks and pending approvals, you can remove the records that have stayed at the Open or Pending stage for longer than a specified number of days. You use the `Remove Open Tasks` scheduled task to achieve this.

Note: The `Remove Open Tasks` scheduled task deletes only a copy of information about open tasks and pending approvals. This information is still available in the two tables that store information about all tasks.

However, open tasks and pending approvals for which the copy of information has been deleted are not displayed on the Administrative and User Console. If you want to view deleted information, then you must create reports that query the original tables in which this information is retained. See *Oracle Identity Manager Audit Report Developer's Guide* for more information.

You can use APIs of the Request and Provisioning operations to create a report based on information about open tasks and pending approvals from these tables. See the Javadocs for more information about APIs of these operations.

To use the `Remove Open Tasks` scheduled task:

See Also: *Oracle Identity Manager Design Console Guide* for detailed information about each step of the following procedure

1. Enable the scheduled task.
2. Specify the frequency at which the scheduled task must run.
3. Specify a value for the `Day Limit` attribute of the scheduled task. The value of this attribute indicates the number of days for which information about an open task or pending approval must be retained in the table before the information is deleted. The default value of this attribute is 60 days.

When the scheduled task runs, it removes all open task and pending approval records that have been in the table for longer than the specified number of days.

7.3 Managing Attestation Requests

Attestation is a mechanism by which reviewers are periodically notified of a report they must review that outlines the provisioned resources that certain users have. The reviewer can attest to the entitlements accuracy with an appropriate response. You can display all open attestation tasks that are assigned to you, and certify, reject, decline, or delegate attestation tasks.

The rest of this section discusses the following topics:

- Viewing Attestation Requests
- Saving Attestation Actions
- Updating Comments and Delegations
- Submitting Attestations

7.3.1 Viewing Attestation Requests

Attestation requests enable you, as a reviewer, to determine if user entitlements are valid. You can certify, reject, decline, or delegate requests for attestation.

Note: A request that is declined is reassigned to a member of a process owner group.

To view attestation requests:

1. In the left navigation pane, click **To-Do List**, then click **Attestation**.

   The Attestation Request Inbox page is displayed. This page contains a results table that provides the following information about your pending attestation process requests:

Field	Description
Process Names	Specifies the name of the process.
Process Code	Specifies the code for the process.
Data Type	Specifies the type of data being attested.
Scope	Indicates whether the attestation scope is by manager, group, organization, or resource.
Delegated By	Identifies the user who delegated the task to you. This field is blank if the task is assigned by the attestation process.
Current Request	Specifies the date and time on which the attestation task is created.

2. In the results table on the Attestation Request Inbox page, click the link of the process name that you want to manage.

   The request page shows the entitlements that the user must attest to as a part of the task. The reviewer can also see the details (process form data) of the entitlement that they are attesting to. The results table contains the following columns:

Field	Description
User	The user whose entitlement is being attested
Resource	The resource for which the entitlement is being attested. The data is a link with pop-up a page that displays the entitlement process form data as it is on the Attestation Date.
Descriptive Data	A description of the provisioned resource instance
Last Attested	The date and time when this entitlement was last attested
Comments	Comments that you entered about the entitlement
Actions	The Certify, Reject, Decline, and Delegate options that you can select from to specify the action for the entitlement

3. To display only records for which actions are not already specified, select **Hide records where action has already been specified**.
4. To view additional rows in the results table, click **Next**.

7.3.2 Saving Attestation Actions

The following procedure describes how to save an attestation action.

Note: Saving an attestation is not the same as submitting one. To submit attestations, follow the procedures in "Submitting Attestations" on page 7-8.

To save an attestation action:

1. Follow the steps listed in "Viewing Attestation Requests" on page 7-6 to select the attestation process that you want to save.
2. On the Attestation Request page, select any actions you want to take for the listed entitlements and click **Save**.

   The Save Actions page is displayed. This page shows a table that lists the resource entitlements in the current attestation request for which you have selected an action. Any entitlement for which you select the Delegate action also lets you search for a reviewer in the Delegated Reviewer field.
3. On the Save Actions page, enter any desired comments for the listed entitlements, or select a reviewer for any entitlements with a value of **Delegate** in the **Reviewer Action** column.
4. The reviewer can provide values for the Default Comment and Default Delegated Reviewer columns.

   These values are used for all entitlements on a page when a specific value is not provided in the table.
5. Click **Save**.

7.3.3 Updating Comments and Delegations

To update an attestation request:

1. Follow the steps in "Viewing Attestation Requests" on page 7-6 to select the attestation process that you want to update.
2. Follow the steps in "Saving Attestation Actions" on page 7-7 to enter comments or select delegated reviewers for any entitlements.
3. Click **Update Existing Comments & Delegation Information**.

   The Update Comments and Delegates page is displayed. The table shown on this page lists the entitlements in the current attestation request for which you have selected an action.
4. On the Update Comments and Delegates page, select the entitlements that you want to update, enter comments (if required), and select the reviewer to whom you want to delegate the attestation request.
5. Click **Save**.

7.3.4 Submitting Attestations

The following procedure describes how to submit an attestation.

Note: You can submit an attestation only if you have designated an action for each entitlement in the current attestation process request. If you have not designated an action, then the **Submit Attestation** button is inactive.

To submit an attestation:

1. Follow the steps in "Viewing Attestation Requests" on page 7-6 to select the attestation process that you want to submit.
2. Follow the steps in "Saving Attestation Actions" on page 7-7 to enter comments or select delegated reviewers for any entitlements.
3. On the Attestation Request page, click **Submit Attestation**.

   The Attestation Request Confirmation page is displayed.
4. On the Attestation Request Confirmation page, click **Submit**.
5. After the task is submitted, it is removed from the attestation inbox.

8

Creating and Managing Users

Any identity that exists within Oracle Identity Manager and is managed within Oracle Identity Manager is called an **OIM User**. An OIM User can be created in the following ways:

- Through reconciliation from one or more trusted identity sources, such as HRMS or LDAP
- Manually through the Administrative and User Console
- Through the Java APIs and/or the SPML Web Service

An OIM Account is granted to an OIM User to give the OIM User the ability to log in to Oracle Identity Manager to access Oracle Identity Manager features. At the minimum, these features involve self-service and request. An OIM Account can be granted additional permissions including delegated administration of various entities, such as users, organizations, and roles, and the ability to define workflows. As an administrator, even if you allow users to self-register, you may still want to provide other administrators with the ability to create accounts on behalf of other users. Not all users will be able to create accounts for other users.

This chapter discusses the following topics:

8.1 Creating Users

To create an OIM User:

1. In the left navigation pane of the Administrative and User Console, click **Users**, and then click **Create**.
2. On the Create User page, enter the data required for user registration.

   Table 8–1 describes the GUI elements on the Create User page.

Table 8–1 GUI Elements on the Create User Page

Label on the Create User Page	Action or Description
User ID field	Enter a user ID for the user account. An exception is thrown if you attempt to reuse an existing user ID after setting the User ID Reuse property to `true` in the Design Console. To resolve this issue, delete the unique index for the `USR_LOGIN` column in the `USR` table and create a non-unique index. See *Oracle Identity Manager Design Console Guide* for more information about User ID Reuse property.

Table 8–1 (Cont.) GUI Elements on the Create User Page

Label on the Create User Page	Action or Description
First Name field	Enter the first name of the user.
Middle Name field	Enter the middle name of the user.
Last Name field	Enter the last name of the user.
Status field	During user account creation, this display-only check box is grayed out (disabled). On the User Detail page, which is displayed after you click Create User, this check box shows the current status of the user account. The status value can be one of the following: ■ Active ■ Disabled ■ Disabled Until Start Date ■ Deleted
Organization lookup field	Select the organization in which you want to create the user account.
User Type list	Select one of the following user types: ■ End-User ■ End-User Administrator
Employee Type list	Select one of the following employee types: ■ Full-Time Employee ■ Part-Time Employee ■ Temp ■ Intern ■ Consultant
Manager ID field	Enter the user ID of the user's manager.
Email field	Enter an e-mail address for the user.
User Disabled check box	During user account creation, this display-only check box is grayed out (disabled). If the user is in the Disabled or Disabled Until Start Date state during or at any time after account creation, then this check box is selected on the User Detail page displayed after you click Create User. A user account is in the Disabled Until Start Date state if you enter a future date value in the Start Date field during user account creation.
Password field	Enter a password for the user.
Confirm Password field	Reenter the password.
User Locked check box	During user account creation, this display-only check box is grayed out (disabled). At any time after account creation, if the user is in the Locked state, then this check box is selected on the User Detail page that is displayed during a Manage User operation. The user account is locked after a specified number of unsuccessful login attempts. If this happens, then the user can answer the challenge questions and unlock the account. If the user is not able to correctly answer the challenge questions, then only an administrator can unlock the user account.
Start Date date editor	Enter a start date for the user account. If you enter a future date, then the user account is disabled until the start date. If you do not enter a start date, then the user is active immediately after account creation and the Start Date value is set to the current date.

Table 8–1 (Cont.) GUI Elements on the Create User Page

Label on the Create User Page	Action or Description
End Date date editor	Enter an end date if you want the user account to be deleted (that is, moved to the Deleted state) and all the resources provisioned to be revoked on a particular date.
Provisioning Date date editor	Enter the date from which resources can be provisioned to the user. Provisioning requests for the user can be initiated before the specified provisioning date. However, the actual provisioning of those resources to the user will not occur until after the specified provisioning date. If you do not specify a provisioning date, then resources can be provisioned to the user immediately after the account is created.
Provisioned Date field	This display-only field shows the date on which provisioning was enabled for the user.
Deprovisioning Date date editor	Enter the date on which you want to deprovision (that is, revoke) all resources provisioned to the user. After this date, resources cannot be provisioned to the user.
Deprovisioned Date field	This display-only field shows the date on which provisioning was disabled for the user.
Change Password at next logon check box	Select this check box if you want the user to change the user's password at first logon. If you select the **Change password at next logon** check box, then the Change Password page is displayed for the user when the user logs in after the option is set. When a user is created in Oracle Identity Manager, the user is forced to change the password when logging in for the first time. This is done by setting the value of the `Force Password Change At First Login` property, which has the `XL.ForcePasswordChangeAtFirstLogin` keyword, to `True` by using the System Configuration form of the Design Console. Note that the user is forced to change the password at first logon only when the user is created with the `XL.ForcePasswordChangeAtFirstLogin` keyword already set to `True`. **See Also:** The "Password Policies Form" section in *Oracle Identity Manager Design Console Guide* for information about creating a password policy Whenever you change the value of the `Force Password Change At First Login` property, you must restart the server or purge the cache for the change to take effect. For this, the cache category is `ServerCachedProperties`. **Note:** ■ The default value of the `Force Password Change At First Login` property is `True`. To disable the property, set the value to `False`. ■ See *Oracle Identity Manager Best Practices Guide* for information about running the `PurgeCache` utility.

3. Click **Create User**.

   Oracle Identity Manager creates the user account and displays the User Details page with the user's account information.

   If you select any of the options in the Additional Details region, then you will see limited information because you have just created the user.

On the User Detail page, you can select the following:

- **Edit:** Change the user profile.
- **Disable:** Disable the user from being provisioned.

- **Unlock:** Unlock the user account if it is locked after login retry limit was exceeded.
- **Delete:** Delete the user account.
- **Change Password:** Change the current password.

8.1.1 Editing User Profiles

To edit a user profile:

1. On the left navigation pane, click **Users**, and then click **Manage**.
2. On the Manage User page, select one or more attributes from the menus, and then enter search criteria, including an asterisk (*) if you need a wildcard, in the field next to the menu.

   To use the **Employee Type** and **Status** search criteria, select values from the corresponding fields.
3. Click **Search User**.
4. From the list of users that is displayed, click the field for the user whose information you want to edit.

   The User Detail page is displayed. See Table 8–1 for information about the GUI elements displayed on this page.
5. Click **Edit**.
6. Edit the user's data, and then click **Save**.

8.1.2 Disabling Users

By disabling a user, you can ensure that nothing will be provisioned to the user. Depending on your role or status, the Edit User page allows the Disable button to toggle between Disable and Enable.

To disable a user profile:

1. In the left navigation pane, click **Users**, and then click **Manage**.
2. On the Manage User page, select one or more attributes from the menus, and enter search criteria, including an asterisk (*) if you need a wildcard, in the field next to the menu.

   To use the Employee Type and Status search criteria, select values from the corresponding fields.
3. Click **Search User**.
4. From the list of users that is displayed, select the check box for the user whose information you want to disable, and then click **Disable**.

8.1.3 Changing User Passwords

To change a user's password:

1. Click **Change Password**.

   The Change Password page is displayed.
2. Enter a new password and confirm.
3. Click **Save Password**.

8.2 Managing Users

You can modify, disable, delete, and unlock user accounts. You can also change the passwords of user accounts.

> **Note:** Only locked accounts can be unlocked. An account becomes locked if a user has exceeded the maximum number of login retry attempts.

The following procedure describes how to manage a user account:

1. In the left navigation pane, click **Users**, then click **Manage**.

   The Manage User page is displayed.

2. Enter information related to the user in the fields.

   Use one or more menus to deselect search attributes. After making a selection, enter text to be matched in the next field or use a wildcard asterisk (*). The more information you provide, the more precise the retrieved list of user records will be. To use the Employee Type and Status search criteria, select values from the corresponding boxes.

   > **Note:** If you specify a search criterion, leave the value field blank, and click **Search User**, then the results displayed include NULL values from the user table. This is because the search criterion field is not included in the query criteria at all.
   >
   > However, if you specify a search criterion, enter the asterisk (*) in the value field, and click **Search User**, then the results displayed include only non-NULL values of the field specified as the search criterion.

3. Click **Search User**.

   Oracle Identity Manager displays the list of users who match the criteria you entered.

4. To disable, enable, unlock or delete an account, select the appropriate check box and button.

   For example, to disable the user accounts, select the **Disable** check box in the applicable rows and click **Disable.**

5. To edit a user's account, click the user ID for that account.

   Oracle Identity Manager displays the user's profile.

6. To edit, disable, enable, unlock, delete, or change the password of an account, click the appropriate button.

   Use the menu to view additional details about the user.

   - Click **Resource Profile** to view resources that are provisioned for the user.

     You can also provision resources in this page by clicking **Provision New Resource**.

   - Click **Group Membership** to view the Group Membership page, which lists any group membership that the user is associated with.

     You can also use the Group Membership page to assign users to groups.

- Click **Proxy Details** to view the Proxy Details page, which lists any proxy user that the user is associated with.

  You can also use the Proxy Details page to assign a proxy.

9

Creating and Managing Organizations

This chapter describes how to create and manage organizations in Oracle Identity Manager and contains the following topics:

- Creating Organizations
- Managing Organizations
- Managing Organization Details

9.1 Creating Organizations

To create an organization:

1. In the left navigation pane, click **Organizations**, then click **Create**.

   The Create Organization page is displayed

2. Enter data required for the organization, as indicated by the fields marked with an asterisk (*).

   From the **Type** list, select the type of organization you want. It provides the following types:

   - Company (default)
   - Department
   - Branch

     In the **Parent Name** field, you can click the magnifying glass icon to display the **Lookup Organization** lookup window.

   - Select the desired organization name and click **Select**.

     The organization name is entered in the Create Organization page.

   - Click **Create Organization**.

     The Organization Detail page is displayed. The Organization Detail page is described in "Managing Organization Details" on page 9-3.

9.2 Managing Organizations

You can enable, disable, and delete an organization, as described in the following sections:

- Searching for and Viewing Organizations
- Enabling Organizations

9.2.1 Searching for and Viewing Organizations

To search for and view existing organizations in Oracle Identity Manager:

1. In the left navigation pane, click **Organizations**, then click **Manage**.

   The Manage Organizations page is displayed.

2. Use the boxes at the top of the page to select the following search criteria:
   - **Organization Name**: This is the name of the organization.
   - **Organization Parent Name**: The organization of which this organization is a member. If an organization is displayed in the results table, it will be in the Organization Name field, which is a suborganization of the parent organization.
3. Use the Organization Type and Organization Status boxes to select the following search criteria:
   - **Organization Type**: The classification type of the organization (for example, Company, Department, Branch).
   - **Organization Status**: The current status of the organization (Active, system administrator, or Deleted).
4. Enter the appropriate value that corresponds with the search criteria, or use the asterisk (*) wildcard to query for all the organizations.

   Note: If you specify a search criterion, leave the value field blank, and click **Search Organization**, then the results displayed include NULL values from the organization table. This is because the search criterion field is not included in the query criteria at all.

   However, if you specify a search criterion, enter the asterisk (*) in the value field, and click **Search Organization**, then the results displayed include only non-NULL values of the field specified as the search criterion.

   The results page is displayed. This page lets you disable and delete an organization.

9.2.2 Enabling Organizations

To enable an organization:

1. Select the **Enable** check box and click **Enable**.

   The Confirm Enable page is displayed.

2. Click **Confirm Enable** to complete enabling this organization, or click **Cancel**.

9.2.3 Disabling Organizations

You can disable an organization only if the Organization Delete/Disable Action parameter of the System Configuration form is set to `True`. The System Configuration form is a menu option in the Oracle Identity Manager Design Console.

To disable an organization:

1. Select the **Disable** check box and click **Disable**.

   The Confirm Disable page is displayed.

2. Click **Confirm Disable** to complete disabling this organization, or click **Cancel**.

9.2.4 Deleting Organizations

You can delete an organization only if the Organization Delete/Disable Action parameter of the System Configuration form is set to `True`. The System Configuration form is a menu option in the Oracle Identity Manager Design Console.

To delete an organization:

1. Select the **Delete** check box and click **Delete**.

   The Confirm Delete page is displayed.

2. Click **Confirm Delete** to complete the deletion of this organization, or click **Cancel**.

9.3 Managing Organization Details

You can enable, disable, revoke, and provision resources to organizations and suborganizations. You can also assign administrators and administrative groups, and change administrative permissions.

To manage an organization:

1. Create a new organization as described in "Creating Organizations" on page 9-1, or do the following for an existing organization:

   a. Search for an organization as described in "Managing Organizations" on page 9-1.

   b. Click an organization name in the results table. The Organization Detail page is displayed.

2. Use the View Additional Detail about the Organization menu to view the information associated with this organization based on the following:

   - Resource Profile
   - Users
   - Sub-Organizations
   - Administrative Groups
   - Permitted Resources

   On the Organization Detail page, you can do the following:

   - **Edit**: Make changes to the organization profile.
   - **Disable**: Disable the organization from being provisioned.
   - **Delete**: Delete the organization.

3. If you view information based on the resource profile for this organization, the Resource Profile page is displayed. In the Resource Profile page, you can:

   - **Enable**: Enable a resource associated with an organization.
   - **Disable**: Disable a resource associated with an organization.

- **Revoke**: Revoke a resource associated with an organization.
- **Provision New Resource**: Provision a new resource associated with an organization

4. If you view information based on users in this organization, the Users page is displayed.

   On the Users page, you can:

   - **Enable**: Enable a user associated with an organization.
   - **Disable**: Disable a user associated with an organization.
   - **Unlock**: Unlock a user associated with an organization.
   - **Delete**: Delete a user associated with an organization.
   - **Move**: Move a user to a different organization.

5. If you view information based on the suborganization for this organization, the Sub-Organization page is displayed.

   On the Sub-Organization page, you can move suborganizations to a different organization.

6. If you view information based on administrators for this organization, the Administrative Groups page is displayed.

   On the Administrative Groups page, you can perform one of the following actions:

   - **Assign** a new administrator
   - **Create New Group**
   - **Update Permissions**
   - **Remove** groups

7. If you view information based on permitted resources for this organization, the Permitted Resources page is displayed.

   On the Permitted Resources page, you can assign and update permitted resources that are associated with an organization.

10

Creating and Managing User Groups

As an administrator, you use user groups to create and manage the records of a collection of users to whom you want to permit access to common functionality, such as access rights, roles, or permissions.

User groups can be independent of an organization, span multiple organizations, or contain users from a single organization.

Using user groups, you can:

- Designate the menu items that the users can access through the Administrative and User Console.
- Assign users or subgroups to the user groups.
- Designate status to the users so that they can specify defined responses for process tasks.
- Make modifications and request permissions for data objects.
- Designate group administrators to perform actions on groups, such as enabling members of another user group to assign members to the current user group.
- Designate provisioning policies for a user group. These policies determine if a resource object is to be provisioned to or requested for a member of the user group.
- Assign or remove membership rules to or from the user group. These rules determine which users can be assigned to the user group.

Oracle Identity Manager provides three default user groups:

- System Administrators
- Operators
- All Users

You can modify the permissions associated with the default user groups. You can also create additional user groups.

Members of the system administrators user group have full permission to create, edit, and delete records in Oracle Identity Manager, except for system records. These users can control the permissions of other users, change the status of process tasks even when the task is not assigned to them, and administer the system from the highest level.

Members of the Operators user group have access to the Organizations, Users, and Task List forms. These users can perform a subset of functions on these forms.

Members of the All Users user group have minimal permissions, including the ability to access the user's own user record. By default, each user belongs to the All Users user group.

This chapter discusses the following topics:

- Creating Groups
- Managing Groups

Note:

- A user cannot be removed from the All Users group.
- A user group, SELF OPERATORS, is added to Oracle Identity Manager by default. This user group contains one user, XELSELFREG, who is responsible for modifying user permissions for performing self-registration in the Administrative and User Console.

  Oracle recommends that you do not modify the permissions associated with the SELF OPERATORS group and do not assign users to this group.

10.1 Creating Groups

When you first create a new user group, the Group Detail page shows the group name. You can add information to a user group by using the Additional Detail menu as described in "Managing Groups" on page 10-2.

To create a user group:

1. In the left navigation pane, click **User Groups**, and then click **Create**. The Create User Group page is displayed.
2. Enter the name of the user group in the **Name** field.
3. Click **Create**. The Group Detail page is displayed.
4. Click **Edit** to modify the Group Name. Alternatively, click **Delete** to delete the user group.

10.2 Managing Groups

You can find user groups, add information to them, and perform other administrative functions for user groups.

This section discusses the following topics:

- Searching for User Groups
- Deleting User Groups
- Viewing and Administering a User Group

10.2.1 Searching for User Groups

To search for a user group:

1. In the left navigation pane, click **User Group**, then click **Manage**.

   The Manage Group page is displayed.

2. Select **Group Name** from the menu, then enter a value in the field next to the menu.

   You can use the asterisk (*) as a wildcard character to query for all user groups.

3. Click **Search**.

   The results page is displayed. In this page, you can view and delete user groups.

10.2.2 Deleting User Groups

To delete a user group:

1. Search for a group as described in "Searching for User Groups" on page 10-2.
2. Select the **Delete** check box next to the group you want to delete, then click **Delete**.

   The Confirmation page is displayed.

3. Click **Confirm Delete** to complete the deletion of this user group, or click **Cancel**.

10.2.3 Viewing and Administering a User Group

After selecting the user group that you want to view, you can view the following details about the selected user group:

- Members and Subgroups
- Menu Items
- Administrative Groups
- Access Policies
- Membership Rules
- Data Object Permissions
- Allowed Reports

10.2.3.1 Members and Subgroups

You can assign a user or a subgroup to a group. The Assign Users and Assign Sub-groups options are similar in functionality. In the following procedure, the Assign Users subgroup is used as an example.

To assign users to a group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.
2. From the additional details box, select **Members and Sub-Groups**.

   The Members and Sub-Groups page is displayed.

3. Click **Assign Users**.
4. Click **Search Users** to display a list of user names, or click **Clear**.

   The results table is displayed.

5. To increase or decrease the priority of a member, click the option associated with the member in the Increase/Decrease Priority column of the results table, and then click **Increase** or **Decrease**.

6. To remove a member of the group, click the option for the member in the Remove column of the results table, and then click **Remove Member.**
7. Select the appropriate option for the user ID, and then click **Assign**.

   The Confirmation page is displayed with the user ID names that you have just selected.
8. If you want to proceed with the user assignment, then click **Confirm Assigns**.

   Otherwise, click **Cancel**.

10.2.3.2 Menu Items

The Menu Items search criteria display all menu items that are permitted for the user group. The Menu Items option lets you assign a new menu item for the user group.

To assign menu items to a user group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.
2. From the additional details box, select **Menu Items**.

   The Menu Items page is displayed.
3. Click **Assign Menu Items**.

   The Assign Menu Items page is displayed.
4. Select the appropriate options for the menu items, and then click **Assign**.

   The Confirmation page is displayed.
5. If you want to proceed with the menu assignment, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Result table is displayed with the menu items permitted for this user group. This page also lets you delete the menu items that you do not want to permit.
6. To delete a menu item, select the option for the menu item, and then click **Delete**.

   The menu item is no longer associated with this user group.

10.2.3.3 Administrative Groups

You can view all administrative groups associated with a user group. In addition, you can:

- Assign an administrative group
- Create a new administrative group
- Update the permissions for the administrative group

Assigning an Administrative Group

To assign an administrative group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.
2. From the additional details box, select **Administrative Groups**.

The Administrative Groups page is displayed.

3. Click **Assign Administrative Groups**.

   The Assign Administrative Groups page is displayed. This page displays all the administrative groups available to be associated with the user group.

4. Select the appropriate option for the administrative group and respective permission settings for write and delete accesses, and then click **Assign**.

   The Confirmation page is displayed.

5. Click **Confirm Assign**, or click **Cancel**.

   The Result table is displayed with the administrative group that can administer the user group.

Creating an Administrative Group

To create a new administrative group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, and then click the name of a group in the results table.

   The Group Detail page is displayed.

2. From the additional details box, select **Administrative Groups**.

   Administrative Groups page is displayed.

3. You can create a new administrative group for this user group by clicking **Create New Group.**

   The Step 1: Assign Administrators page of the Assign Administrators Wizard is displayed.

4. Select the option for the user or users that you want to be in this new administrative group, and click **Add**.

   The User Login names appear in the Selected list.

5. Click **Continue**, or click **Back** or **Exit** to end the wizard.

   The Step 2: Specify Alias page is displayed.

6. Enter an alias name for the new administrative group, and then click **Continue**.

   Otherwise, click **Back** to go to the previous page or **Exit** to end the wizard.

   The Step 3: Specify Permissions page is displayed. By default, the option for Read permission is selected.

7. Select the option for the Write or Delete permission, and then click **Continue**.

   The Step 4: Verify Delegation Information page is displayed.

   This page displays the alias of the administrative group, the users who belong to this administrative group, and the permissions for the group.

8. To modify this administrative group, click **Change**.

   Clicking Change brings you back to the appropriate wizard page where you can make modifications. Otherwise, click **Continue**.

   The Administrative Groups page is displayed.

Updating Group Permissions

To update group permissions:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.

2. From the additional details box, select **Administrative Groups**.

   The Administrative Groups page is displayed.

3. To update the permission for the administrative groups associate with the user group, click **Update Permission**.

   The Update Permissions page is displayed.

   This page displays the administrative group names and permissions for write and delete access.

4. To change the permission setting for an administrative group, click the options for **Write Access** and **Delete Access**, then click **Update** to make the modifications.

   Otherwise, click **Cancel**.

   The Confirmation page is displayed. This page displays the administrative group names that you have updated.

5. If this page contains the correct names, click **Confirm Update**.

   Otherwise, click **Cancel**.

   The Administrative Groups page is displayed.

   The updated administrative group or groups are displayed with their modified write or delete access permissions.

6. To delete an administrative group, select the option for the group name, and then click **Delete**.

10.2.3.4 Access Policies

You can display all available access policies for this user group and assign and delete access policies for the user group.

To assign access policies to a user group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.

2. From the additional details box, select **Access Policies**.

   The Access Policies page is displayed.

3. To assign a new access policy, click **Assign**.

   The Assign Access Policies page is displayed.

   This page displays the policy name and brief description of the policy.

4. Select the option for access policy for the user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Confirmation page is displayed.

5. To assign the access policy, click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Access Policies page is displayed.

6. To delete this access policy, select the option for the policy, and then click **Delete**.

10.2.3.5 Membership Rules

You can display all available membership rules for this user group, assign a new membership rule for the user group, and delete membership rules.

To work with membership rules:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.

2. From the additional details box, select **Membership Rules**.

   The Membership Rules page is displayed.

3. To assign a new membership rule, click **Assign Rules**.

   The Assign Membership Rules page is displayed. This page displays the name of the membership rule.

4. Select the option for the membership rule for this user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Confirmation page is displayed.

5. To assign the membership rule, click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Membership Rules page is displayed.

6. To delete this membership rule, select the option for the membership rule, and then click **Delete**.

10.2.3.6 Data Object Permissions

Most permissions in Oracle Identity Manager concern data objects. You can define data objects as an internal object representation of tables in the Oracle Identity Manager data model. In this model, the business logic is executed and responsible for inserting, updating, and deleting data from the data store. Permissions for these actions are defined at a group level. Depending on the table or data objects, these permissions can be categorized into the following:

- Explicit Insert/Update/Delete Permission Required
- Administrative Groups
- Explicit Permission Not Required

Explicit Insert/Update/Delete Permission Required

Data objects for which explicit insert, update, or delete permission is required are the ones for which you must specify the insert, update, or delete permission by using Permissions from the Group Details list in Oracle Identity Manager Administrative and User Console to create, modify, and delete entities of these data objects.

Consider the following example: A user belongs to multiple groups and a data object is assigned to both of these groups. Suppose you want to delete an entity of this data object type. To be able to do so, you must ensure that both groups have update permission on the data object.

Table 10–1 lists the data objects listed in this category and the entities of these data objects.

Table 10–1 Data Objects Requiring Explicit Insert/Update/Delete Permissions

Data Object Type	Entities
com.thortech.xl.dataobj.tcACS	Organization.Lnk_Act_Svr
com.thortech.xl.dataobj.tcADL	Adapter Factory Logic/SetVariable tasks
com.thortech.xl.dataobj.tcADM	Adapter Factory Input/output parameters
com.thortech.xl.dataobj.tcADP	Adapter Definitions
com.thortech.xl.dataobj.tcADS	Adapter Factory Stored Procedure tasks
com.thortech.xl.dataobj.tcADT	Adapter Tasks
com.thortech.xl.dataobj.tcADU	Adapter Factory WebServices tasks
com.thortech.xl.dataobj.tcADV	Adapter Factory Variables
com.thortech.xl.dataobj.tcAPA	Attestation Process Administrators
com.thortech.xl.dataobj.tcARS	Adapter Statuses
com.thortech.xl.dataobj.tcATP	Adapter Factory Parameter Task Table
com.thortech.xl.dataobj.tcDAV	Data Object Adapter Variable
com.thortech.xl.dataobj.tcDVT	Event handlers associated with data objects
com.thortech.xl.dataobj.tcEMD	Email Definitions
com.thortech.xl.dataobj.tcERR	Error Message Definitions
com.thortech.xl.dataobj.tcEVT	Event Handlers
com.thortech.xl.dataobj.tcGPY	User Group Properties
com.thortech.xl.dataobj.tcLKU	Lookup Definitions
com.thortech.xl.dataobj.tcLKV	Lookup values for a lookup
com.thortech.xl.dataobj.tcOBA	Resource object authorizers
com.thortech.xl.dataobj.tcODF	Object To Process Data Flow
com.thortech.xl.dataobj.tcODV	Resource object Events
com.thortech.xl.dataobj.tcOOD	Resource Objects Organization Object Dependencies
com.thortech.xl.dataobj.tcOUD	Resource Objects User Object Dependencies
com.thortech.xl.dataobj.tcPDF	Process Integration Data Flow Mappings
com.thortech.xl.dataobj.tcPKH	Package Hierarchy
com.thortech.xl.dataobj.tcPOC	Access Policies Child Table Data
com.thortech.xl.dataobj.tcPOF	Policy parent data
com.thortech.xl.dataobj.tcPOG	User groups defined on access policy
com.thortech.xl.dataobj.tcPOL	Access policy definition
com.thortech.xl.dataobj.tcPOP	Assigned Objects on access policies
com.thortech.xl.dataobj.tcPRF	Process Reconciliation Field Mappings
com.thortech.xl.dataobj.tcPTY	System Configuration
com.thortech.xl.dataobj.tcPWP	Policy Process Targets

Table 10–1 (Cont.) Data Objects Requiring Explicit Insert/Update/Delete Permissions

Data Object Type	Entities
com.thortech.xl.dataobj.tcPWR	Password Policies
com.thortech.xl.dataobj.tcPWT	Policy User Targets
com.thortech.xl.dataobj.tcRAV	Prepopulate Adapter Mappings
com.thortech.xl.dataobj.tcRCA	Reconciliation Matched Organizations
com.thortech.xl.dataobj.tcRCH	Reconciliation Event Action History
com.thortech.xl.dataobj.tcRCP	Reconciliation Event Processes Matched
com.thortech.xl.dataobj.tcRCU	Reconciliation Event Users Matched
com.thortech.xl.dataobj.tcRCX	Reconciliation Exceptions
com.thortech.xl.dataobj.tcRES	Adapter Factory Resources
com.thortech.xl.dataobj.tcRGP	Group Membership Rules
com.thortech.xl.dataobj.tcRML	Task Assignment Rules
com.thortech.xl.dataobj.tcRPG	Reports on user groups
com.thortech.xl.dataobj.tcRUL	Rules
com.thortech.xl.dataobj.tcRUE	Rule Element
com.thortech.xl.dataobj.tcSDC	User defined columns on system user-defined forms
com.thortech.xl.dataobj.tcSDH	Parent child hierarchy of user defined forms
com.thortech.xl.dataobj.tcSDL	Form Definition Version Label
com.thortech.xl.dataobj.tcSDP	Form Definition Properties
com.thortech.xl.dataobj.tcSPD	IT Resources Type Parameter Definition
com.thortech.xl.dataobj.tcSRE	Association between user defined columns and pre-populate adapters
com.thortech.xl.dataobj.tcSRS	IT Resource Link
com.thortech.xl.dataobj.tcSUG	IT Resources Administrators
com.thortech.xl.dataobj.tcSVD	IT Resources Type Definition
com.thortech.xl.dataobj.tcTDV	Process Event Handlers
com.thortech.xl.dataobj.tcTLG	System Log
com.thortech.xl.dataobj.tcTSA	Schedule Task Attributes
com.thortech.xl.dataobj.tcTSK	Scheduled Tasks
com.thortech.xl.dataobj.tcUHD	Users Objects History Details
com.thortech.xl.dataobj.tcUPL	User Defined Field Lookups
com.thortech.xl.dataobj.tcUPT	User Defined Field Values
com.thortech.xl.dataobj.tcUPY	System Configuration Users
com.thortech.xl.dataobj.tcWIN	Form Information

Administrative Groups

These data objects do not use permissions that are defined using Permissions in the Group Details list of the Oracle Identity Manager Administrative and User Console.

They follow administrator concepts in which you define certain groups as administrators. Table 10–2 lists these data objects and their permissions.

Table 10–2 Data Object Permissions for Administrative Groups

Data Object Type	Entities	Permissions
com.thortech.xl.dataobj.tcUSR	Users	Permissions for users are defined at the organization level. If you define a group as an administrator of an organization with read, write, and delete permissions, then users in this group are able to view user details, modify user details, or delete users.
com.thortech.xl.dataobj.tcACT	Organizations	If you define a group as an administrator of an organization, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View user details in the organization ■ View organization details, such as the organization type and the parent organization of that organization With Write permissions: ■ Update attributes of any users in that organization ■ Update organization attributes ■ Cannot delete users from the organization With Delete permissions: ■ Delete users in that organization ■ Delete organization ■ Cannot update user attributes
com.thortech.xl.dataobj.tcUGP	User Groups	If you define a group as an administrator of another group, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View group attributes ■ View group members ■ Cannot add or remove group members With Write permissions: ■ Add or remove group members ■ Switch priority between group members ■ Update group attributes With Delete permissions: ■ Delete the group

Table 10–2 (Cont.) Data Object Permissions for Administrative Groups

Data Object Type	Entities	Permissions
com.thortech.xl.dataobj.tcOBJ	Resource Objects	If you define a group as an administrator of a resource, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View resource attributes ■ View the list of users or organizations that are provisioned with the resources ■ View the list of administrators and authorizers ■ View resource audit objectives With Write permissions: ■ Update resource attributes ■ Assign or remove resource administrators and update their permissions ■ Cannot assign or remove resource authorizers or update their priority ■ Cannot add resource audit objectives With Delete permissions: ■ Cannot delete the resource
com.thortech.xl.dataobj.tcAPD	Attestation Process Definitions	If you define a group as an administrator of an attestation process, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View attestation process definition ■ View administrators and execution history With Write permissions: ■ Update the attestation process definition ■ Cannot assign or remove administrators and update their permissions ■ Can disable or enable the attestation process definition With Delete permissions: ■ Delete the attestation process
com.thortech.xl.dataobj.tcQUE	Administrative Queues	If you define a group as an administrator of an administrative queue, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View or read administrative queue definitions With Write permissions: ■ Update queue definition ■ Add or delete queue members ■ Add or update administrators and their permissions With Delete permissions: ■ Cannot delete the queue

Table 10–2 (Cont.) Data Object Permissions for Administrative Groups

Data Object Type	Entities	Permissions
com.thortech.xl.dataobj.tcTOS	Process Definition	If you define a group as an administrator of a process definition, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ View the workflow process With Write permissions: ■ Update the workflow definition ■ Add, modify, or delete tasks from the workflow definition ■ Update or remove administrators The deletion of workflow definitions is not supported.
com.thortech.xl.dataobj.tcSDK	Form Designer	If you define a group as an administrator of a form, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ Read or view user defined form definition With Write permissions: ■ Update the form definition attributes ■ Add new versions ■ Update or delete administrators and their permissions ■ Cannot add new fields to the form ■ Cannot add or update existing field properties ■ Cannot add prepopulate adapters to any fields The deletion of user-defined forms is not supported.
com.thortech.xl.dataobj.tcSVR	IT Resources	If you define a group as an administrator of an IT resource, then the users of this group can perform the following actions based on the permissions assigned: With Read permissions: ■ Read or view the IT resource details including parameters With Write permissions: ■ Update the IT resource definition and parameters ■ Cannot add or update administrators and their permissions With Delete permissions: ■ Delete an IT resource instance

If you define a group as an administrator of any of the entities in Table 10–2 with read, write, and delete permissions, then the users in this group can view entity details, modify entity details, or delete entities.

Whenever an entity of the data object types listed in Table 10–2 are created by a user, the groups that the user belongs to are automatically defined as administrators of the newly formed entity with read, write, and delete permissions.

For example, user1 belonging to groups Group1 and Group2 creates an entity of type com.thortech.xl.dataobj.tcACT, which is an organization. Group1 and Group2 are

automatically made administrators of this newly created organization with read, write, and delete permissions.

Explicit Permission Not Required

Data objects for which explicit permission is not required are the ones for which permissions do not need to be defined because either there are no permissions enforced or they simply follow parent data object permissions. Data objects that use parent data object permissions follow a simple paradigm that if a group has update permissions on a parent data object, the same group will have insert, update, and delete permissions on child data objects. Table 10–3 lists these data objects and their entities.

Table 10–3 Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
Com.thortech.xl.dataobj.tcMEV	Email definitions defined on task statuses	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcMIL	Process task definitions	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcRSC	Process task response codes	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcUNM	Undo milestones	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcRPC	Reconciliation Matched Processes Child Table	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcAAD	Organization Administrators	Follows parent data object (ACT) permissions.
Com.thortech.xl.dataobj.tcRCE	Reconciliation events	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcPCQ	User Questions	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcUSG	Users in a group	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcGPP	Group administrators	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcUWP	User Groups.Navigation Tree Layout	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcFUG	User Defined Field Definition.Administrators	Follows parent data object (SDK) permissions.
com.thortech.xl.dataobj.tcMAV	Process Data.Milestone.Adapter Variable	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcAtomic Process	Process Definition	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcATR	Attestation Requests	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIF	Export Import File history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcCIH	Connector Installation history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcORR	Reconciliation Action Rules	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRRE	Reconciliation User Matching Elements	No permission check. Always returns true.

Table 10–3 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcRPW	Password Policy Rules on resources	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcOBD	Resource Object Dependencies	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcACP	Objects allowed	Follows parent data object (ACT) permissions.
com.thortech.xl.dataobj.tcRCM	Reconciliation Data Multi-Value	No permission check. Always returns true.
com.thortech.xl.dataobj.tcATD	Attestation Task Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcOST	Statuses defined on resource	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcEIS	Export import history substitution	No permission check. Always returns true.
com.thortech.xl.dataobj.tcAPT	Attestation Tasks	No permission check. Always returns true.
com.thortech.xl.dataobj.tcGCD	Generic Connector Definition	No permission check. Always returns true.
com.thortech.xl.dataobj.tcDEP	Process Task Dependencies	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcROP	Process determination rules	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcGPG	Sub groups	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcSEL	User Groups.Set Up Permissions	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcQUM	Queue Members	Follows parent data object (QUE) permissions.
com.thortech.xl.dataobj.tcQUG	Queue Administrators	Follows parent data object (QUE) permissions.
com.thortech.xl.dataobj.tcMSG	Milestone.Status.User Group	This data object has been deprecated.
com.thortech.xl.dataobj.tcPUG	Process Integration.Administrators	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcOUD	Resource Objects.User Object Dependencies	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRQE	Request Queues	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRVM	Recovery Milestones	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcOUG	Resource Objects.Administrators	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcMST	Process Definition.Tasks.Object Status	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcRRT	Reconciliation.User Matching Rule Element Properties	No permission check. Always returns true.
com.thortech.xl.dataobj.tcSVP	IT Resource Properties table	Follows parent (SVR) permissions.
com.thortech.xl.dataobj.tcORF	Resource Objects.Object Reconciliation Fields	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRCD	Reconciliation Event Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIO	Export and import objects	No permission check. Always returns true.

Table 10–3 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcRRL	Reconciliation Rules	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRQC	Requests.Comments for Requests	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRCB	Reconciliation Events.Unprocessed Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcPXD	Proxy Definitions	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIH	Export and import history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcMAP	Map Information	Not using maps any more.
com.thortech.xl.dataobj.tcORC	Process Detail	Permissions are given to all users group.
com.thortech.xl.dataobj.tcSTA	Process task status Definitions	We do not allow define custom statuses on tasks.
com.thortech.xl.dataobj.tcScheduleItem	Process task instances	Permissions are given to all users group.
com.thortech.xl.dataobj.tcSCH	Task instance information	Permissions are given to all users group.
com.thortech.xl.dataobj.tcOIO	Requests Object Instance for Organization	Users can never directly create these entities.
com.thortech.xl.dataobj.tcOIU	Requests Object Instance for User	Users can never directly create these entities.
com.thortech.xl.dataobj.tcOBI	Requests.Object Instance	Users can never directly create these entities.
Com.thortech.xl.dataobj.tcREQ	Requests	No permission check for insert. Update and delete permissions are computed using the user relationship to request.
com.thortech.xl.dataobj.tcRequestObject	Request Object	No permission check. Always returns true.
com.thortech.xl.dataobj.tcDOB	Data Objects	OIM Users never create data objects.
Thor.CarrierBase.tcACN	Contacts.Organization Information	Not used anymore.
Thor.CarrierBase.tcAFM	Adapter Factory.Form	Not used anymore.
Thor.CarrierBase.tcAHY	Organization.Parent-Child	Not used anymore.
Thor.CarrierBase.tcCCG	Contact.Organization Groups	Not used anymore.
Thor.CarrierBase.tcESD	Structure Utility.Encrypted Columns	No UI or APIs exposed to define data.
Thor.CarrierBase.tcGSC	Contact.Schedule Items	Not used anymore.
Thor.CarrierBase.tcGSI	Schedule Items.User Groups	Not used anymore.
Thor.CarrierBase.tcPGP	Process Integration.Request Permissions	Not used anymore.
Thor.CarrierBase.tcUDF	User Defined Field Definition	Not used anymore.
com.thortech.xl.orb.dataobj.tcAOA	Adapter Factory.Open Adapter	Not used anymore.

Table 10–3 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.orb.dataobj.tcOrganizationContact	Organization.Contact Information	Not used anymore.
com.thortech.xl.orb.dataobj.tcRPT	Report Definition	Not used anymore.
com.thortech.xl.dataobj.tcRPP	Report Parameters	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSC	Task Instance.Contact Information	Not used anymore.
com.thortech.xl.orb.dataobj.tcUserScheduleItem	User Tasks	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSI	Users.User Defined Tasks	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSK	Email Notification.USI.Contacts	Not used anymore.
com.thortech.xl.dataobj.tcAAG	User Groups.Organization Members	Not used anymore.
com.thortech.xl.dataobj.tcORD	Orders	Not used anymore.
com.thortech.xl.dataobj.tcRLO	External JAR File Directory	Not used anymore.
com.thortech.xl.dataobj.tcAGS	Organization.Contact groups	Not used anymore.
com.thortech.xl.dataobj.tcATS	Organization.Services Per Organization	Not used anymore.
com.thortech.xl.dataobj.tcSGK	System Generator Key Values	Not used anymore.
com.thortech.xl.dataobj.tcSRP	Service Rate plan	Not used anymore.
com.thortech.xl.dataobj.tcSRS	Service Rate plan	Not used anymore.
com.thortech.xl.dataobj.tcUDP	User Defined Fields	Not used anymore.
com.thortech.xl.dataobj.tcUPD	Users Objects Policy Details	Users can never directly create these entities.
com.thortech.xl.dataobj.tcUPP	Users Objects Policy Profile	Users can never directly create these entities.
com.thortech.xl.dataobj.tcUPH	Users Objects Policy History	Users can never directly create these entities.
com.thortech.xl.dataobj.tcRQU	Request Object Target User Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQA	Request Target Organization Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQO	Request Object Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRIO	Request Organizations Resolved Object Instances	Follows associated request permissions.
com.thortech.xl.dataobj.tcRIU	Request Users Resolved Object Instances	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQY	Request Organizations Requiring Resolution	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQZ	Request Users Requiring Resolution	Follows associated request permissions.
com.thortech.xl.dataobj.tcUserProvisionObject	User Provision Object	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcOrgProvisionObject	Organization Provision Object	Follows parent (OBJ) permissions.

Table 10–3 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
Com.thortech.xl.dataobj.tcMEV	Email definitions defined on task statuses	Follows parent (TOS) permissions.

While assigning data objects or fine-grained permissions to groups, Oracle Identity Manager uses the following permission model:

- Assigning a data object to a user without any insert/update/delete option results in an error.
- To assign a data object to a group with, say insert and update permissions, a user who is logged in must have insert and update permissions on that data object.
- In order to modify any data permission (insert/update/delete) on a group, a user who is logged in must have the same permissions on that data object.
- To be able to delete a data object permission from a group, a user who is logged in must have insert and update permissions on the same data objects.
- If a user who is logged in updates data object permissions that result in no permissions on a data object, the system automatically deletes that entry from the group.

Menu Items and Group Entitlements

Using Oracle Identity Manager, you can also assign permissions in the form and menu item levels. Form-level permissions can be assigned in the Design Console and menu item-level permissions can be assigned in the Administrative and User Console. However, assigning permissions on the forms or menu items does not automatically grant a user access to the entities associated with the forms or menu items (for example, if you grant permission to a user for the Manage Users menu item).

When the user logs in, the menu item will be visible. In addition, when you search for the users, you might not get any results because you might not be assigned permission to view users belonging to a certain group. This permission can be defined in the Administrative and User Console. To assign or remove a menu item or group entitlement, a user must have the corresponding menu item or group entitlement assigned to one of the groups to which he or she belongs.

10.2.3.7 Allowed Reports

You can list the reports that group members are allowed to run, and select reports for the group.

To work with reports permissions for a group:

1. Search for a group as described in "Searching for User Groups" on page 10-2, then click the name of a group in the results table.

   The Group Detail page is displayed.

2. From the additional details box, select **Allowed Reports**.

   The Reports page is displayed.

3. To provide access to new reports for users, click **Assign Reports**.

   The Assign Reports page is displayed. This page displays available report names and types.

4. Select the option for the report, and then click **Assign**, or click **Cancel**.

The Confirmation page is displayed.

5. To assign the report, click **Confirm Assign**.

   The Reports page is displayed.

6. To delete a report, select the option for the report, and then click **Delete**.

11

Creating and Managing Access Policies

Access policies are a list of user groups and the resources with which users in the group are to be provisioned or deprovisioned. Access policies are defined using the Access Policies menu item in the Oracle Identity Manager Administrative and User Console.

This chapter describes how to create and use access policies for users, organizations, and resources in Oracle Identity Manager.

This chapter discusses the following topics:

11.1 Features of Access Policies

This section describes the various features offered by the policy engine.

Provisioning Options

While defining policies, you can specify whether you want resources in a particular policy to be provisioned with or without approval. If an access policy of type *with approval* is applied to a user and if the access policy specifies that resources be provisioned, then Oracle Identity Manager generates a request. This request must be approved before the user gets the resources. Without the approval option, whenever an access policy is applied, the resources are directly provisioned to the user without any request being generated.

Revoking the Policy

Oracle Identity Manager access policies are not applied to subgroups. Policies are only applied to direct-membership users (that is, users who are not in subgroups) in the groups that are defined on the access policies. You can specify if a resource in a policy must be revoked when the policy no longer applies. If you do so, then these resources are automatically revoked from the users by Oracle Identity Manager when the policy no longer applies to the users.

Denying a Resource

While creating an access policy, you can select resources to be denied along with resources to be provisioned for groups. If you first select a resource for provisioning and then select the same resource to be denied, then Oracle Identity Manager removes the resource from the list of resources to be provisioned. If two policies are defined for a group in which one is defined to provision a resource and the other is defined to

deny the resource, then Oracle Identity Manager does not provision the resource irrespective of the priority of the policies. If policies are defined to deny resources to users belonging to a group, then the resources will not be made available for selection during request-based or direct provisioning to these users.

Evaluating Policies

In Oracle Identity Manager, access policies can be evaluated in the following scenarios:

- When a user is made a part of a group or removed from a group

  The policy for the user is evaluated as part of the add or remove operation.

- If the retrofit flag is set for the policy

  These evaluations do not happen immediately after the action. Instead, they happen during the next run of the `Set User Provisioned Date` schedule task. The evaluations can happen in the following scenarios:

  – Policy definition is updated so that the retrofit flag is set to ON. Policies are evaluated for all applicable users.

  – A group is added or removed from the policy definition. Policies are evaluated only for users of the group that is added or removed.

  – A resource is added, removed, or the Revoke If No Longer Applies flag value is changed for the resource. Policies are evaluated for all applicable users.

  – When policy data is updated or deleted. This includes both parent and child form data. Policies are evaluated for all applicable users.

Access Policy Priority

Policy priority is a numeric field containing a number that is unique for each access policy you create. The lower the number, the higher is the priority of the access policy. For example, if you specify Priority =1, it means that the policy has the highest priority. When you define access policies through the Administrative and User Console, the value 1 is always added to the value of the current lowest priority and the resultant value is automatically populated in the Priority field. Changing this value to a different number might result in readjusting the priority of all the other access policies, thus ensuring that the priorities remain consistent. The following actions are associated with the priority number:

- If the priority number entered is less than 1, then Oracle Identity Manager will change the value to 1 (highest priority).
- If the priority number entered is greater than M, in which M is the current lowest priority, then Oracle Identity Manager will specify the value as less than or equal to M+1.
- Two access policies cannot have the same priority number. Therefore, assigning an already existing priority number to an access policy will lower the priority by 1 for all policies of lesser priority.

Conflicts can arise from multiple access policies being applied to the same user. Because a single instance of a resource is provisioned to the user through access policies, Oracle Identity Manager uses the highest priority policy data for a parent form. For child forms, Oracle Identity Manager uses cumulative records from all applicable policies.

Access Policy Data

There are multiple ways in which process form data is supplied for resources during provisioning. The following is the order of preference built into Oracle Identity Manager:

1. Default values from the form definition
2. Organization defaults
3. Values obtained through data flow from object form to process form
4. Prepopulate adapters
5. Access policy data if resource is provisioned because of a policy
6. Data updated by Process Task or Entity Adapters

If a given option is available, then the rest of the options that are at a lower order of preference are overridden. For example, if Option 4 is available, then Options 3, 2, and 1 are ignored.

11.2 Creating Access Policies

You can define an access policy for provisioning resources to user groups and users by using the Access Policy Wizard.

To create an access policy:

1. To open the Create Access Policies page, in the left pane of Administrative and User console, click **Access Policies.**
2. Click **Create**.

   The Create Access Policy page is displayed.
3. Enter information in the required fields indicated with an asterisk (*).

   Select **With Approval** to require a defined approver or proxy user to approve the resource to be provisioned to the user or group.

   Select **Without Approval** if no approval is required.
4. Select **Retrofit Access Policy** to retrofit this access policy when it is created.

   Note: If you select Retrofit Access Policy, then the access policy is applied to all existing users of the groups that you select in Step 12 of this procedure.

   If you do not select this option, then existing group memberships are not taken into consideration.
5. Click **Continue**.

   The Create Access Policy - Step 2: Select Resources (to provision) page is displayed.
6. Specify the resource to be provisioned for this access policy.

   Search for resources by using the filter search menu.

   - Select the name of the resource from the results table, and then click **Add**.

- The names of the desired resources to provision appear in the Selected list. If you want to create an access policy that only denies resources, click **Continue** without selecting a resource.
- To unassign the selected resources, highlight the resource in the Selected list and click **Remove**.

7. Click **Continue**.

   If there is a form associated with this resource, the subsequent pages display the required fields. Otherwise, the Create Access Policy - Step 2: Select Resources to Revoke page is displayed. It is strongly recommended that you do not specify policy defaults for passwords and encrypted attributes.

8. Specify whether or not access policies are to be revoked if they no longer apply.

   Select the check boxes for the resources you want to revoke automatically from the results table.

9. Click **Continue**.

   The Create Access Policy - Step 3: Selected Resources (to deny) page is displayed.

10. Use this page to select resources to be denied by this access policy.

    To select resources to be denied:

    a. Select the resources from the results table.

    b. Click **Add** to place the resource in the Selected list.

       You must select at least one resource to deny if you have not selected any resources to be provisioned. Selecting the same resources to be denied as to be provisioned will automatically unassign them from the resources to be provisioned selection.

       Similarly, in Step a, assigning the same resources to be provisioned as you have already selected to be denied will automatically remove them from the resources to be denied selection. You can remove the resources that were selected to be denied. You do this by selecting those resources from the **Selected** list, and clicking **Remove**.

    c. Click **Continue**.

    The Create Access Policy - Step 4: Select Group page is displayed.

11. Use the Create Access Policy - Step 4: Select Group page to associate a group with the access policy.

12. To associate a group with this access policy:

    - Select the group from the results table, and then click **Add**.
    - The name of the selected group is displayed in the **Selected** field. You can delete the group name by using the **Remove** button.
    - You can specify user groups for this access policy. You can search for the required user groups by using the filter search menu.
    - Select the user groups from the results table, and then click **Add**. You must select at least one user group. The names of the selected user groups appear in the Selected list.
    - You can unassign the selected user groups by highlighting the resource in the Selected list and then clicking **Remove**.

13. Click **Continue.**

The Create Access Policy - Step 5: Verify Access Policy Information page is displayed.

14. If you want to modify any of the selections you made in the preceding steps of this procedure, then click **Change** to go to the corresponding page of the wizard. After making the required modifications, click **Continue** to return to the Step 5: Verify Access Policy Information page.

15. Click **Continue** to create the access policy.

Note: When you create an access policy on a resource having a process form with Password field, the password policy is not evaluated. For information about password policies, see *Oracle Identity Manager Design Console Guide*.

11.3 Managing Access Policies

You can use the Administrative and User Console to modify information in existing access policies.

To manage access policies:

1. Click **Manage** under the Access Policies menu.

   The Manage Access Policies page is displayed.

   Use the menu in the search criteria field to select an access policy attribute. You can use the asterisk (*) wildcard character to search for all access policy instances that have any value for the attribute selected. Click **Search Access Policies**.

   The Manage Access Policies page is displayed with your search results.

2. To view the details of the Access Policy you want, click **Access Policy Name**.

   The Access Policy Details page is displayed.

   To make modifications to this access policy, use the **Change** link at the end of each selection category.

3. After you make the required modifications, click **Update Access Policy**.

   This access policy is updated, and the updated information is displayed on the Access Policy Details page.

12

Working with Resources

The Resource Management features of the Administrative and User Console enable you to manage resource objects for an organization or individual user. Managing resources includes the following activities:

- Searching for and viewing the details of a resource
- Disabling, enabling, and revoking a resource from users or organizations
- Managing resource administrator and authorizer groups
- Viewing, creating, and modifying workflows
- Creating and managing IT resources
- Creating and managing scheduled tasks

This chapter includes the following topics related to managing resources:

12.1 Viewing Resource Details

To view the details of a resource:

> **Note:** As described in the following procedure, when performing a search, if you select a value from a list and do not enter a corresponding search value, then an error occurs. In addition, if you select the same value twice from the lists, then an error occurs.

1. In the Administrative and User Console, click **Resource Management**, and then click **Manage**.

The Resource Search page is displayed.

2. Use the fields at the top of the page to select the search criteria, and enter the corresponding search value in the adjoining field or use the asterisk (*) wildcard character. To use the Resource Type and Target criteria, select a value from the corresponding box.
3. From the Resource Audit Objective list, select the required option.

   The Resource Audit Objective list lets you group resources by any data type. You can select multiple values for the same resource. You can also add audit schedule values for quarterly, semiannual and annual reviews in the list of values of the field, and select a combination, such as SOX and quarterly, as audit requirements.

   The predefined values in the Resource Audit Objective list are as follows:

   - SOX (Hosts Financially Significant Information)
   - HIPAA (Hosts Private Healthcare Information)
   - GLB (Hosts Non-Public Information)
   - Requires Quarterly Review
   - Requires Annual Review
4. Click **Search**.

   The results table is displayed.
5. Click the name of a resource. For example, you can select a resource named Oracle Identity Manager User.

   The Resource Detail page is displayed.
6. To view detailed information about the resource, use the menu.

   Detailed information that you can view includes the following:

   - Organization Associated With This Resource
   - Resource Administrators
   - Resource Authorizers

12.2 Working with Organizations Associated with Resources

You can enable, delete, and revoke resources that are associated with an organization. You can also determine mapping categories for resources that are provisioned more than once to an organization.

To work with an organization that is associated with a resource:

1. Perform Steps 1 through 3 of the procedure described in the "Viewing Resource Details" section on page 12-1.
2. Select the **Organization Associated For the Resource** option.

   The Organization Associated For the Resource page is displayed.
3. Use the options to filter the list of associated organizations.

   Selecting the **All** option lists all the organizations. The By Status option filters the organizations on the basis of values in the Resource Status column. The organizations associated with the resource are listed under the Organization Name column. The resource status in this case, indicates that the resource is provisioned

for each of the organizations listed. To modify the resource for the organization, select one of the following:

- Enable
- Disable
- Revoke

The value in the Identifier column corresponds with a field type that you can map from the Process Definition form in the Design Console by using the Map Descriptive Field. This value lets you distinguish which mapping category is defined, such as Process Type, Organization Name, or Request Key, when the same resource has been provisioned several times to the same organization.

12.3 Using the Resource Administrator Option

On the Resource Detail page, select **Resource Administrator**. The Resource Administrators page displays the names of groups that are assigned as administrators to this resource. This page also displays the Write Access and Delete Access permissions. These are permissions that the administrator groups have on the resource, but not with resource parameters. Write access allows the group to make changes to the resource. Delete access allows the group to delete the resource.

You can perform the following operations:

- Assigning User Groups as Administrators for Resources
- Creating Administrator Groups
- Updating Permissions of an Administrative Group

12.3.1 Assigning User Groups as Administrators for Resources

To assign a user group as administrators for resources:

1. Click **Assign**.

   The Assign Administrators page is displayed.

   This page displays all group names that can be assigned to this resource. Select the options to activate the write and delete access and assign the group to this resource.

2. Click **Assign**.

   The Confirm Assign page is displayed. This page displays the new user groups assigned to this resource.

3. Click **Confirm Assign** or click **Cancel**.

   The Resource Administrators page is displayed with a list of all group names associated with this resource. You can modify this information.

12.3.2 Creating Administrator Groups

To administer a resource, you can create a group by using the Delegated Administrator Wizard.

Note: When you create a group, if you belong to other groups with write and delete access, then these other groups become administrative groups for the new group. This rule is applied even when you create an organization.

To create a new group:

1. Expand **Resource Detail**, click **Resource Administrator**, and then click **Create New Group**.

   The Assign Administrators – Step 1: Assign Administrators page is displayed.

   In the results table, click the user login names that you want in the administrative group, and then click **Add**.

   The names appear in the Selected display panel.

   Click **Continue**, or click **Exit** to end the wizard.

   The Assign Administrators – Step 2: Specify Alias page is displayed.

2. Enter the alias name for the administrator group, and click **Continue**.

   Otherwise, click **Back** to return to the previous page, or click **Exit** to end the wizard.

   The Assign Administrators – Step 3: Specify Permissions page is displayed.

3. Select the **Write** and **Delete** options to assign these permissions to the administrator group, then click **Continue**.

   Otherwise, click **Back** to return to the previous page, or click **Exit** to end the wizard.

   The Assign Administrators – Step 4: Verify Delegation Information page is displayed.

4. To make a change to the information you entered in the previous steps, click **Change**.

   After verifying your changes, click **Continue**. Click **Back** to return to the previous page, or click **Exit** to end the wizard.

   The Resource Administrator page is displayed. The new group is added to the results table.

12.3.3 Updating Permissions of an Administrative Group

You can update the permissions of an administrative group.

To update the permissions:

1. Click **Update Permissions**.

   The Update Administrators page is displayed.

2. To change the permission setting for an administrative group, click the options for write and delete access.

3. Click **Update** to make the modifications, otherwise, click **Cancel**.

   The Confirmation page is displayed. It displays the administrative group names that you updated.

4. If these are the correct names, click **Confirm Update**, otherwise, click **Cancel**.

12.4 Using the Resource Authorizers Option

You can determine which user groups are authorized to provision the resource.

To determine the resource authorizer:

1. On the Resource Detail page, select **Resource Authorizer** from the menu.

   The Resource Authorizers page is displayed.

2. To set the level of priority for authorizing this resource, select **Increase/Decrease Priority**.

3. To delete the authorizer of this resource, select the appropriate **Group Name** option, and then click **Delete**.

4. To add additional user groups to authorize resources, click **Assign**.

   The Assign Authorizers page is displayed.

5. Select the appropriate group name option and click **Assign**, otherwise, click **Cancel**.

   The Confirmation page is displayed.

6. If the information is correct, click **Confirm Assign**, otherwise, click **Cancel**.

   The Resource Authorizers page is displayed. Note that the group name that you assigned to this resource is added to the results table.

12.5 Using the Resource Workflows Option to View Workflows

The Resource Workflows option in the Administrative and User Console consists of the Workflow Visualizer and the Workflow Designer. Using the Workflow Visualizer, you can view workflows. Using the Workflow Designer, you can create and edit workflows. This section discusses the Workflow Visualizer.

See Also: "Using the Resource Workflows Option to Create and Modify Workflows" on page 12-17

The Workflow Visualizer tool provides a visual representation of task sequences, dependencies, and other components of a workflow definition. The visual representation provides an overview of the workflow, its relationships, and the task components that constitute the flow. You can also print the workflow view.

The Workflow Visualizer tool displays processes of types Approval and Provisioning. You use the Approval type process to approve the provisioning of Oracle Identity Manager resources to users or organizations. Unlike provisioning processes, approval processes usually consist of tasks that must be completed manually. The Provisioning type process is used to provision Oracle Identity Manager resources to users or organizations.

Note: To access the Workflow Visualizer, the Nexaweb applet requires your Web browser configuration to use Java Virtual Machine 1.4.2.*x*.*x*.

This section includes the following topics:

- Opening the Workflow Visualizer
- Elements of the Workflow Visualizer

- Operations on the Workflow Visualizer

12.5.1 Opening the Workflow Visualizer

To open the Workflow Visualizer:

1. On the Resource Detail page, select **Resource Workflows** from the list.

   The Resource Workflows page is displayed. This page displays the resource name and a table that lists the names of the workflow definitions for this resource.

2. To render the workflow definition into a graphic flowchart, select the required workflow.

   A graphical representation of the workflow definition is displayed in a new window.

12.5.2 Elements of the Workflow Visualizer

For provisioning workflows, multiple tabs are displayed on the Workflow Designer page. For approval workflows, a single workflow is displayed on the Workflow Designer page with no tabs on the page.

> **See Also:** "Overview of the Resource Model" on page 1-2 for information about provisioning and approval processes

The Approval Workflow Definition is displayed as one workflow that represents the entire approval process. Provisioning workflows can have forms associated with them, and the workflow details header shows the form name. Approval workflows do not have forms associated with them, and therefore, the workflow details header shows no information on the form.

Table 12–1 lists the information fields in the Workflow Visualizer.

Table 12–1 Information Fields in the Workflow Visualizer

Field	Description
Workflow Name	The name of the Process Definition.
For Resource	The name of the Object (resource object that is either approved or provisioned).
Workflow Type	The Process Definition type (Approval or Provisioning). The type also indicates whether or not the workflow is the default for the resource.
Form Name	The name of the form associated with a provisioning workflow. In case of an approval workflow, this information is not shown.

Table 12–2 describes the toolbar menu items in the Workflow Visualizer.

Table 12–2 Toolbar Menu items in the Workflow Visualizer

Field	Description
Display Option	This option lets you view the elements on the page. You can show or hide the elements on the page, which helps in keeping the page uncluttered.
	Display Unknown Response Code: The Unknown Response Code is defined for every task in the workflow. It is not used in the logic of the workflow. However, you can use this option to display the Unknown Response Code.
	Display Adapter Name On-Screen: You can display the name of the automated adapter.
	Display Undo Tasks: You can display the undo tasks for the tasks.
	Display Recovery Tasks: You can display the recovery tasks for the tasks.

Table 12–2 (Cont.) Toolbar Menu items in the Workflow Visualizer

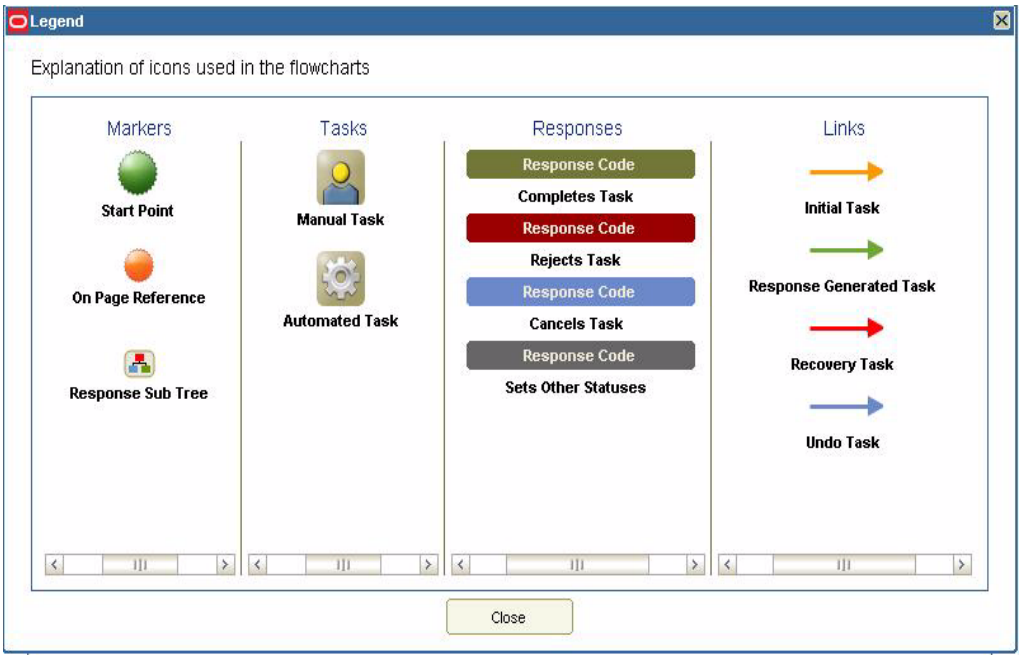
Field	Description
Generate Image	This option enables you to save the workflow view as an image that can be printed. When you click this menu item, a new browser window opens and it displays a JPEG formatted image. The entire workflow is displayed, even parts of the flowchart that are hidden due to scrolling limitations of the display area. You can then use the standard Web browser features to save the image on your computer.
Reload Workflow	This option refreshes the workflow view and rearranges the different items on the page based on a predefined graph algorithm.

Table 12–2 (Cont.) Toolbar Menu items in the Workflow Visualizer

Field	Description
Legend	This option provides an explanation of all the visual components that are used to create the flowchart of the workflow definition. Figure 12–1 shows the Legend page. **Markers** The Markers nodes represent position markers for special conditions. These conditions are: Start Point: This marker represents the logical start point within the workflow. It is not an actual task within the workflow definition. On-Page Reference: This marker represents a task node that has already been drawn somewhere else in the workflow chart. It is used to show connectivity to other tasks without crowding the workflow view with crossing links. Response Sub-Tree: The Response Sub-Tree (Expansion Nodes) helps keep the workflow uncluttered by hiding significant subtrees of response nodes. You can double-click the Expansion Node marker to redraw the flowchart with the responses. **Tasks** The Tasks nodes represent the tasks in the workflow. They are: Manual Tasks: These tasks require user action in order to be completed. Approval processes are generally composed of manual tasks. Automated Tasks: These tasks do not require user interaction in order to be completed. Automated tasks always require a process task adapter. Provisioning processes generally consist of automated tasks. **Responses** The Response nodes represent the response codes that are defined on the tasks. The Response node shows the actual response code within it. The response code is based on the status that the response has set on the task. Completes Task: The process task has been completed, and this is indicated in green color. Rejected Task: The process task has been rejected, and this is indicated in red color. Cancels Task: The process task has been canceled, and this is indicated in blue color. **Links** Direction arrow lines connect the task and response nodes and indicate the flow of the workflow. The color of the link indicates the type of relationship between two nodes that it connects. The types of links are: Initial Task: The Initial Task is the first process task in the workflow definition. Response Generated Task: The Response Generate Task is defined as a process task that is triggered when the current task has the Completed status. In general, a new process task can be triggered when the conditional task receives a particular response code in conjunction with the running of the process task. Recovery Task: The Recovery Task is defined as a process task that is triggered when the current process task has the Rejected status. Undo Task: The Undo Task is defined as a process task that is triggered when the current process task has the Canceled status. Dependent Task: The Dependent Task is defined as a process task that is dependent on another process. Oracle Identity Manager can start this type of task only when the process task on which it is dependent is completed.

Figure 12–1 shows the Legend page.

Figure 12–1 Legend Page



In addition to the Information Fields and Toolbar Menu Items of the Workflow Visualizer, the UI elements of the workflow are tasks and responses. For information about tasks and responses, see Table 12–1 on page 12-6 and the "Creating and Configuring Tasks and Responses" section on page 12-31.

12.5.2.1 Using the Provisioning Workflow Definition Event Tabs

The Provisioning Workflow Definition is displayed with associated event tabs of the logical flow of the way tasks get executed based on their responses. The event tabs represent the various task sequences for a specific event in the workflow definition. When you click an event tab, it displays the appropriate tasks for the workflow event of the process. You can arrange the flowchart to meet your requirements. If there is no task defined for the workflow event, then the tab displays a blank view. If there is more than one task sequence for the workflow event type, then the tab displays a menu from which you can select the process flowchart that you want to view.

12.5.2.1.1 Provisioning Tab The Provisioning tab shows the tasks that will provision a resource. When the workflow type is Provisioning, the workflow shows all the tasks needed to provision a resource.

12.5.2.1.2 Reconciliation Tab The Reconciliation tab shows the reconciliation event for the provisioning process with marker tasks inserted into it: either `Reconciliation Insert Received`, `Reconciliation Update Received`, or `Reconciliation Delete Received`. These tasks can have adapters attached to them to start a provisioning action. If a task has no adapters attached to it, then a response code of `Event Processed` is assigned to the task. Additional provisioning process tasks can be generated based on this response code to start a provisioning flow due to the reconciliation event.

12.5.2.1.3 Service Account Tab The Service Account tab shows all the provisioning processes of service accounts for users (administrators). When a user is provisioned with a service account, Oracle Identity Manager manages a mapping from the user's identity to the service account. When the resource is revoked or the user is deleted, the

provisioning process for the service account is not canceled. Instead, a task is inserted into the provisioning process to remove the mapping from the user to the service account. The provisioning processes of the service account are: `Service Account Changed`, `Service Account Alert`, and `Service Account Moved`.

12.5.2.1.4 User Event Tab The User Event tab shows the workflows that respond to changes to a user record, for example, updating the password or user ID.

12.5.2.1.5 Org Event Tab The Org Event tab shows workflows that respond to changes to an organization record (for example, updating the name or parent name) that the resource is provisioned to or the organization of the user that the resource is provisioned to.

12.5.2.1.6 Resource Event Tab The Resource Event tab shows workflows that respond to state changes of the provisioned resource instance, for example, being enabled or disabled.

12.5.2.1.7 Form Event Tab The Form Event tab shows workflows that respond to data changes in the process form of the provisioned resource instance.

12.5.2.1.8 Attestation Tab The Attestation Event tab shows the workflows that respond to data changes in an attestation process.

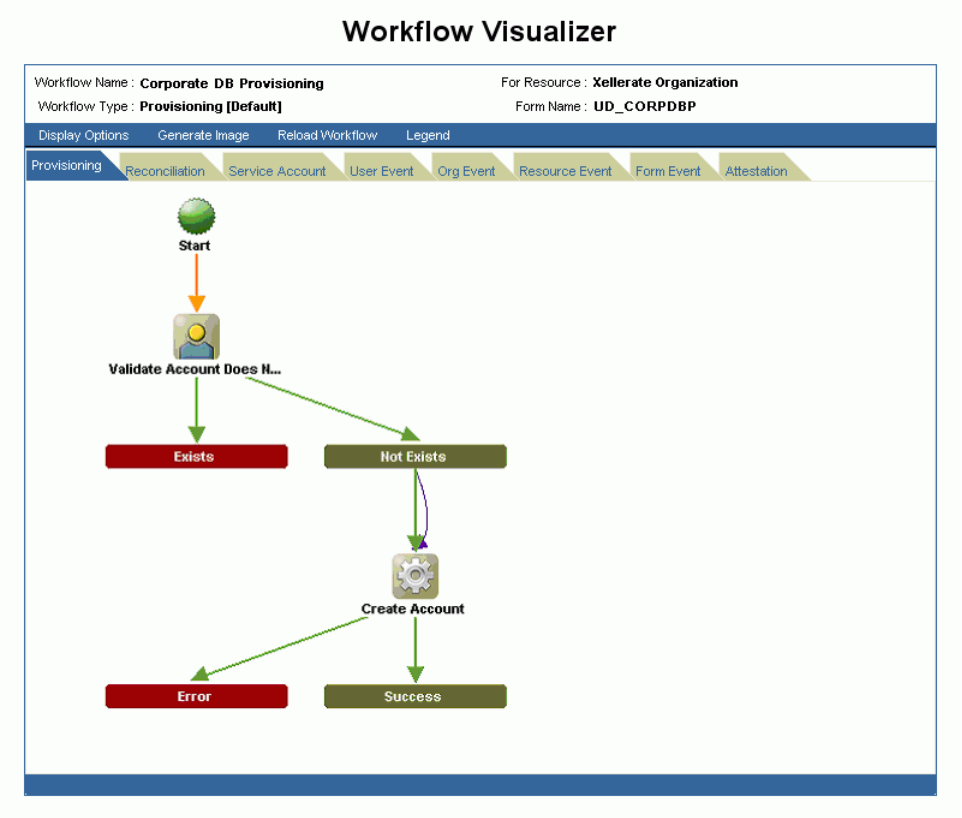
12.5.3 Operations on the Workflow Visualizer

This section discusses the various operations that you can perform by using the Workflow Visualizer:

- Rearranging Elements
- Using the Expansion Nodes
- Accessing the Task Details

Suppose the Corporate DB Provisioning workflow definition is shown. Selecting an event tab displays the appropriate sequence of tasks for that event. These event tabs are discussed in the "Using the Provisioning Workflow Definition Event Tabs" section on page 12-10. Figure 12–2 shows a sample workflow in the Workflow Visualizer.

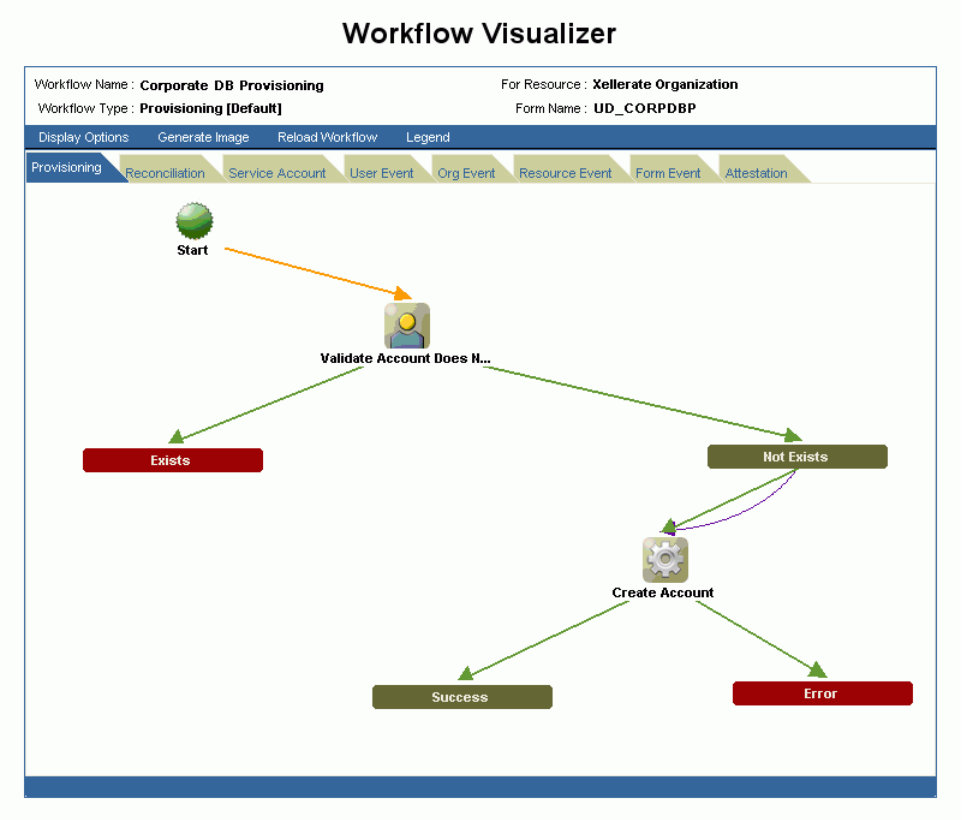
Figure 12–2 Sample Workflow Displayed in the Workflow Visualizer



12.5.3.1 Rearranging Elements

You can rearrange the graphical workflow by moving the icons that constitute the workflow definition to any location in the workflow view. As you move an icon component, the direction arrow continues to be associated with the link. The drag-and-drop functionality of the components in a workflow is illustrated in Figure 12–3.

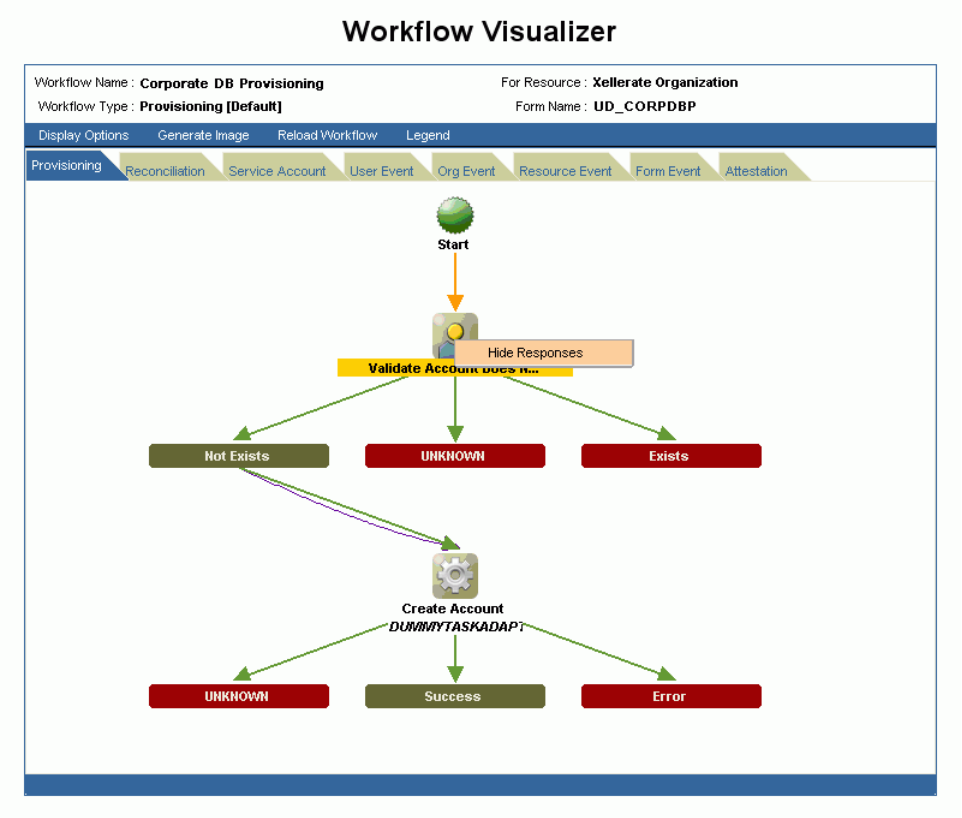
Figure 12–3 Using Drag-and-Drop in the Workflow Visualizer



You can also use the **Display Options** toolbar menu item to display or hide Unknown Response Code, Adapter Name, Undo Tasks, and Recovery Tasks. The workflow automatically refreshes and redraws the workflow based on the changes that you made.

When you right-click a task node, the Hide Responses option is displayed. When you click this option, the response subtree collapses and is replaced with an expansion node. The task node label is highlighted in yellow to denote that it was collapsed. If the node is collapsed, then the Hide Responses option does not appear. Figure 12–4 shows the task node.

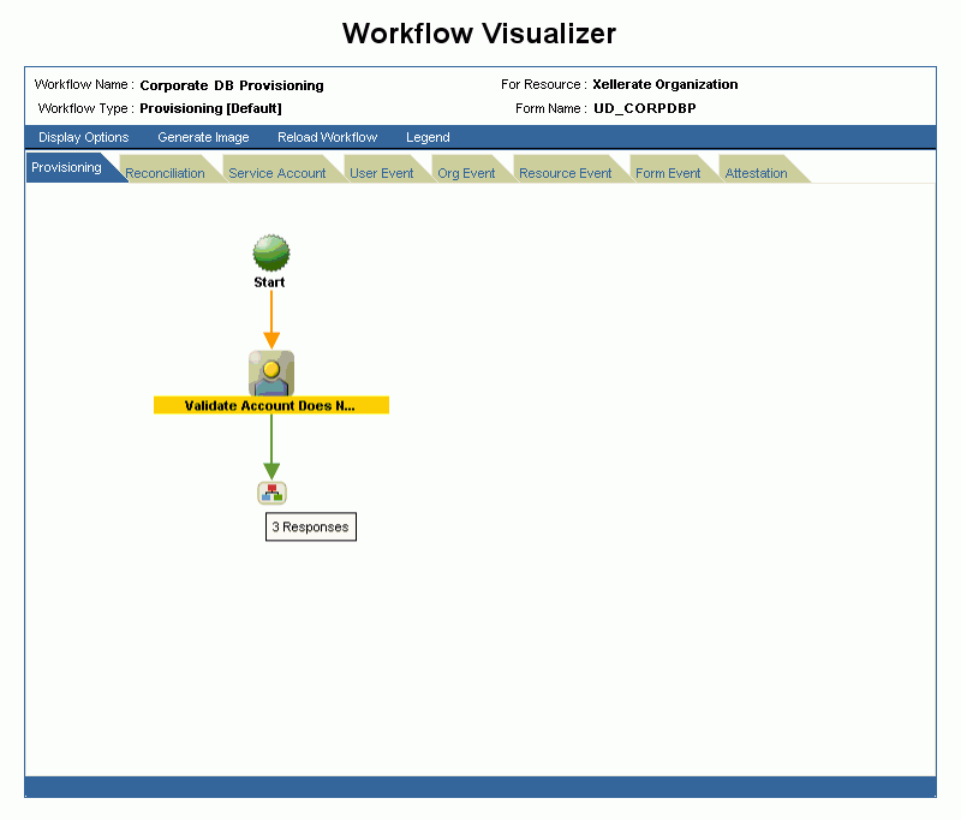
Figure 12–4 Using the Task Node (Shortcut Menu)



12.5.3.2 Using the Expansion Nodes

Task Nodes with more than five response codes, not including the Unknown Response code, are not to be drawn with their responses in the flowchart. Instead, an expansion node replaces the entire response subtree. When you double-click the expansion node, the flowchart is redrawn to display the response subtree for the parent task (node). The label of the task node is highlighted in yellow. Figure 12–5 shows a collapsed response subtree.

Figure 12–5 Collapsed Response Subtree in the Workflow Visualizer



Note: When you place the cursor over the expansion node, a tooltip indicates how many response codes are associated with it. Unknown Response Codes are hidden, by default.

12.5.3.3 Accessing the Task Details

To view detailed information about a particular task, double-click the task icon. The Task Detail page displays information about the task definition on the following tabs:

- **General:** This tab displays task information, for example, the name and description.
- **Automation:** This tab provides information about any adapter automating the task, its status, and variable mappings.
- **Task Assignment:** This tab displays information about how the task is assigned and all associated information.
- **Depends On:** This tab lists all tasks that the selected task depends on.
- **Resource Status Management:** This tab shows the mapping between the task status and the resource status.

12.5.3.3.1 General Tab

Table 12–3 describes the fields on the General tab:

Table 12–3 Fields on the General Tab

Field	Description
Task Name	This field displays the name of the process task.
Task Description	This field displays explanatory information about the process task.
Task Effect	This field indicates the process action for this task. It can be `ENABLED`, `DISABLED`, or `NONE`. A process is enabled or disabled for a user's access to a resource. A disabled action will also disable all associated tasks. The `NONE` action indicates that this task is not associated with a particular process action.
Retry Interval	This field indicates the time in minutes, for which you want to wait before adding this process task instance.
Retry Attempt Limit	This field indicates the number of times Oracle Identity Manager will retry a rejected task.
Conditional Task	This field specifies any condition that must be met for the process task.
Complete On Recovery	This field indicates that Oracle Identity Manager will change the status of the current process task from `Rejected` to `Unsuccessfully Completed` on completion of all recovery tasks that are generated. This flag triggers other dependent process tasks.
Allow Cancellation While Pending	This field indicates whether or not the process task can be canceled if its status is `Pending`.
Allow Multiple	This field indicates whether or not the task is allowed to be inserted multiple times within a single process instance.
Required For Workflow Completion	This field indicates that the process cannot be completed if the process task does not have a `Completed` status.
Manual Insert	This field indicates whether or not a user can manually add the current process task to the process.

12.5.3.3.2 Automation Tab Tasks belonging to provisioning processes are usually automated. Table 12–4 describes the fields on the Automation tab.

Note: If the task is not automated, then this tab is not displayed.

Table 12–4 Fields on the Automation Tab

Field	Description
Adapter Name	This field shows the name of the adapter.
Adapter Status	This field indicates whether or not the adapter is completely mapped.
Adapter Variable	This field contains a user-defined placeholder within the adapter that contains run-time application data used by its adapter tasks.
Mapped?	This field indicates whether or not the adapter variable is mapped.

12.5.3.3.3 Task Assignment Tab This tab specifies the assignment rules for the process task. These rules determine how the process task is assigned.

Task assignment rules are associated with tasks of approval processes, because these tasks are usually completed manually. Tasks belonging to provisioning processes are usually automated. As a result, they do not need task assignment rules.

12.5.3.3.4 Depends On Tab This tab displays the task name that the current task is dependent on.

12.5.3.3.5 Resource Status Management Tab A resource is provided with predefined provisioning statuses that represent the various statuses of the resource object throughout its lifecycle as it is provisioned to the target user or organization. This tab displays the link between the status of a process task (Task Status) and the provisioning status of the resource (Resource Status) to which it is assigned. Table 12–5 describes the fields on the Resource Status Management tab.

Table 12–5 Fields on the Resource Status Management Tab

Field	Description
Task Status	The status can be one of the predefined provisioning status types.
Resource Status	The status can be one of the following: `Waiting`, `Provisioning`, `None`, `Ready`, `Enabled`, `Disabled`, `Revoked`, `Provisioned`, and `Provide Information`.

12.6 Using the Resource Workflows Option to Create and Modify Workflows

The Workflow Designer provides the ability to create and modify workflows. While the Workflow Visualizer provides a graphical view of the workflows, the Workflow Designer provides the ability to create workflows and to edit them.

> **See Also:** *Oracle Identity Manager Design Console Guide* for information about the Process Definition form

This section discusses the following topics:

- Opening the Workflow Designer
- Creating a Workflow
- Workflow Designer Main Page
- Creating and Configuring Tasks and Responses
- Configuring Data Flows

12.6.1 Opening the Workflow Designer

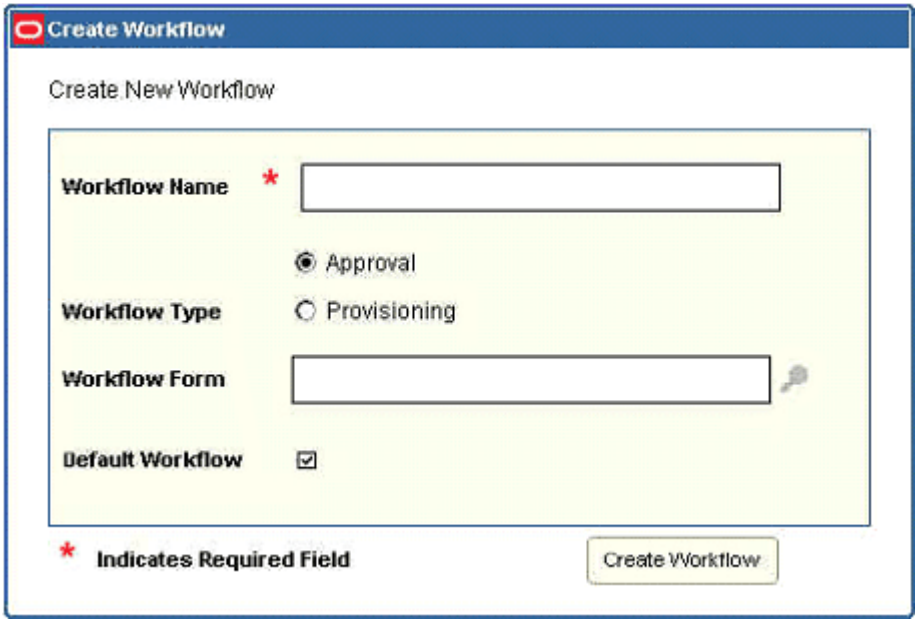
To open the Workflow Designer:

1. In the left navigation pane, click **Resource Management**, and then click **Manage**. The Resource Search page is displayed.
2. Search for a resource.
3. Select a resource by clicking the resource name. The Resource Detail page is displayed.
4. Select **Resource Workflows** from the additional details list. The Resource Workflows page is displayed.
5. Click **Create New Workflow** to open the Workflow Designer and create a new workflow. Alternatively, click **Edit** in the Edit Workflow column of the results table to open the Workflow Designer and edit an existing workflow.

12.6.2 Creating a Workflow

On the Resource Workflows page, when you click **Create New Workflow**, the Workflow Designer opens with the Create Workflow dialog box, as shown in Figure 12–6.

Figure 12–6 Create Workflow Dialog Box



In this dialog box, you must specify the values that are required to create a new workflow. Table 12–6 describes the fields in the Create Workflow dialog box.

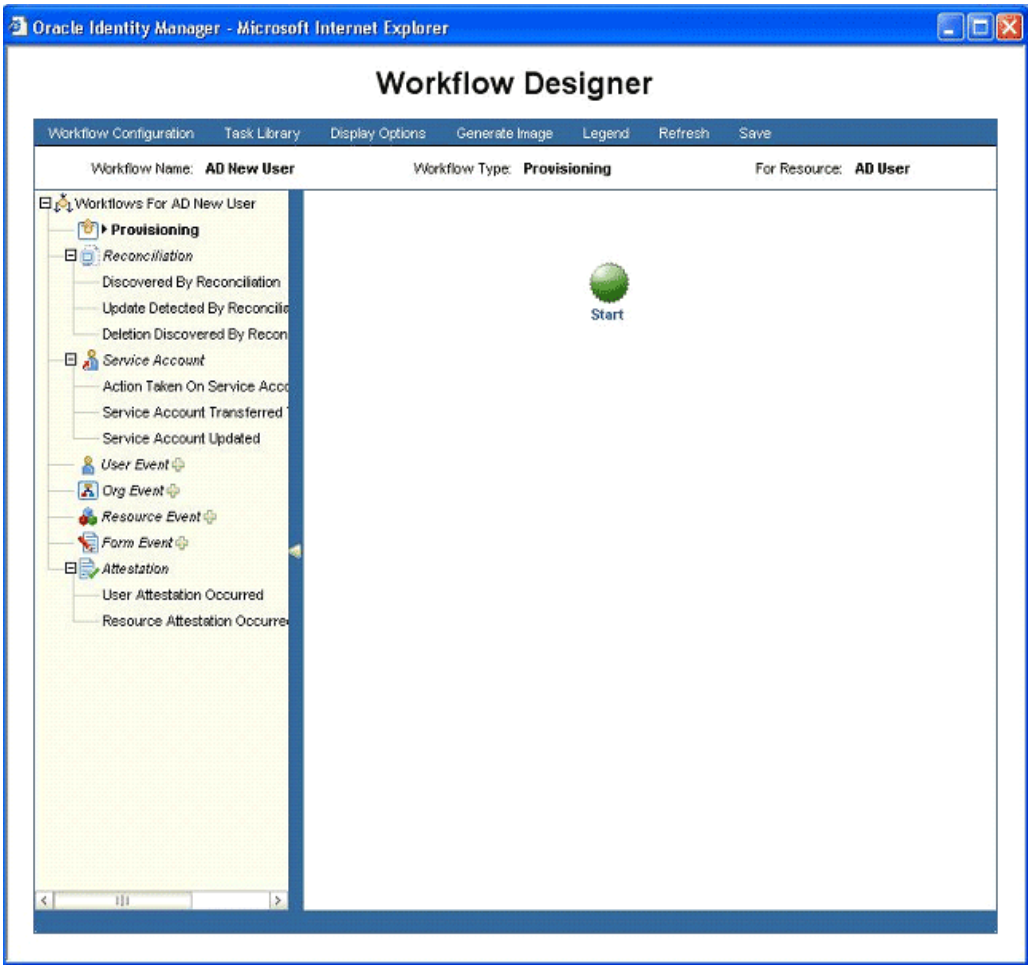
Table 12–6 Fields in the Create Workflow Dialog Box

Field	Description
Workflow Name	The name of the new workflow.
Workflow Type	The Business Workflow definition type (Provisioning or Approval). **Approval** is selected, by default.
Workflow Form	The form associated with the resource for which the workflow is defined. The forms can be: ▪ All the process forms that are not yet assigned to any processes ▪ All the process forms assigned to the other processes defined for the current resource, for which this workflow is being defined This field is enabled if the workflow type is Provisioning. It is disabled if the workflow type is Approval.
Default Workflow	This check box specifies whether or not the current Business Workflow is to be designated as the default approval or provisioning Business Workflow for the resource object with which it is associated. If this check box is selected, then the Business Workflow will be set as the default approval or provisioning Business Workflow for the resource object to which it is assigned. If this check box is not selected, then the process will start only if a process selection rule causes it to be selected.
Create Workflow	The button to create the workflow.

12.6.3 Workflow Designer Main Page

After you click **Create Workflow** in the Create Workflow dialog box by selecting the Provisioning option, the Workflow Designer main page is displayed as shown in Figure 12–7.

Figure 12–7 Workflow Designer Main Page



This page has different sections, with each section giving more information or options to extend the new workflow.

The Workflow Designer main page consists of the following sections:

- Information
- Toolbar
- Designer Page
- Menu Section

  For Approval workflows, the Workflow Designer main page looks different without the left menu section.

12.6.3.1 Information

This section displays the following labels that provide global information about the current workflow:

- **Workflow Name**: The name of the current workflow
- **Workflow Type**: The type of the current workflow, Provisioning or Approval
- **For Resource**: The resource to which the current workflow is attached

12.6.3.2 Toolbar

The toolbar provides features to manage and view the workflow designer pages. This includes options to configure the global workflow information such as the name, form name, auto save, auto prepopulate, generating an image of the graphical workflow view, reloading the workflow, a popup legend, saving the workflow, and providing display options.

This section discusses the functions of the following toolbar buttons:

- Workflow Configuration
- Task Library
- Display Options
- Generate Image
- Legend
- Refresh
- Save

12.6.3.2.1 Workflow Configuration Clicking **Workflow Configuration** opens the Workflow Configuration dialog box, as shown in Figure 12–8. This dialog box provides options for configuring the current workflow.

Figure 12–8 Workflow Configuration Dialog Box

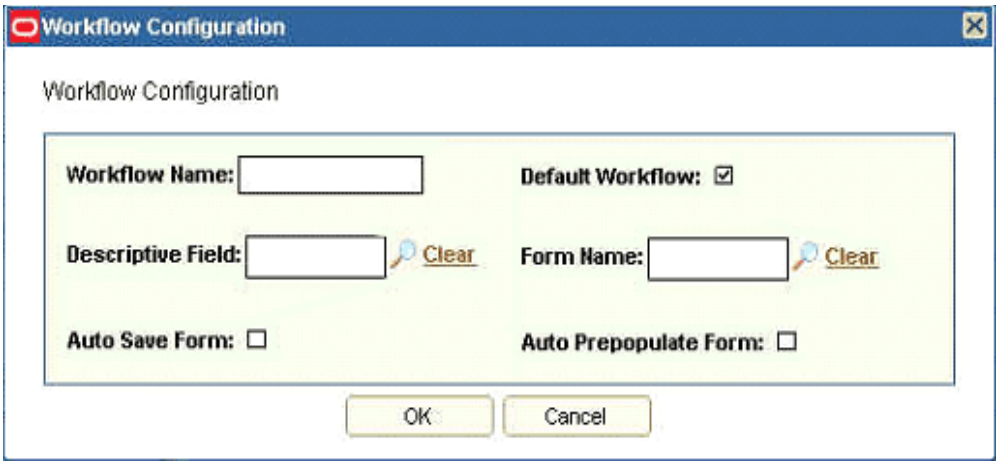


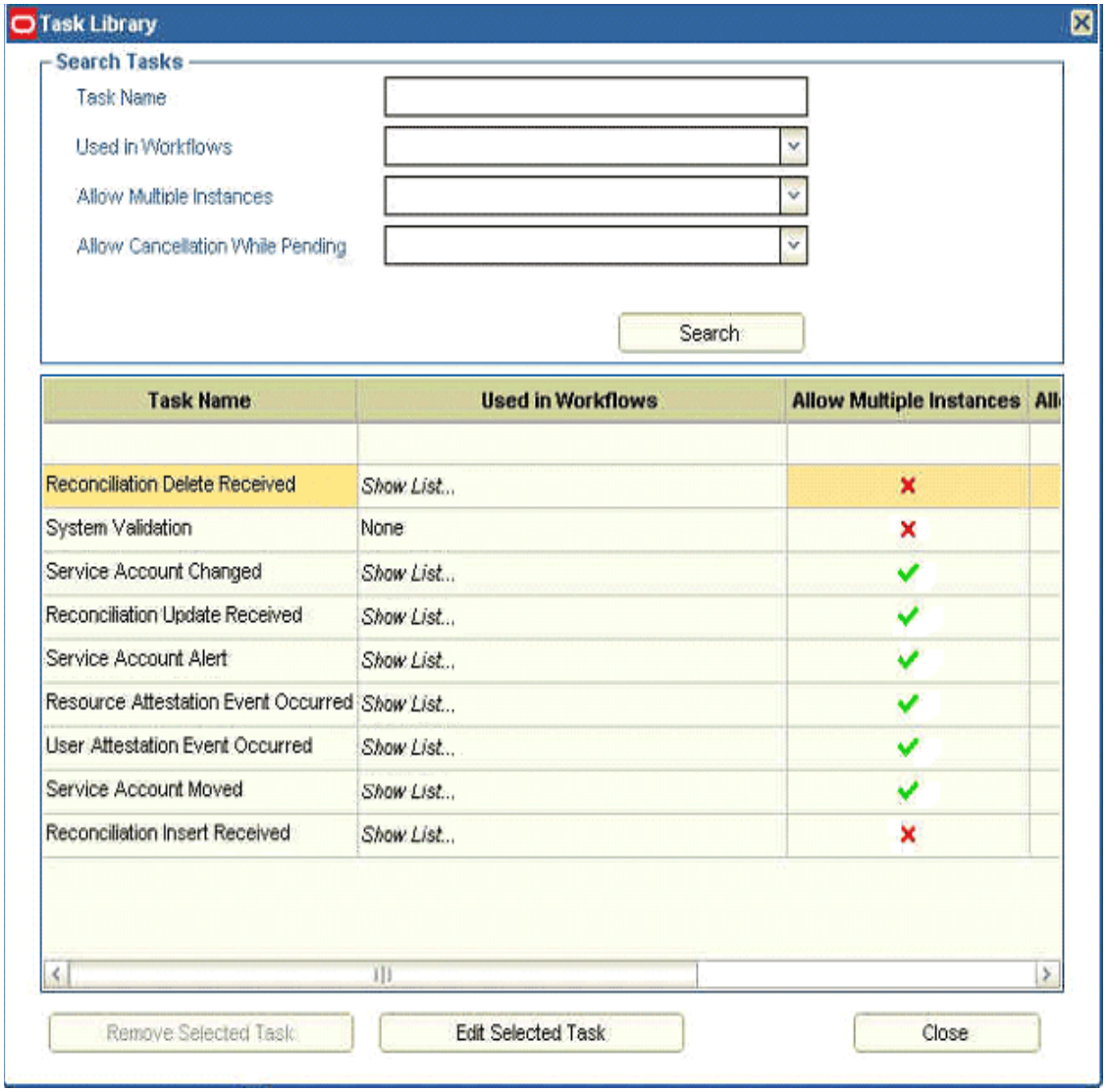
Table 12–7 describes the fields in the Workflow Configuration dialog box.

Table 12–7 Fields in the Workflow Configuration Dialog Box

Field	Description
Workflow Name	The name of the current workflow.
Default Workflow	This check box specifies whether or not the current process is to be designated as the default approval or provisioning process for the resource object with which it is associated. **Note:** For more information about this check box, see "Creating a Workflow" on page 12-17.
Descriptive Field	This is used to map any of the following to a particular instance of the provisioned resource: ▪ Request Key ▪ User Login ▪ Organization Name ▪ Process Type ▪ Data From Workflow Form This information is available only for the Provisioning workflow and not for the Approval workflow.
Form Name	The form assigned to the current workflow. This information is available only for the Provisioning workflow and not for the Approval workflow.
Auto Save Form	This check box is used to set autosave for the form during provisioning without prompting the user for form data. This helps in setting default values for form fields either through predetermined set default values or through data flows. This information is available only for the Provisioning workflow and not for the Approval workflow.
Auto Prepopulate Form	This check box is used to prepopulate the fields during provisioning, with data either from default values or from data flows. Setting this option lets you see the forms while provisioning, along with the data on the fields that you can modify. This information is available only for the Provisioning workflow and not for the Approval workflow.

12.6.3.2.2 Task Library Clicking **Task Library** opens the Task Library page. The Task Library page displays a list of all the tasks in the workflow across all subworkflows. This page also shows a few parameters related to each task, such as in which subworkflows it is present (for provisioning workflows), whether or not multiple instances are allowed, whether or not cancellation while pending is allowed, retry period, and retry count. In addition, you can edit and delete tasks on this page. Figure 12–9 shows the Task Library page.

Figure 12–9 Task Library Page



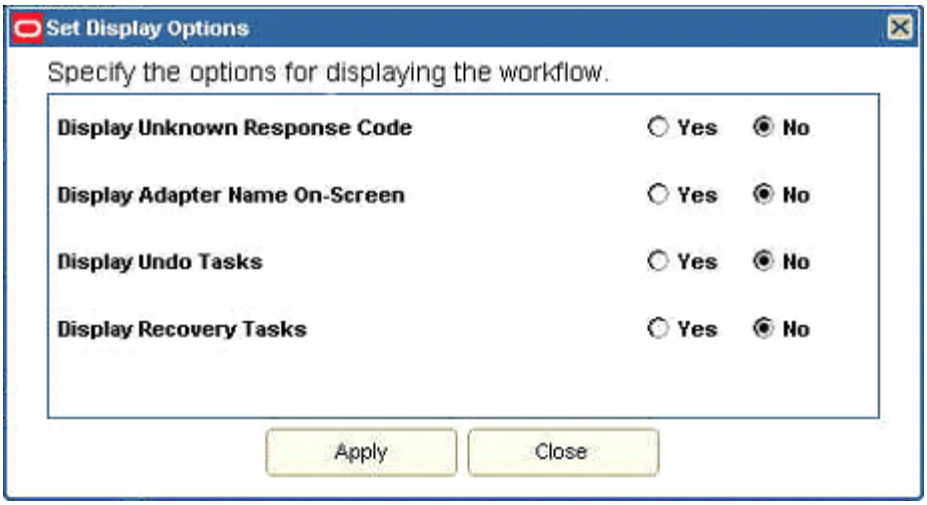
You can delete a task only after both the following conditions are met:

- The task is removed from all workflows. This implies that the task is deleted by right-clicking the task on any subworkflow and clicking **Remove Task and Subflow**.
- No instance of the task is present in the system. For instance, if a workflow is created with a task and if the resource for that workflow is provisioned to a user and the workflow is started resulting in the task being run, then an instance of that task is created in the system. In that case, the task cannot be deleted.

The Task Library page has search criteria on the top that you can use to search for tasks. The main section lists the tasks with various parameters. You can click a row to highlight it. If a task can be deleted, then the Remove Selected Task button is enabled along with the Edit Selected Task button.

12.6.3.2.3 Display Options Clicking **Display Options** opens the Set Display Options dialog box that provides options to specify how the workflow is displayed when you are designing the workflow. Figure 12–10 shows the Set Display Options dialog box.

Figure 12–10 Set Display Options Dialog Box



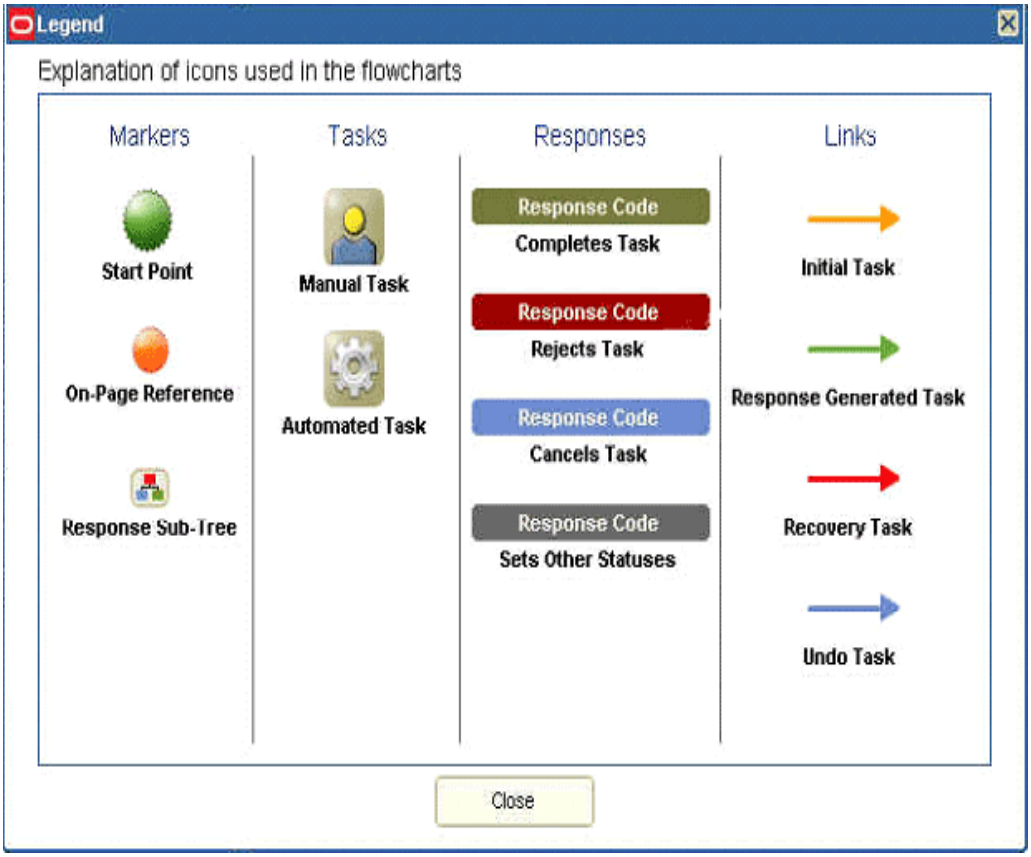
You can use this dialog box to enable or disable the following options:

- **Display Unknown Response Code**: Display or hide unknown response codes.
- **Display Adapter Name On-Screen**: Display or hide adapter names attached to the tasks.
- **Display Undo Tasks**: Display or hide undo tasks.
- **Display Recovery Tasks**: Display or hide recovery tasks.

12.6.3.2.4 Generate Image Clicking **Generate Image** saves the current view of the workflow as a JPEG image. The image opens in a new browser window.

12.6.3.2.5 Legend Clicking **Legend** opens the Legend dialog box, which is shown in Figure 12–11. This dialog box shows the following types of elements:

Figure 12–11 Legend Dialog Box



- **Markers:** These elements represent a particular marking or place in the workflow. For example, the starting point, an on-page reference, or a place representing an extended workflow with more elements underneath can be represented with a marker.

  You can right-click a Task element and select the option to hide the responses. When you hide a response, the icon for the Response subtree is displayed to indicate that there are hidden responses. The on-page reference marker refers to other elements on the page whose relationship is not shown with links. An example of this is a response code defined for a task and for that response a response-generated task is defined. If this response-generated task has its response referring to the original task in a circular manner, then an on-page reference marker makes it easier to show the relationship.

- **Tasks:** These icons are used to indicate manual and automated tasks. If a task has an event handler or an adapter attached to it for autocompletion, then it is an automated task. Otherwise, it remains a manual task.

- **Responses:** These are the different color codes used for different types of response codes, such as Completes, Rejects, and Cancels. Any user-defined response code is shown with a different color code.

- **Links:** These are the different color codes used for links that display the relationship or linkage between elements. Depending on the type of task the link refers to, the color code for the link is different. For example, the color code indicates whether or not the task is undo or recovery. The different types of links are: Initial Task, Response Generated Task, Recovery Task, and Undo Task.

12.6.3.2.6 Refresh Clicking **Refresh** reloads the workflow to display it with default indentations and locations for the labels and icons. It regenerates the topology to arrange the elements on the workflow by using the JGraph algorithm.

12.6.3.2.7 Save Clicking **Save** saves all changes made to the workflow, including all the additions and modifications to the Oracle Identity Manager database.

Caution: You must click **Save** to commit the changes. If you close the Workflow Designer main page without saving the workflow, then all the changes will be lost.

12.6.3.3 Designer Page

The designer page displays the workflow with all the elements and their positions in the process flow with the help of links. This is similar to a drawing board in which the components, such as tasks and responses, can be created by using appropriate options. These components on the designer page can be further configured. On this page, the different entities of the workflow can be graphically shown along with their relationship with each other. For a newly created workflow, this page displays a start marker that indicates the starting point for the workflow process. All the objects that are added to this page are relative to this marker, which acts as a reference point.

12.6.3.4 Menu Section

The menu section consists of the menu items that represent a particular subsection of the workflow. This section is available only for Provisioning workflows. The menu items available are the following:

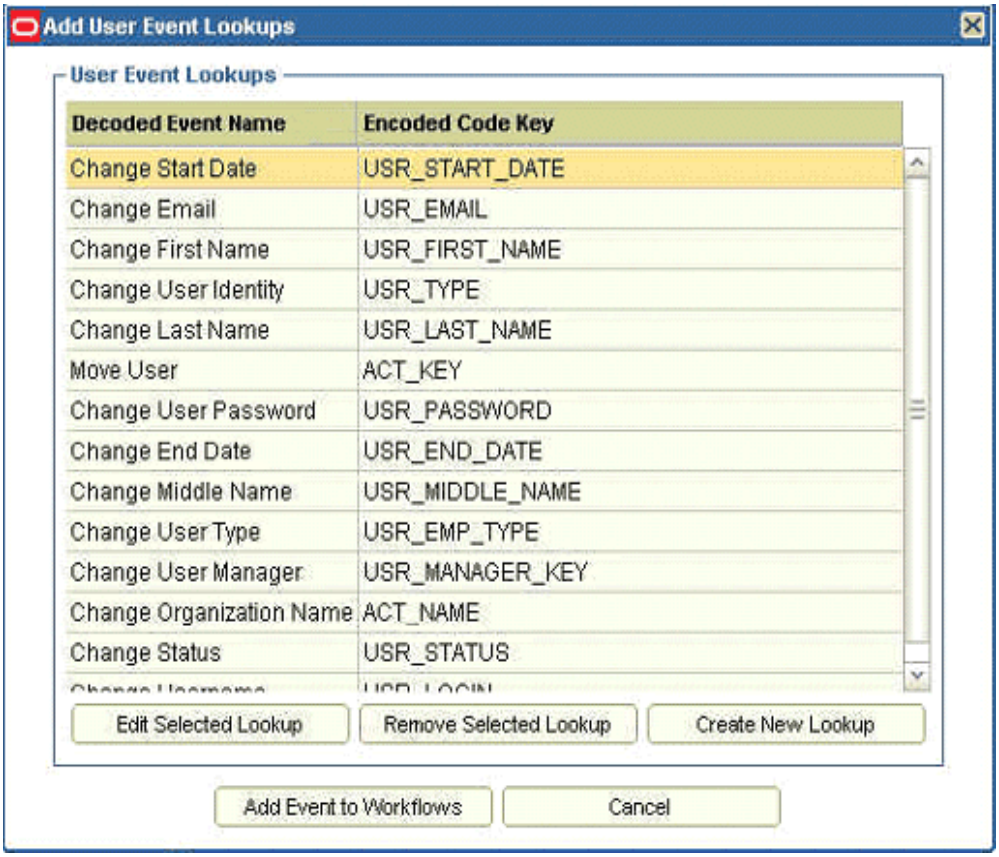
- **Provisioning:** This is the default page displayed when the Workflow Designer application is started.
- **Reconciliation:** This provides a list of tasks that are run on reconciliation events, such as Reconciliation Insert Received, Reconciliation Update Received, and Reconciliation Delete Received. These tasks are submenu items under the Reconciliation menu item.
- **Service Account:** Service accounts are general administrator accounts, such as admin1, admin2, and admin3, that are used for maintenance purposes. Usually, these accounts are used to allow one system, rather than a user, to interact with another system. The model for managing and provisioning service accounts is different from standard provisioning. Service accounts are requested, provisioned, and managed in the same manner as regular accounts. Service accounts use the same resource objects, provisioning processes, and process or object forms as regular accounts. A service account is distinguished from a regular account by an internal flag. When a user is provisioned with a service account, Oracle Identity Manager manages a mapping from the user's identity to the service account. This user is considered the owner of the service account. The tasks that are available under the Service Account menu item are Service Account Change, Service Account Alert, and Service Account Moved.
- **User Event:** This provides a list of tasks that are run based on the events on users. They have the following default names:
  - Change User Location
  - Move User
  - Change User Type

- Change User Password
- Change User Manager
- Change Username
- Change First Name
- Change Last Name
- Change User Identity

Note: These names are derived from the decoded values of `Lookup.USR_PROCESS_TRIGGERS` in the design console Lookup Definition form. If the values are modified, then these names will be different accordingly.

A user event can be inserted into the workflow by clicking the plus sign (+) icon next to the User Event menu item. Clicking the + icon opens the Add User Event Lookups dialog box with a list of currently available event tasks, as shown in Figure 12–12. Selecting a task and clicking **Add Event to Workflows** will create a new menu item under the User Event menu and open the page for that workflow.

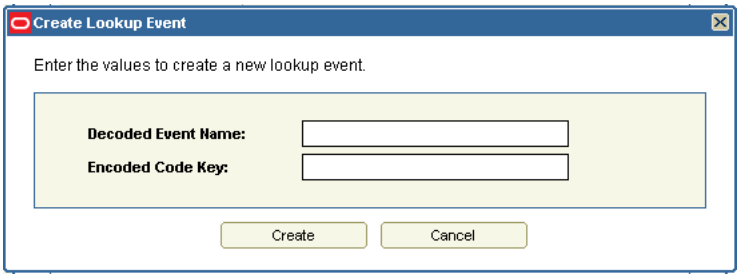
Figure 12–12 Add User Event Lookups Dialog Box



The Add User Event Lookups dialog box also provides the following options to create new lookup events and edit or remove existing lookup events:

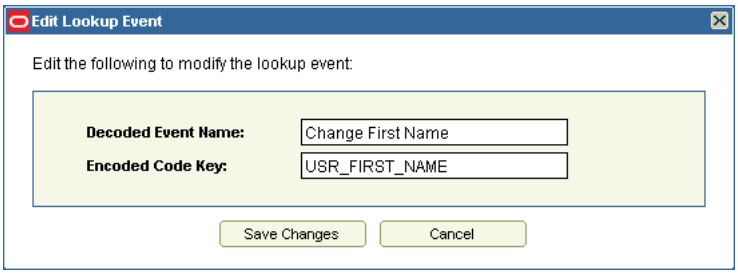
– Create New Lookup: When you click this button, the Create Lookup Event dialog box is displayed, as shown in Figure 12–13.

Figure 12–13 Create Lookup Event Dialog Box



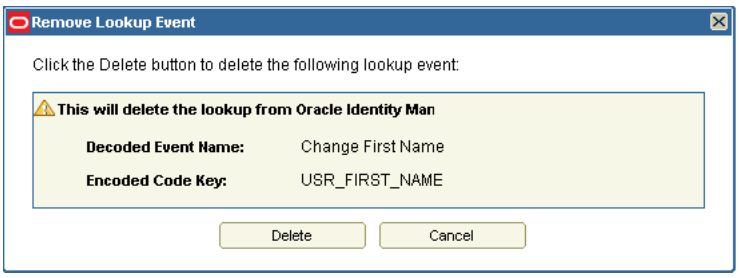
– Edit Selected Lookup: When you click this button, the Edit Lookup Event dialog box is displayed, as shown in Figure 12–14.

Figure 12–14 Edit Lookup Event Dialog Box



– Remove Selected Lookup: When you click this button, the Remove Lookup Event dialog box is displayed, as shown in Figure 12–15.

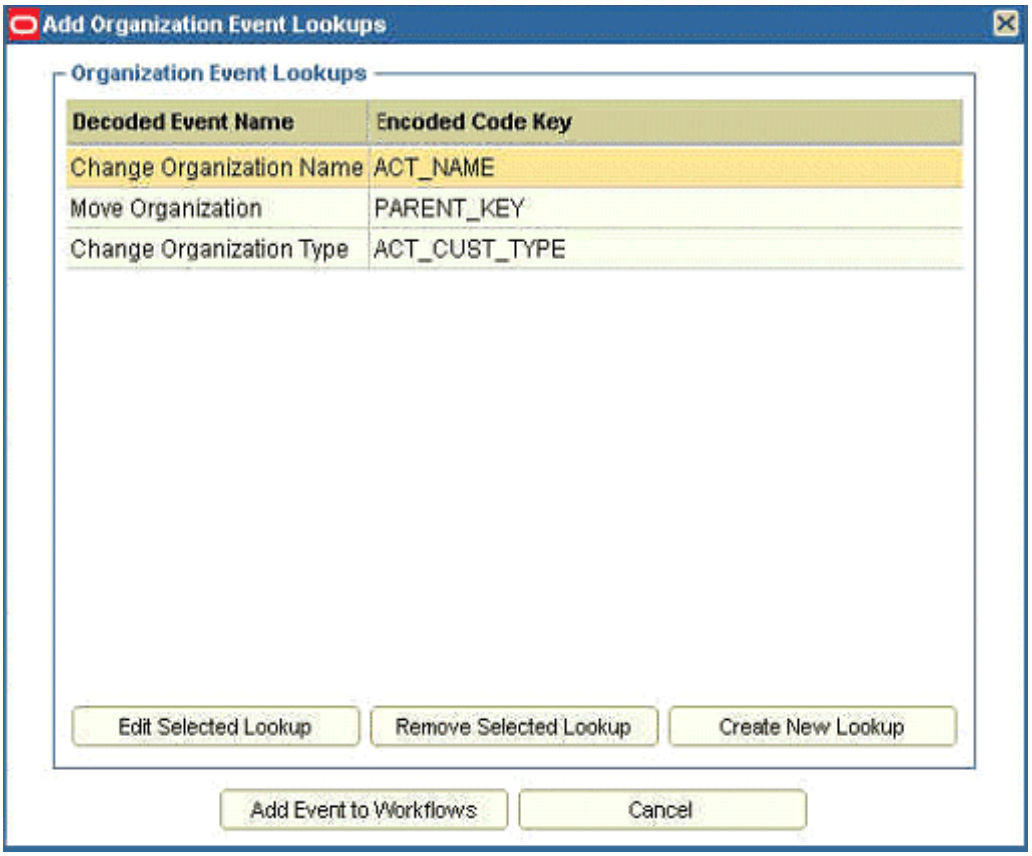
Figure 12–15 Remove Lookup Event Dialog Box



- **Org Event:** This provides a list of tasks that are run based on the events on organizations. They have the following default names:
  - Change Organization Type
  - Change Organization Name
  - Move Organization

  An organization event can be inserted into the workflow by clicking the + icon next to the Org Event menu item. Clicking the + icon opens the Add Organization Event Lookups dialog box with a list of currently available event tasks, as shown in Figure 12–16. You can select a task and click **Add Event to Workflows** to create a new menu item under the Org Event menu and open the page for that workflow.

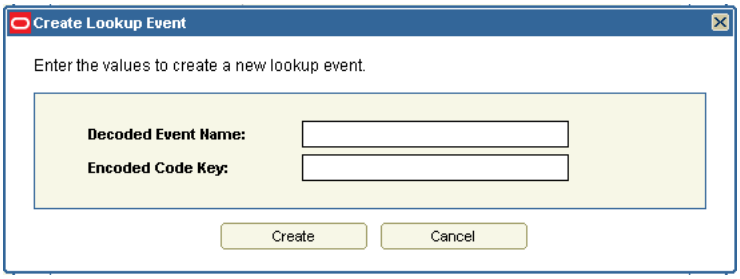
Figure 12–16 Add Organization Event Lookups Dialog Box



The Add Organization Event Lookups dialog box also provides the following options to create new lookup events and edit or remove existing lookup events:

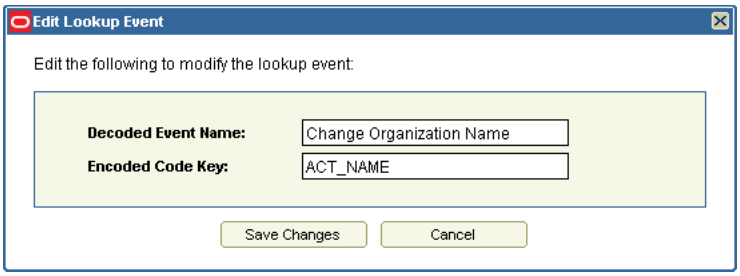
– Create New Lookup: When you click this button, the Create Lookup Event dialog box is displayed, as shown in Figure 12–17.

Figure 12–17 Create Lookup Event Dialog Box



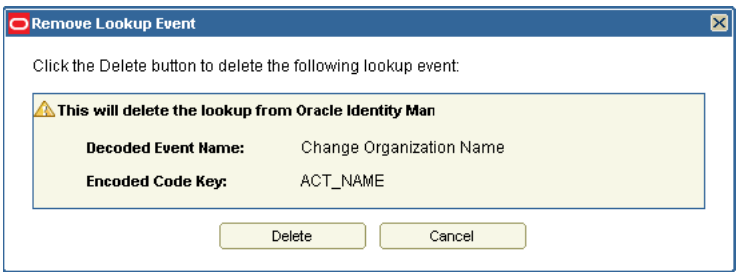
– Edit Selected Lookup: When you click this button, the Edit Lookup Events dialog box is displayed, as shown in Figure 12–18.

Figure 12–18 Edit Lookup Event Dialog Box



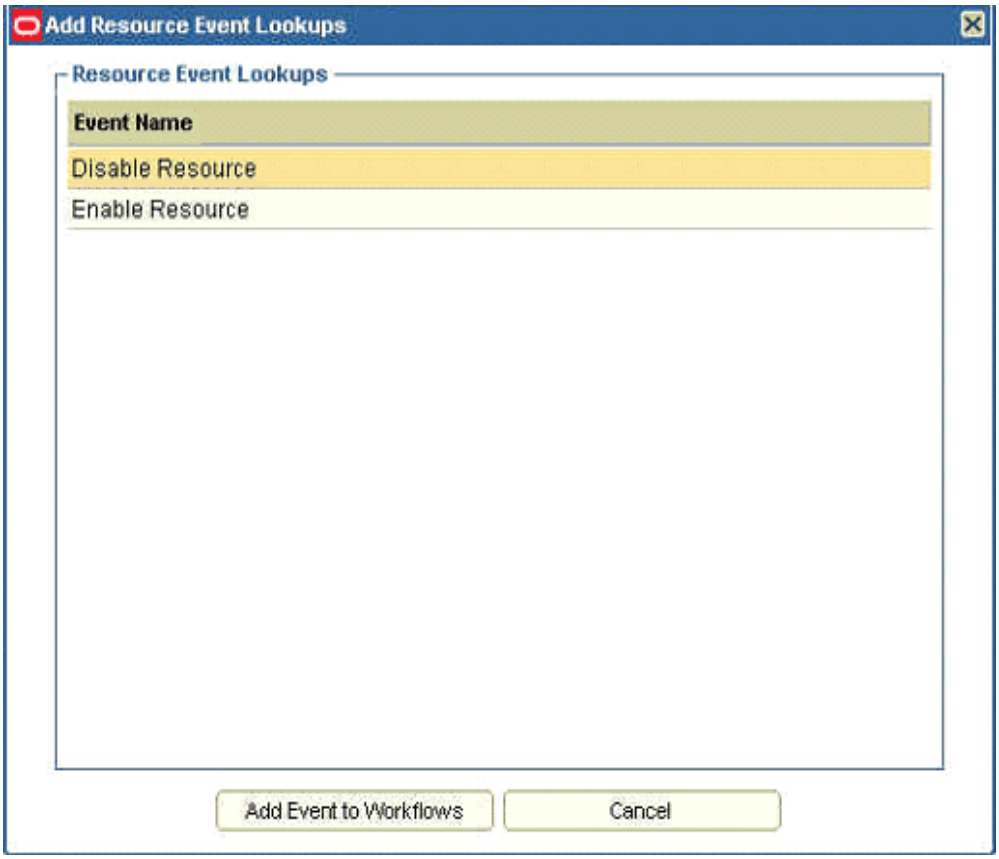
– Remove Selected Lookup: When you click this button, the Remove Lookup Events dialog box is displayed, as shown in Figure 12–19.

Figure 12–19 Remove Lookup Event Dialog Box



- **Resource Event:** This provides a list of tasks that are inserted into the workflow and run when an event occurs on the resource. These events are defined as disabled or enabled events on the resource. There are submenu items for Enable Resource and Disable Resource under the Resource Event menu item. A resource event can be inserted into the workflow by clicking the + icon next to the Resource Event menu item. Clicking the + icon opens the Add Resource Event Lookups dialog box with two options, Enable Resource and Disable Resource, as shown in Figure 12–20. You can select an option and click **Add Event to Workflows** to create a new menu item under the Resource Event menu and open the page for that workflow.

Figure 12–20 Add Resource Event Lookups Dialog Box

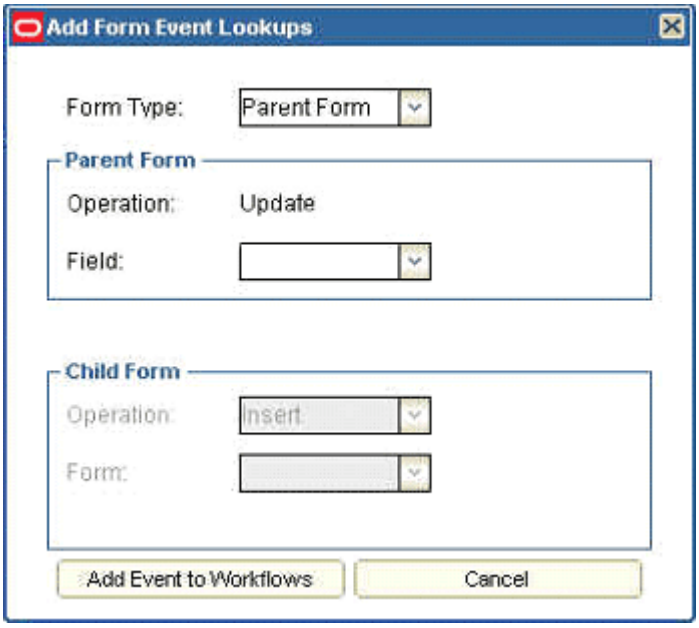


- **Form Event:** This provides a list of tasks that get inserted and run based on an event on a form field or child table. For events on parent process form fields, the name of the tasks have the following convention:

  `Field field_name Updated`

  The events on child tables are named based on the child table name and the type of event such as insert, update, and delete. A form event can be inserted into the workflow by clicking the + icon next to the menu item. Clicking the + icon opens the Add Form Event Lookups dialog box with the fields shown in Figure 12–21.

Figure 12–21 Add Form Event Lookups Dialog Box



In the Add Form Event Lookups dialog box, you can select either parent form or child form in the Form Type field. When you select **Parent Form**, the fields in the Child Form section are disabled. Similarly, when you select **Child Form**, the fields in the Parent Form section are disabled. In the Parent Form section, only the Update operation is available. In the Child Form section, the available operations are Insert, Update, and Delete. These operations trigger the event. Each section has fields for the form fields of the parent form, or the form names in case of child forms. The Task names for only the child table event tasks can be modified after creation.

Note: The parent form field event names are fixed, and the task name fields cannot be edited. Although the name is inherently in a fixed format, it can be customized and localized by updating the `global.workflow.startMarker.UpdatedField` property in the `xlRichClient.properties` file. See *Oracle Identity Manager Administrative and User Console Customization Guide* for details.

- **Attestation:** This menu item is for the attestation events. There are two types of attestation events, User Attestation and Resource Attestation. No new events can be added to attestation although the existing workflows can be modified similar to other subworkflows.

12.6.4 Creating and Configuring Tasks and Responses

A workflow can consist of more than one task. This section discusses the following topics related to tasks:

- General Menu Options
- Task Options
- Response Options
- Configuring Tasks

- Configuring Responses

12.6.4.1 General Menu Options

You can right-click the designer page to display a menu with general options to create tasks and responses. The general menu options are:

- **Create New Task:** Creates a new task with a default name, which can be further modified and configured. The task is represented as an icon.
- **Insert Existing Task:** Displays the Existing Tasks dialog box with the list of all existing tasks across the subworkflows except the tasks present in the current subworkflow and the main user, organization, resource, and form event tasks for provisioning workflows. You can select a task and insert it in the current workflow.
- **Create Response:** Creates a new response with a default response code, which can be further modified and configured. The response is represented as an icon.

Various options are available when you right-click the task icons, response icons, and the links between the tasks and responses.

12.6.4.2 Task Options

You can right-click a task icon to display a menu that provides the following options related to tasks:

- **Link To Response:** This option is used to link a task to a response. To use this option, first create a response. When you select this menu item, a link is displayed starting from the task icon. This link extends with the mouse pointer. When you click the response, the arrowhead of the link positions itself on the response, and the response is created for the task.
- **Link To Undo Task:** This option is used to link two tasks with the undo relationship. It is used when you want to add a task as the undo task of the current selected task. To do this:
  1. Select the task to which the undo task is to be added.
  2. Right-click the task icon, and select the **Link To Undo Task** menu item.
  3. Select the target tasks icon to add it as the undo task.

  Note: If the **Display Undo Tasks** option in the Display Options toolbar is selected with the value **No**, then the Undo task will not be visible after creating the undo relationship. To see the undo task, select **Yes** for the **Display Undo Tasks** option.

- **Link To Recovery Task:** This is used to link two tasks with the recovery relationship. It is used when you want to add a task as the recovery task of the currently selected task. To do this:
  1. Select the task to which the recovery task is to be added.
  2. Right-click the task icon, and select the **Link To Recovery Task** menu item.
  3. Select the target task to add it as the recovery task.

Note: If the **Display Recovery Tasks** option in the **Display Options** toolbar button is selected with the value **No**, then the recovery task will not be displayed after creating the recovery relationship. To display the recovery task, select **Yes** for the **Display Recovery Tasks** option.

- **Remove Task and Subflow:** This is used to remove a task and all the elements under the task. This includes all the links originating from the task and all their child elements and their child elements and so on. When the same task is present in multiple subworkflows and it is removed from one subworkflow, it gets removed from all the subworkflows where this task has the same parent task, which is the task whose response-generated tasks contain the current removed task.

  Removing a task or the children will not delete the tasks from the system but only from the workflows. Deleting a task from the system permanently can be done from the Task Library. Removing tasks from the designer page still keeps the task definitions and removes them only from the workflows.

12.6.4.3 Response Options

You can right-click a response icon to display a menu that provides the following options related to responses:

- **Add Response Generated Task:** This is used to add a task as a response-generated task for the selected response. To do this:
  1. Create the response-generated task.
  2. Right-click the response, and select **Add Response Generated Task**. A link is created.
  3. Select the task. The link positions on the task and the relationship are created.
- **Remove:** This is used to remove a response. When you select this option, a confirmation page is displayed. Confirming the deletion removes the response and all its children. When a response is removed that contains generated tasks, then those tasks will be removed but not deleted. When a task is removed, it is removed only from the workflow and is not deleted permanently. You can permanently delete a task from the Task Library.

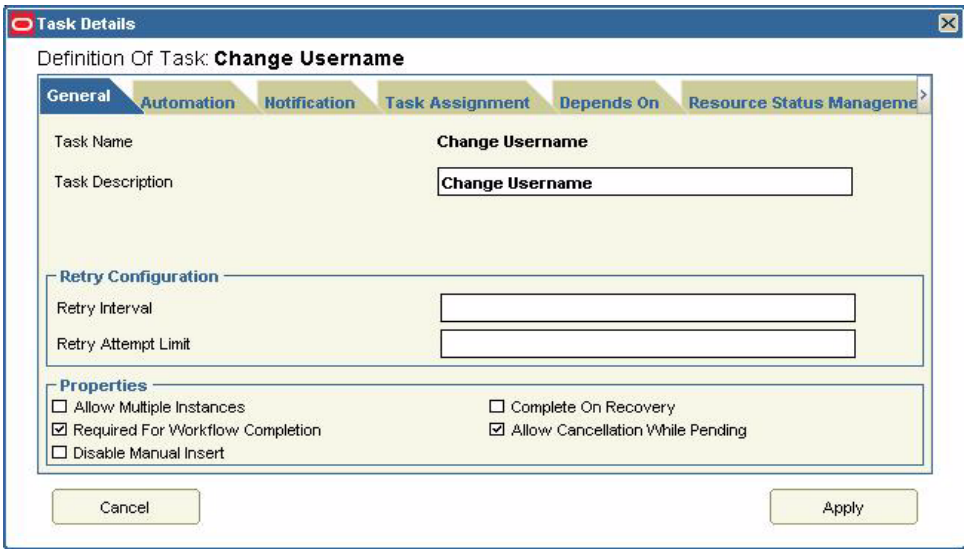
12.6.4.4 Link Options

You can remove the relationships between some elements by right-clicking the link and clicking the **Remove** option. This option is not available for all links. For example, for reconciliation workflows, you cannot delete the default tasks connected to the start marker. Therefore, you cannot remove the relationship between the start markers and the default tasks. The link for which you can remove the relationship is highlighted with a broken arrow when you roll your mouse on the relationship. When the arrow is highlighted, right-click the arrow and the **Remove** option is displayed. This helps in removing the link between a response and a task and to assign another response to the task, or to assign another task to the response, without the need to delete the link and create new ones.

12.6.4.5 Configuring Tasks

You can configure tasks in the Workflow Designer by using the Task Details dialog box. This dialog box is shown in Figure 12–22. To open the Task Details dialog box, double-click the task icon on the designer page.

Figure 12–22 Task Details Dialog Box



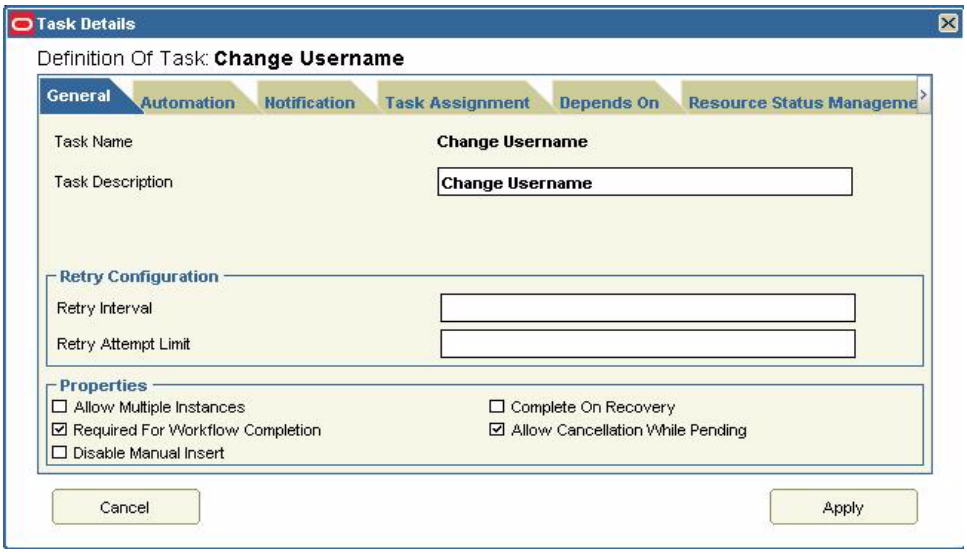
This section discusses the following tabs in the Task Details dialog box:

- General Tab
- Automation Tab
- Notification Tab
- Task Assignment Tab
- Depends On Tab
- Resource Status Management Tab

General Tab

Figure 12–23 shows the General tab of the Task Details dialog box.

Figure 12–23 General Tab



This tab lets you specify the general information about the task:

- **Task Name:** This is the name of the process task. This field can be edited, except when the task name cannot be changed. For example, on the Form Events page, the event task for parent field update.
- **Task Description:** This is descriptive information about the process task.
- **Retry Configuration:** This section is present only for provisioning workflows and consists of the following options:
  - **Retry Interval:** If a process task has the `Rejected` status, then this is the time interval in minutes before Oracle Identity Manager inserts a new instance of that task with a `Pending` status.
  - **Retry Attempt Limit:** This is the number of times Oracle Identity Manager retries a rejected task.
- **Properties:** This section has the following options:
  - **Allow Multiple Instances:** This check box determines whether or not the process task can be inserted into the current process more than once. If you select this check box, then multiple instances of the process task can be added to the process. If you deselect this check box, then the process task can be added to the current process only once.
  - **Required for Workflow Completion:** This check box determines whether or not the current process task must be completed for the process to be completed. If you select this check box, then the process cannot be completed if the process task does not have a `Completed` status. If you deselect this check box, then the status of the process task does not affect the completion status of the process.
  - **Complete On Recovery:** This check box determines whether or not the status of the task must be set to `Completed` on completion of the recovery tasks.
  - **Allow Cancellation While Pending:** This check box determines whether or not the process task can be canceled if its status is `Pending`. If you select this check box, then the process task can be canceled if it has a `Pending` status. If

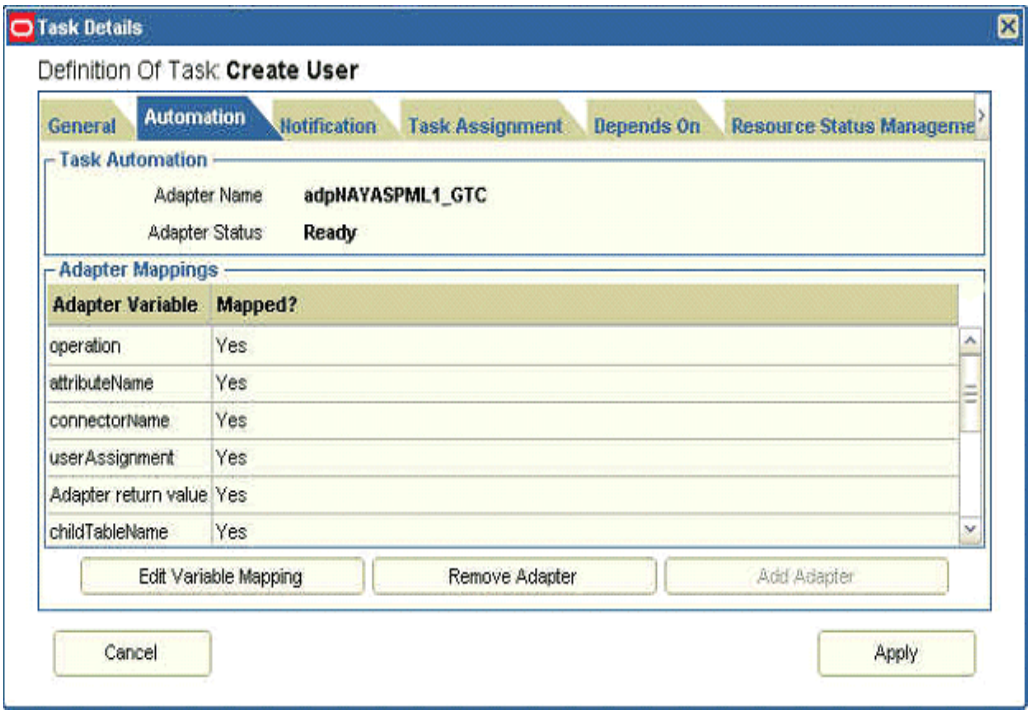
you deselect this check box, then the process task cannot be canceled if its status is `Pending`.

– **Disable Manual Insert:** This check box determines whether or not a user can manually add the current task to the workflow. If this check box is selected, then the task cannot be added to the workflow manually. If you deselect this check box, then a user can add the task to the process.

Automation Tab

Figure 12–24 shows the Automation tab of the Task Details dialog box.

Figure 12–24 Automation Tab



The Automation tab lets you attach an event handler or an adapter with the task that helps in the automation of the process task.

The options on this tab are divided into two parts. The task automation section shows the currently attached adapter with the status of the adapter. The Adapter Mappings section shows the adapter variable mappings. There are buttons on the tab that enable you to add an adapter or event handler, remove the adapter, and edit the variable mappings when an adapter is attached.

When you click **Add Adapter**, a dialog box is displayed. This dialog box consists of a section for the handler type with an option each for system event handlers and adapters. Selecting each option displays the corresponding descriptive text below the handler type section. You can select an item in the list and click **Add**.

The Adapter Mappings section shows the variables associated with the adapters along with the mappings. It displays the variable name and whether or not it has been mapped. When you select a variable, the Edit Variable Mapping button is enabled. You can click this button to open the Adapter Mappings dialog box with all the various options available to map this variable. This dialog box provides the following options:

- **Variable Name:** This text label displays the name of the adapter variable for which you are setting a mapping, such as UUID.
- **Data Type:** This text label displays the data type of the adapter variable. For example, String is the data type for the UUID variable.
- **Map To:** This list displays the types of mappings that you can set for the adapter variable, such as IT Resources.

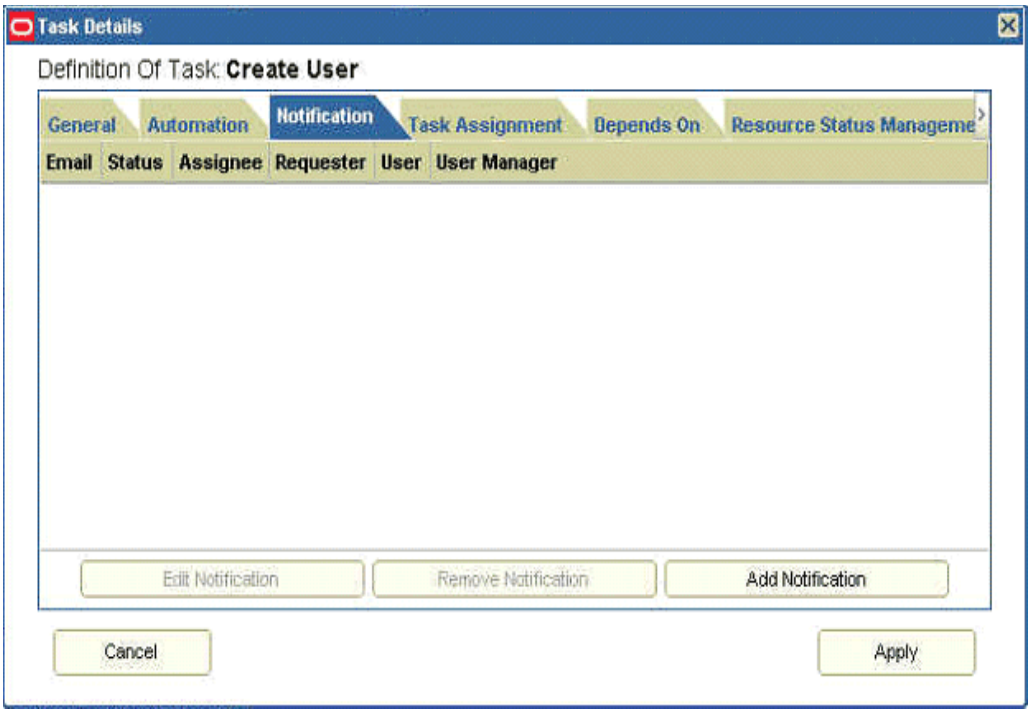
  When you map the adapter variable to a location or contact, Oracle Identity Manager enables a list with values for a specific type of location or contact to which you are mapping the adapter variable. In addition, if you map the adapter variable to a custom process form and this form contains child tables, then Oracle Identity Manager enables the adjacent list. From this list, select the child table to which you are mapping the adapter variable. If you are not mapping the adapter variable to a location, contact, or child table of a custom process form, then this list is disabled.
- **Qualifier:** This list contains the qualifiers for the mapping that is selected in the Map To list, such as IT Asset.
- **Old Value:** This check box specifies whether or not you map the adapter variable to the value that was originally selected in the **Qualifier** check box before modification. Process task adapters associated with process tasks are conditionally triggered when some field on the process form is changed. If you select the **Old Value** option and the process task is marked `Conditional`, then the value that is passed to the adapter is the previous value of the field or variable for which the mapping is being selected. This is useful for fields that accept passwords. For example, if you want to disallow setting the password to the same value, then you can use the old value for comparison. If you are not mapping the adapter variable to a field that belongs to a child table of a custom process form, then this check box is disabled.

  Note: Different fields may be displayed in the Adapter Mappings dialog box, based on what you select from the Qualifier and Map To lists.

Notification Tab

Figure 12–25 shows the Notification tab of the Task Details dialog box.

Figure 12–25 Notification Tab



This tab lets you designate the e-mail notification to be generated when the current process task achieves a particular status. For each status that a task can achieve, a separate e-mail notification can be generated. If an e-mail notification is no longer valid, then you can remove it from the Notification tab.

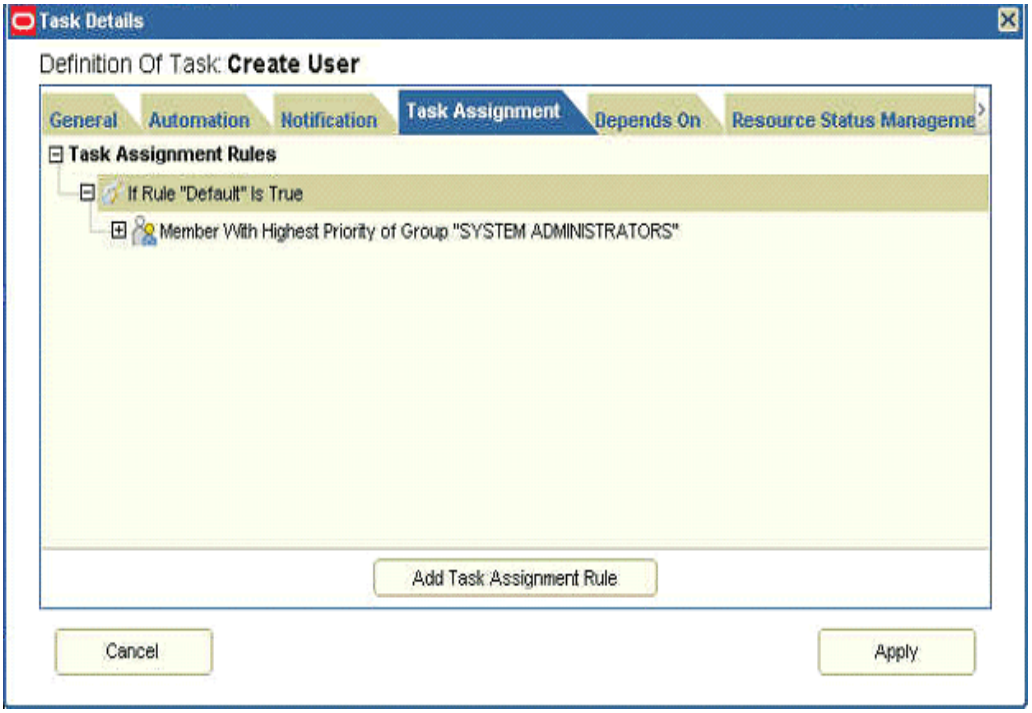
Note: For Oracle Identity Manager to send an e-mail notification to a user, a template for the e-mail message must first be created by using the E-mail Definition form.

There are three buttons in the dialog box: Add Notification, Remove Notification, and Edit Notification. You can use these buttons to configure the notifications tab by adding, deleting, and editing notifications.

Task Assignment Tab

Figure 12–26 shows the Task Assignment tab of the Task Details dialog box.

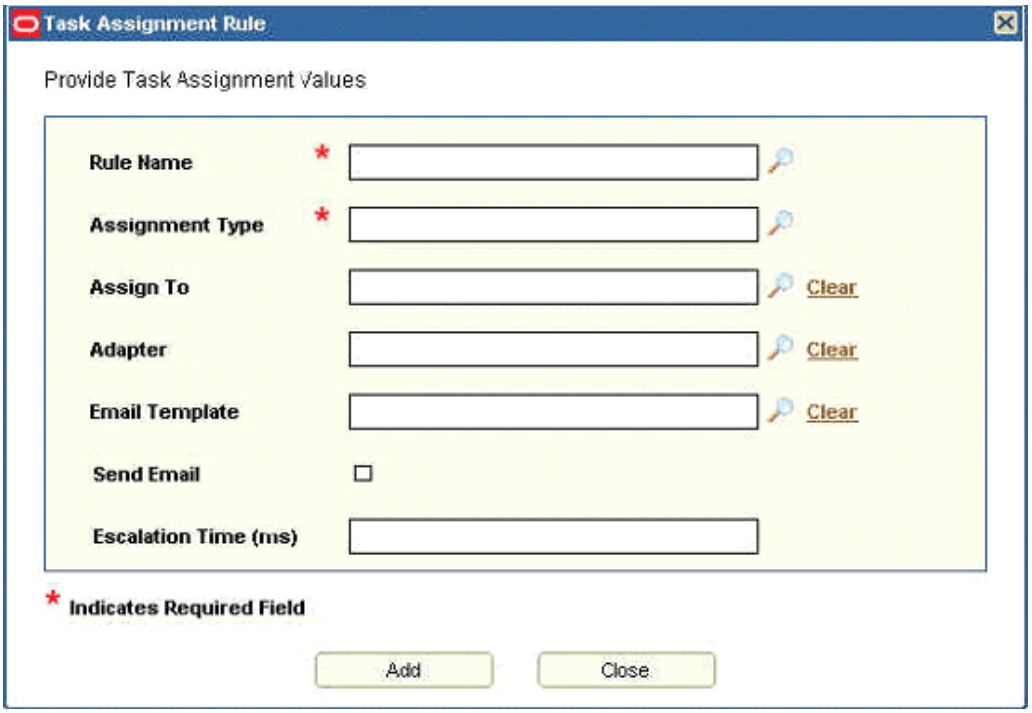
Figure 12–26 Task Assignment Tab



This tab lets you add task assignment rules for the current task. It provides options to add the rules, assignment type, whom the task must be assigned to, adapter, e-mail template, and escalation time. The added rules are displayed in a tree based on the priority. The shortcut menu that is displayed when you right-click the rule provides options to change the priority of the rule, and to edit or delete the rule.

When you click **Add Task Assignment Rule**, the Task Assignment Rule dialog box opens with different input fields needed for assignments, as shown in Figure 12–27.

Figure 12–27 Task Assignment Rule Dialog Box



The Task Assignment Rule dialog box provides the following options:

- **Rule Name:** A lookup field with a list of the rules.
- **Assignment Types:** A lookup field with the following options for assignment types:
  - Object Administrator User with Least Load
  - Group User with Least Load
  - Request Target Users Manager
  - Object Authorizer User with Highest Priority
  - Object Administrator
  - User
  - Group User with Highest Priority
  - Object Authorizer User with Least Load
  - Requestor's Manager
  - Group
- **Assign To:** A lookup field. The values of this field vary with the selection in the Assignment Types field. Therefore, the value selected in the Assignment Types field is validated first.
- **Adapter:** A lookup field that brings up a list of the available task assignment adapters.
- **Email Template:** A lookup field that opens a dialog box with a list of e-mail templates from which to choose.

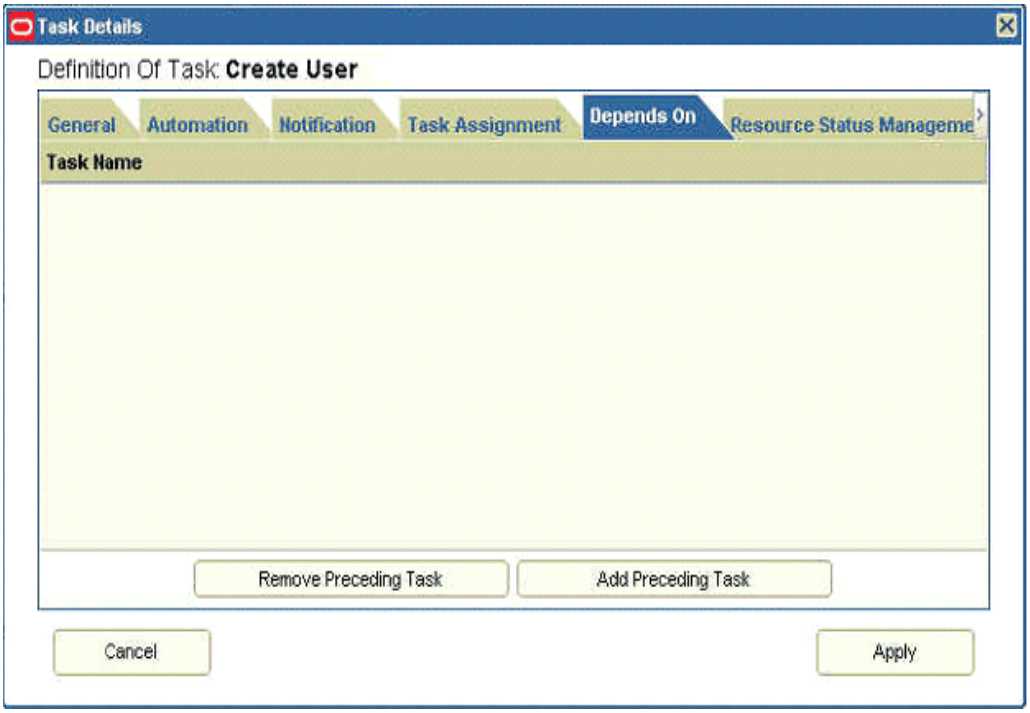
- **Send Email:** A check box. When this is selected, Oracle Identity Manager sends the e-mail notification to a user or user group after the current process task is assigned.
- **Escalation Time (ms):** A text field to specify the amount of time (in milliseconds) in which the user or user group has to complete the process task. The user or user group is associated with the rule that Oracle Identity Manager triggers. If this process task is not completed within the allotted time, then Oracle Identity Manager reassigns it to another user or user group. The escalation rule adheres to the order defined by the assignment type parameter.

When an assignment rule is created, it is displayed in the Task Assignment tab of the Task Details dialog box with a tree structure.

Depends On Tab

Figure 12–28 shows the Depends On tab of the Task Details dialog box.

Figure 12–28 Task Details Dialog Box



This tab lets you add tasks that the current task will depend on. This is useful in setting up dependencies between tasks. This dialog box consists of buttons to add and remove tasks from this list. Any task in this list must be run before the current task is run.

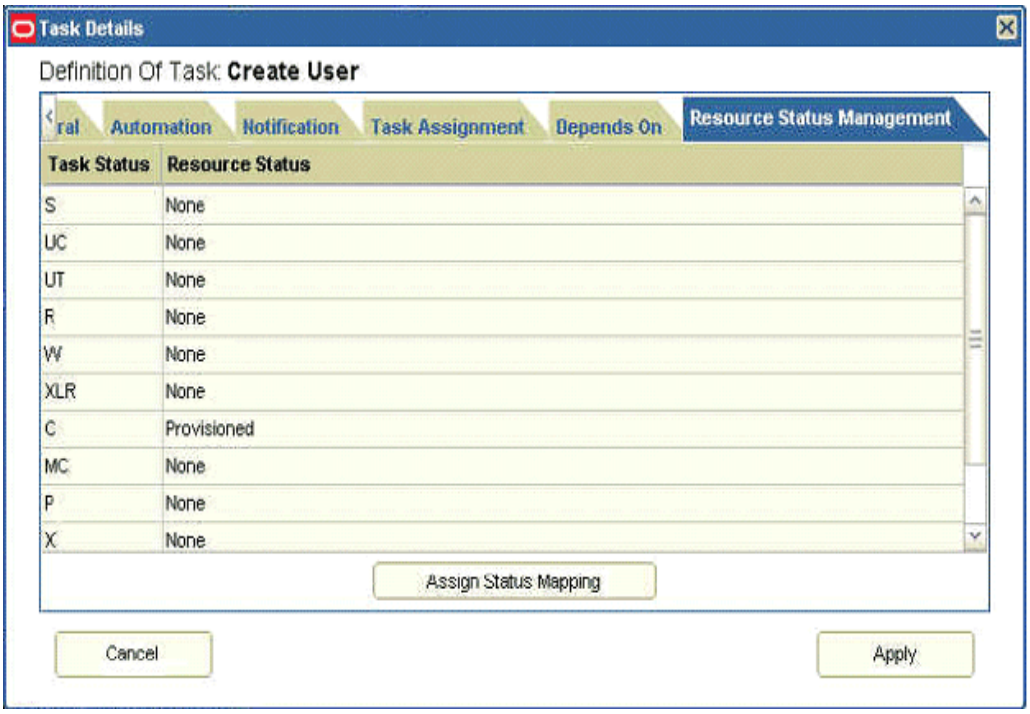
When you click **Add Preceding Task**, the Assign Preceding Task dialog box is displayed. This dialog box list the tasks and the corresponding workflows in which they are used. You can select a task from this list and click **OK**.

When you select a task from the list and click **Remove Preceding Task**, the task is removed from the list.

Resource Status Management Tab

Figure 12–29 shows the Resource Status Management tab of the Task Details dialog box.

Figure 12–29 Resource Status Management Tab



This tab lets you establish a link between the status of a process task and the provisioning status of the resource object to which it is assigned.

A resource object contains data that is used to provision resources to users and applications. This data includes approval and provisioning processes. In addition, a resource object is provided with predefined provisioning statuses. Provisioning status changes through the life cycle of the resource object after the provisioning kicks off. The provisioning status represents the various statuses of the resource object throughout its lifecycle when it is provisioned to the target user or organization. The provisioning status of a resource object is determined by the status of its associated approval and provisioning processes, as well as the tasks that comprise these processes. For this reason, a link between the status of a process task and the provisioning status of the resource object to which it is assigned must be provided.

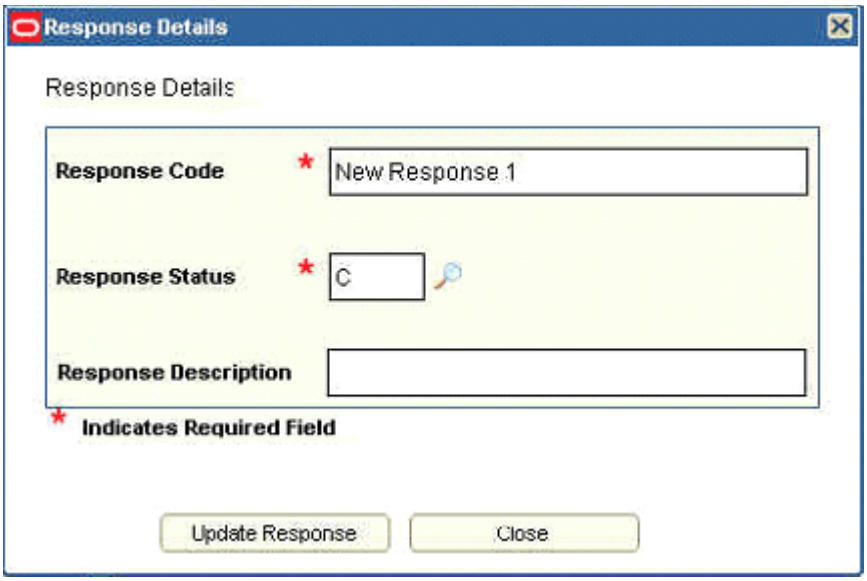
This tab provides two columns that display the tasks status and the resource status. When no mappings are done, the list under the resource status column has a value of `None` for all task status. When you click **Assign Status Mapping**, the Object Status dialog box is displayed. This dialog box has the list of resource statuses from which to select and map to the task status.

After you make changes on all the tabs of the Task Details dialog box, click **Apply** to apply all changes to the task. Alternatively, click **Cancel** to cancel the operation.

12.6.4.6 Configuring Responses

You can double-click a response icon to open the Response Details dialog box that provides options to configure the response. Figure 12–30 shows the Response Details dialog box.

Figure 12–30 Response Details Dialog Box



The Response Details dialog box has the following fields:

- **Response Code:** This field is used to specify the response code. This code for the response uniquely identifies a response for a task.
- **Response Status:** This lookup field is used to select the response status, such as `Cancelled`, `Completed`, or `Rejected`.
- **Response Description:** This field is used to provide a description of the response.

After you specify the response configuration information, click **Update Response** to apply the input for the response. In the designer page, the response code is displayed in the response icon.

12.6.5 Configuring Data Flows

Data flows are used for transferring data to the workflow form fields without the need for the user to enter information. This is used for both provisioning and reconciliation. For provisioning, form data flows are used. For reconciliation, reconciliation data flows are used.

This section discusses the following topics:

- Form Data Flows
- Reconciliation Data Flows

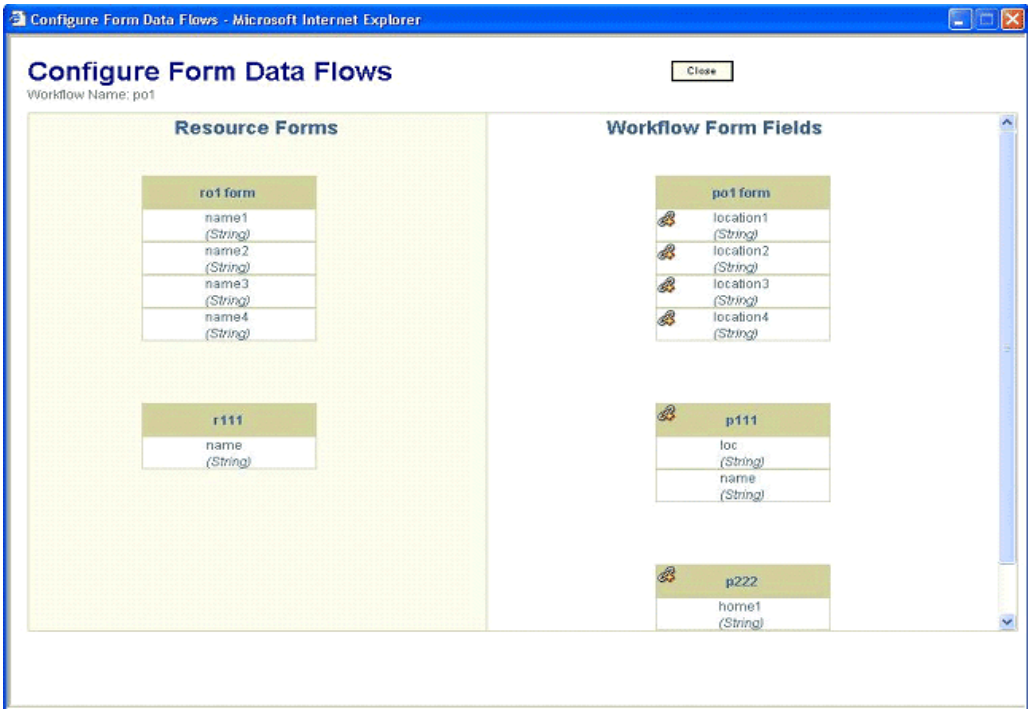
12.6.5.1 Form Data Flows

Form data flows are used to set data flows between the resource form fields and workflow form fields. You can configure data flows in the Configure Data Flows page, which you can open by performing the following steps:

1. In the left navigation pane, click **Resource Management**, and then click **Manage**. The Resource Search page is displayed.
2. Search for a resource.
3. Select the resource by clicking the resource name. The Resource Detail page is displayed.

4. Select **Resource Workflows** from the additional details list. The Resource Workflows page opens.
5. In the Form Data Flow column, the Configure link is displayed only for workflows that have forms attached. The forms can be workflow forms or forms for the associated resource. Click **Configure** to open the Configure Form Data Flows page, which is shown in Figure 12–31.

Figure 12–31 Configure Form Data Flows Page



Adding data flow between fields enables automatic transfer of the form field values from source fields to destination fields. The source fields are from the resource forms and the destination fields are from the process forms.

The form data flow rules are as follows:

- Each destination field can have only one source field. In other words, a process form field cannot act as a destination field for more than one source field.
- A resource parent form field can flow to either a process parent form field or a process child form field.
- A resource child form field can flow to only a process child form field.
- The data flow is always from the resource forms to process forms and never the other way.

The left-hand section of the Configure Form Data Flows page shows the resource forms, and the right-hand section shows the workflow forms and their respective fields. The destination icons are visible in the parent workflow form fields. The link icons are visible in the child tables in the workflow. Clicking a link icon displays the options that you can use to link on the resource forms.

You can click a link on the resource form fields or child table to generate the data flow and to display a link depicting the data flow. The links between the form fields is blue. The link between the child tables at the table level is brown in color.

When a link is established, the icon on the corresponding workflow field or table changes to a broken link icon. You can click the broken link icon to remove the data flow.

12.6.5.2 Reconciliation Data Flows

Reconciliation data flows are similar to form data flows except that the flow is from reconciliation fields to workflow fields instead of between resource fields and workflow fields. For a trusted resource, the user attributes are displayed instead of the workflow form fields. The user interface for reconciliation data flow is also similar to that of form data flows.

The Configure Reconciliation Data Flows page is used to define the relationship between the data elements in the target resource or trusted source and the fields within Oracle Identity Manager with which they are to be linked.

Only the fields defined in the Reconciliation Fields section of the associated resource are available for mappings. These mappings are used to determine which fields in Oracle Identity Manager must be populated with the information provided by using reconciliation events from the target system. In addition, for target resources, the key fields are indicated on this tab. Key fields are fields for which the values on the process form and the reconciliation event must be the same for a match to be generated on the Processes Matched Tree tab of the Reconciliation Manager form.

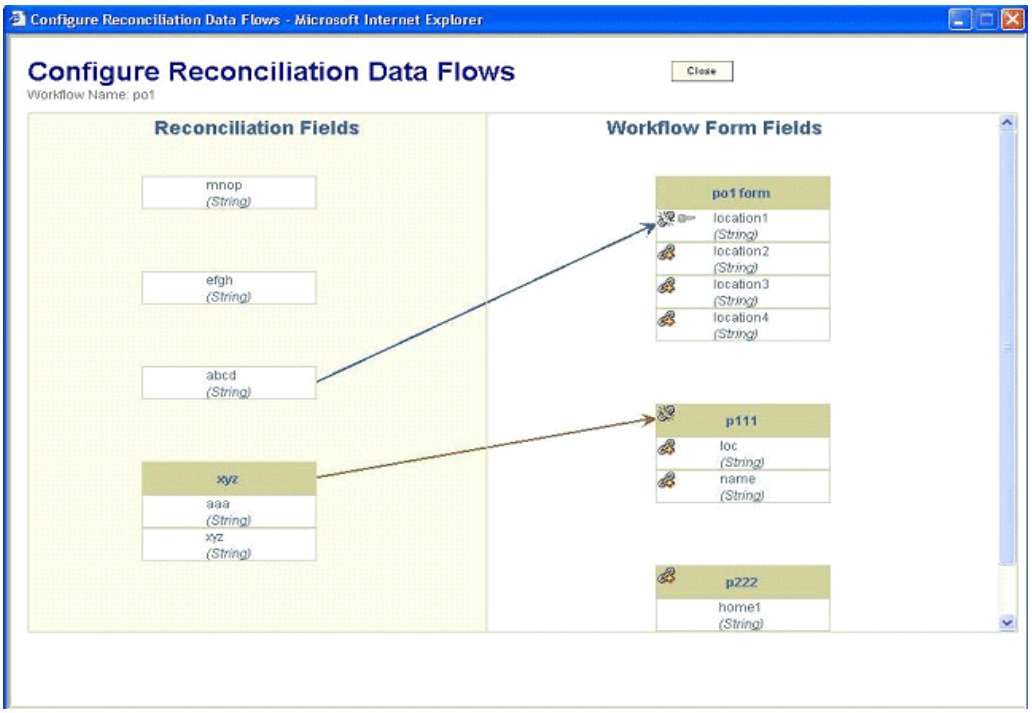
Note: The reconciliation fields created in the Reconciliation Fields tab of the associated resource can be of the types Multi-Valued, String, Number, Date, and IT resource.

You configure reconciliation data flow on the Configure Reconciliation Data Flows page, which is similar to the Configure Form Data Flows page. The reconciliation data flow rules are as follows:

- When a workflow form field or child table is mapped to a reconciliation field, it cannot be mapped to another field unless the first one is removed.
- Each reconciliation field can be mapped only once.

Figure 12–32 shows the Configure Reconciliation Data Flows page.

Figure 12–32 Configure Reconciliation Data Flows Page



An additional property for reconciliation data flows that is not present in the case of form data flows is called the Key Reconciliation field. Each workflow field that is mapped for data flow can be set as a key field for reconciliation. This means that the reconciliation rules corresponding to this field must be met. This is represented in the form of a disabled key icon next to an established data flow. By default, each field is not a key field. To set a field as a key field, click the key icon. Click the key icon again to remove the key field setting.

Clicking the key icon sets the field as a key field, and the icon changes to an enable key icon. Clicking the icon again removes the field as a key field.

See Also:

- The "Workflow Designer Localization" section in *Oracle Identity Manager Globalization Guide* for information about localization in the Workflow Designer
- Appendix A in *Oracle Identity Manager Administrative and User Console Customization Guide* for information about customizing the Workflow Designer
- The "What's New" chapter in *Oracle Identity Manager API Usage Guide* for information about the API methods used by the Workflow Designer

12.7 Creating IT Resources

Note: This feature is in the process of being migrated from the Design Console to the Administrative and User Console. For the current Oracle Identity Manager release, this feature is available in both consoles.

To create an IT resource:

1. Expand **Resource Management**.
2. Click **Create IT Resource**.
3. On the Step 1: Provide IT Resource Information page, enter the following information:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select an IT resource type for the IT resource.

     If you want to create an IT resource of the Remote Manager type, then select **Remote Manager** from the **IT Resource Type** list.
   - **Remote Manager**: If you want to associate the IT resource with a particular remote manager, then select the remote manager from this list. If you do not want to associate the IT resource with a remote manager, then leave this field blank.

     Note: If you select **Remote Manager** from the **IT Resource Type** list, then you must not select a remote manager from the **Remote Manager** list.
4. Click **Continue**.
5. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**.

   The Step 3: Set Access Permission to IT Resource page is displayed. On this page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.
6. On the Step 3: Set Access Permission to IT Resource page, if you want to assign groups to the IT resource and set access permissions for the groups, then:

   a. Click **Assign Group**.

   b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

   c. Click **Assign**.
7. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

   Note: You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

c. Click **Update**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

> **Note:** You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

9. Click **Continue**.
10. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
11. To proceed with the creation of the IT resource, click **Continue**.
12. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Create**. If the test fails, then you can perform one of the following steps:
    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.
    - Proceed with the creation process by clicking **Continue**. You can fix the problem later, and then rerun the connectivity test by using the Diagnostic Dashboard.

> **Note:** If no errors are encountered, then the label of the button is **Create**, not **Continue**.
>
> See "Test Basic Connectivity" on page 16-12 for more information.

13. Click **Finish**.

12.8 Managing IT Resources

> **Note:** This feature is in the process of being migrated from the Design Console to the Administrative and User Console. For the current Oracle Identity Manager release, this feature is available in both consoles.

To locate an IT resource:

1. Expand **Resource Management**.
2. Click **Manage IT Resource**.
3. On the Manage IT Resource page, you can use one of the following search options to locate the IT resource that you want to view:

- IT Resource Name: Enter the name of the IT resource, and then click **Search**.
- IT Resource Type: Select the IT resource type of the IT resource, and then click **Search**.
- Click **Search**.

On the Manage IT Resource page, the list of IT resources that meet the search criteria is displayed.

From this point onward, you can perform one of the following procedures on the IT resource:

- Viewing IT Resources
- Modifying IT Resources
- Deleting IT Resources

12.8.1 Viewing IT Resources

To view an IT resource:

1. From the list of IT resources displayed in the search results, click the IT resource name.

   Note: If you want to edit the IT resource, then click the edit icon in the same row.

2. If you want to view the IT resource parameters and their values, then select **IT Resource Parameters** from the list at the top of the page. Similarly, if you want to view the administrative groups assigned to the IT resource, then select **IT Resource Administrative Groups** from the list.

12.8.2 Modifying IT Resources

To modify an IT resource:

1. From the list of IT resources displayed in the search results, click the edit icon for the IT resource that you want to modify.
2. If you want to modify values of the IT resource parameters, then:
   a. Select **Details and Parameters** from the list at the top of the page.
   b. Make the required changes in the parameter values.
   c. To save the changes, click **Update**.
3. If you want to modify the administrative groups assigned to the IT resource, first select **Administrative Groups** from the list at the top of the page and then perform the required modification.
4. If you want to unassign an administrative group, select the **Unassign** check box in the row in which the group name is displayed and then click **Unassign**.

Note:

- When you click **Unassign**, the administrative groups that you select are immediately unassigned from the IT resource. You are not prompted to confirm that you want to unassign the selected administrative groups.
- You cannot unassign the `SYSTEM ADMINISTRATORS` group.

5. If you want to assign new administrative groups to the IT resource, then:

   a. Click **Assign Group**.

   b. For the administrative groups that you want to assign to the IT resource, select the access permission check boxes and the **Assign** check box.

   c. Click **Assign**.

6. If you want to modify the access permissions of the administrative groups that are currently assigned to the IT resource, then:

   a. Click **Update Permissions**.

   b. Depending on the changes that you want to make, select or deselect the check boxes in the table.

   Note: You cannot change the access permissions of the `SYSTEM ADMINISTRATORS` group.

   c. To save the changes, click **Update**.

12.8.3 Deleting IT Resources

To delete an IT resource:

1. From the list of IT resources displayed in the search results, click the Delete icon for the IT resource that you want to delete.
2. To confirm that you want to delete the IT resource, click **Confirm Delete**.

12.9 Creating Scheduled Tasks

Note:

- This feature is in the process of being migrated from the Design Console to the Administrative and User Console. For the current Oracle Identity Manager release, this feature is available in both consoles.
- If you want to delete a scheduled task, then use the Design Console.
- For information about predefined scheduled tasks, see "Predefined Scheduled Tasks" in *Oracle Identity Manager Design Console Guide*

To create a scheduled task:

1. Expand **Resource Management**.
2. Click **Create Scheduled Task**.
3. On the Step 1: Provide Scheduled Task Details and Schedule page, enter the following information:
   - **Task Name**: Enter a name for the scheduled task.
   - **Class Name**: Specify the Java class for running the scheduled task. To do this, click the magnifying glass icon to open the **Class Name** list of values and then select a class. Alternatively, enter the class name.
   - **Status**: Specify whether or not you want to leave the task in the enabled state after it is created. In the enabled state, the task is ready for use. If the task is disabled, then you must enable it before you can use it.
   - **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.
4. Click **Continue**.
5. On the Step 2: Define Scheduled Task Attributes page, create attributes for the task as follows:
   a. In the **Attribute** field, enter the name of the attribute.
   b. In the **With** field, enter the value of the attribute.
   c. Click **Add**.
   d. Repeat Steps 5a through 5c for each attribute that you want to add.

   Note: Each attribute that you add is displayed in a table. The attributes you add are not posted to the Oracle Identity Manager database until you complete the procedure to create the scheduled task. If required, you can modify the value of a newly added attribute by selecting it from the **Attribute** list, and then editing its value. To delete an attribute, click the cross-shaped icon displayed for that attribute.
6. Click **Continue**.
7. On the Step 3: Verify Scheduled Task Details page, review the information that you provided on the first and second pages. If you want to make changes in this information, click **Back** to revisit the first or second page and then make the required changes.
8. To proceed with the creation of the scheduled task, click **Continue**.
9. If the creation process is successful, then a message stating that the scheduled task has been created is displayed.

12.10 Managing Scheduled Tasks

Note: This feature is in the process of being migrated from the Design Console to the Administrative and User Console. For the current Oracle Identity Manager release, this feature is available in both consoles.

To locate a scheduled task:

1. Expand **Resource Management**.
2. Click **Manage Scheduled Task**.
3. On the Scheduled Task Management page, you can use any one or a combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

Each row of the search results table displays the following information about a scheduled task:

- Scheduled Task: This column displays the name of the scheduled task. If you want to view the details of the scheduled task, then click its name in this column.
- Status: This column displays the status of the scheduled task. The status can be one of the following:
  - `INACTIVE`: The scheduled task has been run successfully, and it is set to run again at the date and time specified in the Next Start field.
  - `RUNNING`: The scheduled task is currently running.
  - `COMPLETED`: The scheduled task has been run successfully, but will not run again (the frequency is set at the **Once** option).
  - `ERROR`: An error was encountered due to which the task could not be started.
  - `FAILED`: The scheduled task failed while running.
- Frequency: This column displays the frequency at which the scheduled task has been set to run.
- Last Start: This column displays the date and time at which the scheduled task began its last run.
- Last Stop: This column displays the date and time at which the scheduled task ended its last run.
- Next Start: This column displays the date and time at which the scheduled task will begin its next run.
- Edit: This column displays the edit icon for each scheduled task. Click the edit icon if you want to modify the task.
- Enable: For a particular scheduled task, if the Enable link is displayed in this column, then it means that the scheduled task is currently disabled and you can enable the task by clicking the **Enable** link. If `Enabled` is displayed, then it means that the task is already enabled.
- Disable: For a particular scheduled task, if the Disable link is displayed in this column, then it means that the scheduled task is currently enabled and you can disable the task by clicking the **Disable** link. If `Disabled` is displayed, then it means that the task is already disabled.

- Run Now: For a particular scheduled task, if the Status column displays INACTIVE and if the gray button is displayed in the Enable column (implying that the task is in the enabled state), then you can run the task by clicking the button in the Run Now column. This button cannot be used if any one of the following conditions is true:
  - The Status column displays RUNNING, which means that the task is currently running.
  - The Enable column displays the green button (and the Disable column displays the gray button), which means that the task must be enabled before it can be run.

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.

The following sections describe the procedures that you can perform by using the features of the Scheduled Task Management page:

- Viewing Scheduled Tasks
- Modifying Scheduled Tasks

12.10.1 Viewing Scheduled Tasks

To view the details of a scheduled task, click the task name in the Scheduled Task column of the search results table displayed on the Scheduled Task Management page.

After viewing the scheduled task details, click **Edit** if you want to modify the scheduled task. Alternatively, you can click **Run now** if you want to run the scheduled task. As mentioned earlier, only a scheduled task that is currently ENABLED can be run.

12.10.2 Modifying Scheduled Tasks

To modify the details of a scheduled task:

1. In the search results table displaying the list of scheduled tasks, click the edit icon in the Edit column of the table.

Note: If you want to run the task, click the task name in the first column of the search results table and then click **Run now**. After you click **Run now**, you need not perform the rest of the steps in this procedure.

If you want to stop a scheduled task while it is running, then use the Stop Execution feature of the Design Console. See "The Task Scheduler Form" in *Oracle Identity Manager Design Console Guide* for information about this feature.

2. On the Scheduled Task Details page, you can modify all the details of the scheduled task, except for the task name and class name. See "Creating Scheduled Tasks" on page 12-50 for information about each GUI element displayed on the Scheduled Task Details page.

3. Click **Continue**.
4. If required, modify the attributes of the scheduled task. You can modify values of existing attributes, delete attributes, or add new ones.
5. Click **Save Changes** to commit all the changes to the database.

13

Using the Deployment Manager

The Deployment Manager is a tool for exporting and importing Oracle Identity Manager configurations. The Deployment Manager lets you export the objects that constitute the Oracle Identity Manager configuration. Usually, you use the Deployment Manager to migrate a configuration from one deployment to another, for example, from a test to a production deployment, or to create a backup of your system.

Important: To use Deployment Manager, JRE 1.4.2 must be installed on any computer that is running the Administrative and User Console.

You can save some or all of the objects in your configuration. This lets you develop and test your configurations in a test environment, and then import the tested objects into your production environment. You can export and import an object and all of its dependent and related objects at the same time. Alternatively, you can export and import each object individually.

This chapter includes the following topics:

13.1 Exporting Deployments

You can export objects from your Oracle Identity Manager system and save them in an XML file. The Deployment Manager has an Export Wizard that lets you create your export file. Add objects by type, one type at a time, for example, user groups, then forms, then processes, and so on. If you select an object that has child objects or dependencies, you have the option to add them or not. After adding objects of one type, you can go back and add other objects to your XML files. When you have all the objects you want, the Deployment Manager saves them all at once in a single XML file.

Note:

- If a user belongs to a group to which the Export menu item has been assigned, then that user can export all the objects that are available for export, regardless of the permissions assigned to the user.

  A system administrator can export any object.

- When user-defined fields are associated with a specific resource object, during the export process one of the following events can occur:

  - If the user-defined fields contain values (entered information), then the Deployment Manager will consider them to be dependencies.

  - If the user-defined fields contain no values (the fields are blank), then the Deployment Manager will not consider them to be dependencies.

To export a deployment:

1. In the left navigation pane of the Administrative and User Console, click **Deployment Management**, then click **Export**.

   The Deployment Manager opens and the Search Objects page of the Export Wizard is displayed.

2. On the Search Objects page, select an object type from the menu, and enter search criteria.

   If you leave the criteria field blank, an asterisk (*) is displayed automatically to find all the objects of the selected type.

3. Click **Search** to find objects of the selected type.

   To select an object, select the option of the object.

4. Click **Select Children**.

   The Select Children page is displayed with the selected objects and all of their child objects.

5. Select the child objects that you want to export.

   To select or remove an item, select the appropriate option.

   Click **Back** to go to the Search Objects page.

6. Click **Select Dependencies**.

   The Select Dependencies page is displayed with any objects required by the selected objects.

7. Select the dependent objects that you want to export.

   To select or remove an item, select the option of the item.

   Click **Back** to go to the Select Children page.

8. Click **Confirmation**.

   The Confirmation page is displayed.

9. Ensure that all the required items are selected, then click **Add for Export**.

After you click **Add for Export**, you can still add more items to this export file.

Click **Back** to go to the Search Objects page.

The Add More page is displayed.

10. Use the wizard to add more items, or finish and exit the wizard. Select the appropriate option and click **OK**.

    If you select **Add more**, repeat Steps 2 through 7. Otherwise, the Export page is displayed.

    The Export page displays your current selections for export. Your selections have icons next to them that indicate what types of objects are selected. The Summary information pane shows the objects you are exporting. The Unselected Dependencies pane displays the list of dependent or child objects that you did not select for export.

11. Make any adjustments to your export file as follows:

    - Click **Reset** to clear the form.
    - Click **Legend** to see icon definitions.
    - Click **Add Object** to restart the wizard and add more items to your export file.

    To remove an object from the Current Selections list:

    - Right-click the object to remove and select **Remove** from the shortcut menu. If the object has child objects, then select **Remove including children** from the shortcut menu to remove the child objects all at the same time.
    - Click **Remove** to confirm. If the object is a child or dependency of a selected item, then it is added to the Unselected Children or Unselected Dependencies list.

    To add an object back to the Current Selections list from the Unselected Children or Unselected Dependencies list,

    a. Right-click the object, and select **Add**.

    b. Click **Confirmation**.

       The Confirmation page is displayed.

    c. Click **Add for Export**.

12. Click **Export**.

    The Add Description dialog box is displayed.

13. Enter a description for the file.

    This description is displayed when the file is imported.

14. Click **Export**.

    The Save As dialog box is displayed.

15. Enter a file name.

    You can browse to find a location.

16. Click **Save**.

    The Export Success dialog box is displayed.

17. Click **Close**.

13.2 Importing Deployments

Objects that were exported into an XML file by using the Deployment Manager can be imported into Oracle Identity Manager by using the Deployment Manager. You can import all or part of the XML file, and you can import multiple XML files at once. The Deployment Manager ensures that the dependencies for any objects you are importing are available, either in the import or in your system. During an import, you can substitute an object you are importing for one in your system. For example, you can substitute a group specified in the XML file for a group in your system.

Note: If a user belongs to a group to which the Import menu item has been assigned, then that user must also have the necessary permissions for the objects that the user wants to import. Without these object-specific permissions, the Import operation fails.

A system administrator can import any object.

This section discusses the following topics:

- Deployment Manager Actions on Reimported Scheduled Tasks
- Importing an XML File

Note: Before importing data that contains references to menu items, you must first create the menu items in the target system.

13.2.1 Deployment Manager Actions on Reimported Scheduled Tasks

A scheduled task is one of the objects that you can import by using the Deployment Manager. Typically, you import a scheduled task into your Oracle Identity Manager environment and later change the values of the scheduled attributes to meet your production requirements. However, if you import the same scheduled task a second time into the same Oracle Identity Manager server, the Deployment Manager does not overwrite the attribute values in the database. Instead, the Deployment Manager compares the attribute value of the reimported XML file to any corresponding attribute values in the database.

The following table summarizes the actions performed by the Deployment Manager during a scheduled task reimport:

Does the Scheduled Task have attribute values in the XML file being imported?	Are there any corresponding attribute values in the database?	Deployment Manager Action
Yes	No	Store attribute values in the database
No	Yes	Delete existing attribute values in the database
Yes	Yes (Newer attribute values indicated by time stamp)	No change in the database
Yes (New attribute values indicated by time stamp)	Yes	Update the database with the new attribute values

13.2.2 Importing an XML File

To import an XML file:

1. In the left navigation pane of the Administrative and User Console, click **Deployment Management**, then click **Import**.
2. Select a file.

   The Import dialog box is displayed.
3. Click **Open**.

   The File Preview page is displayed.
4. Click **Add File**.

   The Substitutions page is displayed
5. To substitute a name, click the **New Name** field adjacent to the item you want to replace, and enter the name.

   You can substitute only items that exist in the target system.
6. Click **Next**. If you are exporting an IT resource instance, then the Provide IT Resource Instance Data page is displayed. Otherwise, you are redirected to the Confirmation page.
7. Modify the values in the current resource instance and click **Next**, or click **Skip** to skip the current resource instance, or click **New Instance** to create a new resource instance.

   The Confirmation page is displayed.
8. Confirm that the information displayed on the Confirmation page is correct.

   To go back and make changes, click **Back**, or click **View Selections**.

   The Deployment Manager Import page displays your current selections.

   The Import page also displays icons next to your current selections. The icons indicate what types of objects are selected. The icons on the right indicate the status of your selections. The file names of any selected files, summary information about the objects you are importing, and substitution information are displayed on the left side of the page. On the right, the **Objects Removed from Import** list displays any objects in the XML file that will not be imported.
9. Make any of the following adjustments:
   - Click **Reset** to clear the form.
   - Click **Legend** to see icon definitions.
   - To remove an object from the Current Selections list, right-click the object, select **Remove** from the shortcut menu, and then click **Remove** to confirm that you want to remove the object.

     If the object has child objects, then select **Remove including children** from the shortcut menu to remove all the child objects at the same time. The item is added to the Objects Removed From Import list.
   - To add an item back to the Current Selections list, right-click the list, and click **Add**.

     If the object has child objects, then select **Add including children** from the shortcut menu to add all the child objects at the same time.
   - To make substitutions, click **Add Substitutions**.

- To add objects from another XML file, click **Add File** and repeat Steps 2 through 7.
- Click **Show Information** to see information about your imported information.

  The Information page is displayed.

  To see more information, select the **Show Info Level Messages** option, and then click **Show Messages**. Click **Close** to close the Information page.

10. To import the current selections, click **Import**.

    A confirmation dialog box is displayed.

11. Click **Import**.

    The Import Success dialog box is displayed.

12. Click **OK**.

    The objects are imported into Oracle Identity Manager.

13.3 Best Practices Related to Using the Deployment Manager

The following are some of the suggested practices and pitfalls to avoid while by using Deployment Manager:

- Do not export system objects.
- Group definition data and operation data separately.
- Use logical names for form versions.
- Enter meaningful descriptions when exporting.
- Check all warnings before performing any imports.
- Check the required dependencies in the target system before performing any exports.
- Understand how scheduled task attributes are affected by imports.
- Compile adapters and enable scheduled tasks.

  Note: This release onward, the Deployment Manager is able to compile adapters automatically while importing the XML file. For more information about automatic adapter compilation, see Chapter 9 of *Oracle Identity Manager Tools Reference*.

- Export entity adapters separately with only essential mappings, and then manually create the required mappings.
- Back up the database before importing it into the production environment.
- Ensure that the correct version of the form is active during a user-defined form import.
- Perform imports during periods of low activity in the system.

  See Also: *Oracle Identity Manager Best Practices Guide* for more information about best practices related to using the Deployment Manager

14

Working with Reports

You can generate operational and historical data reports by using Oracle Identity Manager. These reports provide information about the resources available to Oracle Identity Manager users.

This chapter discusses the following topics:

> **Note:** The Oracle Identity Manager reporting engine is not meant to be a replacement for enterprise reporting solutions. The Oracle Identity Manager reporting engine is not optimized for very large data volume and does not provide the rich features you would find in an enterprise reporting application.
>
> For large-scale deployments, especially those taking advantage of the extensive auditing capabilities of Oracle Identity Manager, it is highly recommended that you deploy a dedicated enterprise-class reporting solution. A solution based on tools such as Oracle Business Intelligence Enterprise Edition can provide the flexibility, automation, and performance required for a large-scale organization.

14.1 Overview of Operational Reports

The following sections describe the default operational reports in Oracle Identity Manager. These reports can be used by Oracle Identity Manager administrators and auditors for operational and compliance purposes.

Table 14–1 lists the operational reports available in the Administrative and User Console.

Table 14–1 List of Operational Reports

Name	Description
Entitlements Summary	Lists the number of users for each status type within each resource.
Policy List	Displays a snapshot of all policies defined within the system.
Delegated Administrators By Organization	Lists all the delegated administrator user groups for organizations.
Attestation Requests by Reviewer	Lists attestation requests by reviewer.
Approval Status By Approver	Provides a summary of all approval tasks.
User Resource Access	Lists the access rights to resources for selected users.
Resource Access List	Lists all users who have access to a selected resource.
Policy Detail	Lists complete details about specific policies defined within the system.
Group Membership Profile	Lists the number of users in different numbers of groups.
OIM Password Expiration	Lists users whose Oracle Identity Manager passwords are about to expire.
Group Membership	Provides a snapshot of users in each group.
Resource Password Expiration	Lists users whose resource passwords are about to expire (as determined by Oracle Identity Manager).
Organization Structure	Lists the hierarchical organization structure and user memberships.
Requests Initiated	Lists all requests initiated in a specified time interval.
Requests Details By Status	Returns details of all requests with a specified status.
Attestation Process List	Provides a snapshot of all defined attestation processes.
Attestation Requests by Process	Lists attestation requests by process.
Attestation Request Detail	Lists complete details of selected attestation requests.
Financially Significant Resources	Lists complete details of financially significant resources.
Delegated Administrators & Permissions By Organization	Lists all administrator user groups and permissions for organizations.
Delegated Administrators & Permissions By Resource	Lists all administrator user groups and permissions for resources.
Delegated Administrators By Resource	Lists all administrator and authorizer user groups for resources.

14.2 Overview of Historical Reports

The following sections describe the historical data reports in Oracle Identity Manager. These reports can be used by administrators and auditors for compliance and auditing purposes.

Table 14–2 lists the historical reports that are available in the Administrative and User Console.

Table 14–2 List of Historical Reports

Name	Description
User Resource Access History	Returns the history of a user's resource access.
Resource Access List History	Returns a history of all users who have had access to a selected resource.
User Profile History	Returns the history of a user's profile.
User Membership History	Returns the history of a user's memberships in a user group.
Group Membership History	Returns the history of a group's memberships.
Resource Activity	Returns the history of all provisioning and approval activities for a resource.
Task Assignment History	Returns the history of all task assignment based on the tasks.
Password Reset Success Failure	Returns the password change metrics for Oracle Identity Manager users.
Account Activity In Resource	Lists all account activities in each resource.
Rogue Accounts By Resource	Lists all the rogue accounts in each resource. **Note**: This report is available only if the exception reporting feature is enabled. For more information, see Chapter 5, "Oracle Identity Manager Reporting" of *Oracle Identity Manager Audit Report Developer's Guide*.
Fine Grained Entitlement Exceptions By Resource	Lists all fine-grained entitlement exceptions associated with a resource. **Note**: This report is available only if the exception reporting feature is enabled. For more information, see Chapter 5, "Oracle Identity Manager Reporting" of *Oracle Identity Manager Audit Report Developer's Guide*.
Users Created	Lists all users created in a specified time interval.
Users Deleted	Lists all users deleted in a specified time interval.
Users Disabled	Lists all users disabled in a specified time interval.
Users Unlocked	Lists all users (accounts) unlocked in a specified time interval.

See Also: These reports are also listed in Chapter 5 of *Oracle Identity Manager Audit Report Developer's Guide*.

14.3 Running Reports

To run a report:

1. In the left navigation pane, click **Reports**, and then click **Operational Reports** or **Historical Reports**.

   The resulting page displays a list of all the reports of that type that are available to the user. The reports are listed in a table with the following fields:

Field	Description
Report Name	Shows the unique name of the operational report, which is also a link to input parameters for that report
Report Code	Identifies a unique alpha numeric code for the report
Report Type	Identifies the report type to help administrators organize their reports

Field	Description
Report Description	Provides a short description of the report

2. Select a report by clicking its name.

   The Report Input Parameters page is displayed. This page displays the input parameters that must be provided to run a report. In some cases, at least one or more input parameter fields are required fields. If this is not the case, then you must populate at least one of the fields to run a report.

   Note: A few reports, for example, the Delegated Administrators & Permissions By Resource and Delegated Administrators & Permissions By Organization reports do not require any input parameters to run.

3. Enter the information required to identify what information the report contains.
4. Click **Submit** to run the report.

   The Report Display page is displayed.

14.4 Display of Data in Report

The Report Display page shows the report contents. Several display formats are available. The format information is included in the report metadata associated with each report. The display formats are:

- Tabular Format
- Sectional Format
- Sectional with Header Format

By default, only 50 records appear on each page. This limit can be changed in the properties file. If there are multiple pages, the First, Previous, Next, and Last navigation links at the top and bottom of the page are active.

14.5 Using Report Filters

You can use a filter to narrow the search criteria for a report. By default, the filters appear as a menu and a text field. Select the type of data from the menu, and then enter a filter string in the text field. The asterisk (*) wildcard character can be used in the filter field. An asterisk represents any number of characters. For example, `S*t` will match `Slashdot` and `Sat`. Filter criteria that represent lookup fields, such as user status and employee type, have boxes from which you can select values.

Filters narrow down the existing report, they do not generate a new report. For example, if the report is run with the input parameter as `[First Name=j*]` (return all records where the first name starts with 'j'), and it is filtered again with `[Last Name=Smith]`, then the report returns only records that have a first name starting with `j` and a last name of `Smith`.

For historical reports that include user status as a filtering parameter, the search is performed on historical data. For example, specifying a filter criterion of `[User Status=Active]` returns all users who were active at some point in the past, even if they are currently system administrators.

After you create the filter and click **Filter**, the resulting report is displayed on the same Report Display page. The filter menu and fields reflect the filter values that were provided. Clicking **Clear** empties the filter fields.

14.6 Change Input Parameters

Click **Change Input Parameters** to return to the Input Parameters page. The input parameter fields contain the information you already entered.

14.7 CSV Export

You can export all the report information as a single Comma Separated Values file, or CSV. Click **CSV Export** and at the prompt, choose to save the CSV file locally on your computer. By default, the name of the file is `report code.csv`.

14.8 Detail Page Links

The resource names and user IDs listed in the report may be links. Clicking these links opens a new Detail page with more detailed information about that resource or user ID.

14.9 Creating Reports Using Third-Party Software

Oracle Identity Manager supports the creation of reports by using third-party tools such as Crystal Reports. You can use a third-party tool to create the operational reports listed in "Overview of Operational Reports" on page 14-1 or the historical reports listed in "Overview of Historical Reports" on page 14-2.

Note: To learn how to create reports by using third-party software, see the third-party software documentation.

15

Working with the Attestation Feature

This chapter is divided into the following sections:

15.1 About Attestation

Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe provisioned resources of other users. A reviewer can attest to the accuracy of the entitlements by providing a response. The attestation action, along with the response the reviewer provides, any associated comments, and an audit view of the data that the reviewer views and attests to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an **attestation task**.

In Oracle Identity Manager, attestation is supported through the definition of scheduled attestation processes. An attestation process is not the same as an Oracle Identity Manager workflow. It is implemented as a configurable business process in Oracle Identity Manager, and it creates an attestation task for a user. The user acts as a reviewer, and must complete this process to provide correct audit information.

Tracking of attestation activity for a provisioned resource instance is done through tasks in the provisioning processes of resource objects. You can initiate workflow activity based on attestation actions. Additional activities to be started, and a workflow that can be modeled in the process definition form or workflow designer can be initiated, based on an initial attestation action. This is possible due to attestation subflows in the provisioning processes defined in Oracle Identity Manager.

Attestation activity can be initiated on a periodic basis or when required.

A reviewer can delegate specific entitlements in an attestation task to another user for review. This action creates another attestation task that is assigned to the delegated user.

This section discusses the following topics:

- Delegation
- Attestation Lifecycle Process
- Attestation Engine
- Attestation Scheduled Task
- Attestation-Driven Workflow Capability
- Attestation E-Mail

15.1.1 Definition of an Attestation Process

An **attestation process** is the mechanism by which an attestation task is set up. Input that an attestation process requires includes information about how to define the components that constitute the attestation task and how to associate the attestation task with a schedule at which the task must be run. This definition is also the basis on which the attestation task can be initiated when required. An attestation process definition includes:

- **Attestation Scope**: This defines the algorithm by which the target user entitlements of the attestation process are determined.
- **Reviewer Setup**: This specifies the reviewer.
- **Definition of Attestation Schedule**: This specifies the schedule for running the attestation process.
- **Process Owner**: This is a designated group of users that are responsible for monitoring activities related to the process.
  - They will be notified of any issues that occur when the process runs.
  - They will have permissions to view the process definition, but will not have administrative permissions by default.
  - They will be able to execute the process whenever required.
- **Process Administrators**: These are the groups of users that have administrative permissions over the process definition. This essentially maps to the typical delegated administrator model.

A single attestation process could result in multiple attestation tasks, if that process defines a set of reviewers. In such a case, the process would result in one attestation task for each reviewer in the set.

15.1.1.1 Attestation Process Control

The following sections describe how you can control attestation processes.

15.1.1.1.1 Disabling Processes An attestation process can be disabled by the system administrator to prevent it from running at its preconfigured schedule. This gives an administrator better control over the environment. A system administrator attestation process can be enabled, but it cannot be enabled if its Next Run Time value is in the past. A user who enables an attestation process must set its next run time in the future.

15.1.1.1.2 Deleting Processes An attestation process can be deleted. This is called a soft delete. It does not actually delete the records because the records must be maintained for audit purposes. Instead, the attestation process will be marked as deleted.

A deleted process is not displayed in the Administrative and User Console. Because process names and codes are unique, a name once used is no longer available, and no new attestation process can be created with the same name.

15.1.2 Components of Attestation Tasks

The basic purpose of the attestation process is to set up an attestation task in Oracle Identity Manager. The attestation task is displayed in a user's attestation inbox. The following are the basic components of an attestation task:

- **A Reviewer**: This specifies the user who performs the attestation.
- **Task Source**: This specifies whether or not the attestation task is a result of a process or because of delegation by another reviewer. In the case of delegation, the task must track the reviewer who delegated the task, and which task is the source of the entitlements.
- **Attestation Data**: This is detailed data about user entitlements in the attestation scope. This data is from the process form of the provisioned resource instance
- **Attestation Date**: This defines the date on which the attestation task is initiated.
- **Attestation Actions**: These are the actions that the reviewer can take on the attestation scope. The action is not at the overall attestation task level, but rather against each entitlement in the attestation scope. The following are attestation actions:
  - **Certify**: The reviewer certifies that the user being reviewed is allowed to have this entitlement in the form with the data and fine-grained permissions that it has.
  - **Reject**: The reviewer does not think that the user must have this entitlement in the form.
  - **Decline**: The reviewer does not want to accept the responsibility of attesting to the entitlement. This action is usually for cases in which processes have been configured incorrectly, and is useful in the early stages of a rollout.

    A reviewer declines a task when the reviewer wants someone else to act upon the task. When a task is declined, it gets assigned to a random user in the attestation administrator group.
  - **Delegate**: The reviewer wants to reassign the attestation of this entitlement to another qualified person.

Note: The attestation tasks are not workflow tasks in the Oracle Identity Manager definition. They are not created as part of workflow. Attestation tasks do not support all the task management features that the workflow engine supports, for example, dynamic assignment, escalation, and proxy management.

15.1.2.1 Attestation Inbox

The attestation inbox enables you to manage attestation tasks that are assigned to you.

From this inbox, you can see the attestation tasks assigned to you, view the details of the tasks, and provide responses and comments.

15.1.3 Attestation Request

When an attestation process is executed, an attestation request is created and recorded in the Oracle Identity Manager database. This request acts as an audit record of the times that an attestation process is executed. The attestation request record consists of basic identity and audit data and statistical data that is used in reports. The data includes the following items:

- A request ID: Each attestation task that is created as a result of a request stores the request ID as part of its record.
- Date and time of execution of the process.
- Date and time of completion of the process: The date and time of completion of the process is considered to be the date and time for that request.
- Total number of entitlements identified for attestation.

  The number of entitlements is as follows:

  ```
  Total Number of Entitlements = Number Certified + Number
  Rejected + Number Declined
  ```

- Number of entitlements certified.
- Number of entitlements rejected.
- Number of entitlements declined.

15.1.4 Delegation

The reviewer who is assigned to an attestation task may not be able to attest to all the entitlements in the task. There may be multiple reasons for this, for example:

- There may be too many entitlements covering too many users in the attestation task
- The reviewer is not sure about the reasons for which the entitlements were provisioned

In these cases, the reviewer may want to involve other people in the review. A reviewer can delegate attestation of certain entitlements in the task.

To delegate attestation, the reviewer selects a set of entitlements in the task and delegates them to another user. This creates a new attestation task that is assigned to the selected reviewer.

> **Note:** A reviewer can view the list of users available for delegation only if the user is a member of a group that has read permissions for the organization to which the users belong. However, if the reviewer is an administrator with read permissions, the reviewer can view all the users available in the organization for delegating the tasks.

The new task contains only those entitlements that the original reviewer selected. The original reviewer is no longer responsible for providing an attestation response for those entitlements. The new attestation task assigned to the delegate would track who performed the delegation, which task it was created from, and some other information, for example, the request ID. The new attestation task is treated in the same manner as any other attestation task. It can even be delegated.

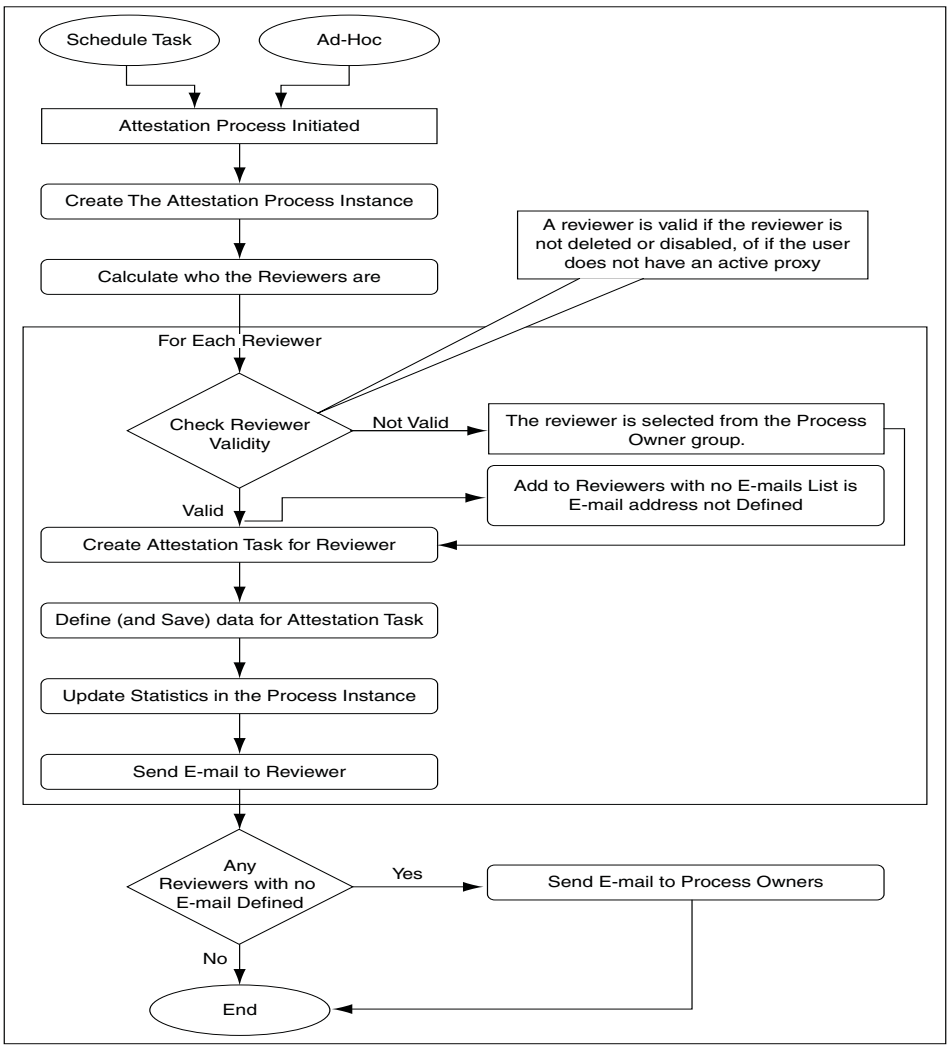
15.1.5 Attestation Lifecycle Process

The following is a description of the attestation lifecycle in Oracle Identity Manager.

15.1.5.1 Stage 1: Creation of an Attestation Task

This stage starts when an attestation process is run. Figure 15–1 describes the workflow involved in this stage.

Figure 15–1 Creating an Attestation Task: Workflow



When the attestation process is run, it first creates a corresponding attestation process instance. It then identifies the reviewers for this run of the process. In most cases, there is only one reviewer. There can even be a set of reviewers.

Whenever an invalid reviewer is found, a new reviewer is fetched from the process owner group. The user that has not yet been used in the attestation request is the highest priority user from the group. Alternatively, if all users are used, then the next priority user from the process owner group is fetched. If no user is found from this process, then the task is assigned to XELSYSADM.

For each valid reviewer, the process calculates all the user entitlements that the reviewer must attest to as part of that task, as determined by the attestation scope defined in the process. The process then adds a reference and any related information

regarding those user entitlements to the attestation data of the task. It also adds the number of entitlements covered by that task to the statistical field for the total number of entitlements identified for attestation in the process instance. The process then sends an e-mail message to the reviewer. It also sends e-mail to process owners about the reviewers with no e-mail address defined.

At the end of this stage, all the attestation tasks are in the attestation inboxes of the reviewers.

15.1.5.2 Stage 2: Acting on an Attestation Task

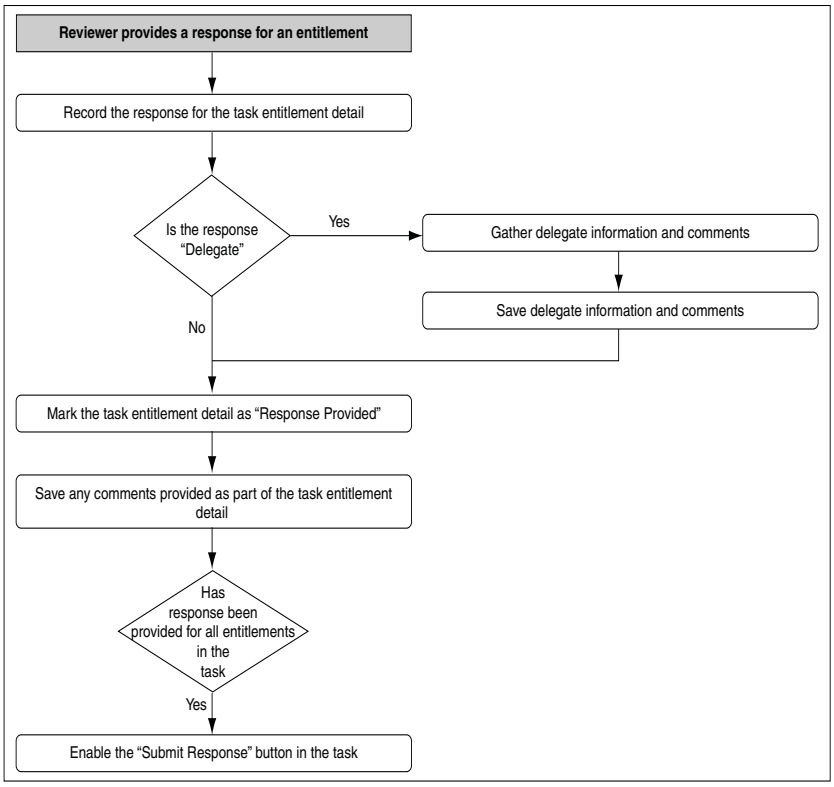
When an attestation task is assigned to a reviewer, the reviewer receives an e-mail, and the task is displayed in the reviewer's attestation inbox. The reviewer views task details in this inbox.

From the task details page, the reviewer provides a response and, if required, a comment for each entitlement. This marks the attestation entitlement detail in the task as **Response Provided**.

If the reviewer's response includes delegating the attestation activity for a specific entitlement, then the reviewer must provide a delegated user. Optionally, the reviewer can provide comments explaining why the reviewer is delegating the attestation activity to that user.

After the reviewer provides responses to all entitlements, the reviewer can commit their action for the attestation task by submitting all responses.

Figure 15–2 Flow of Events When Reviewer Responds to Entitlement



At this point, the next stage of the Attestation Business Process begins.

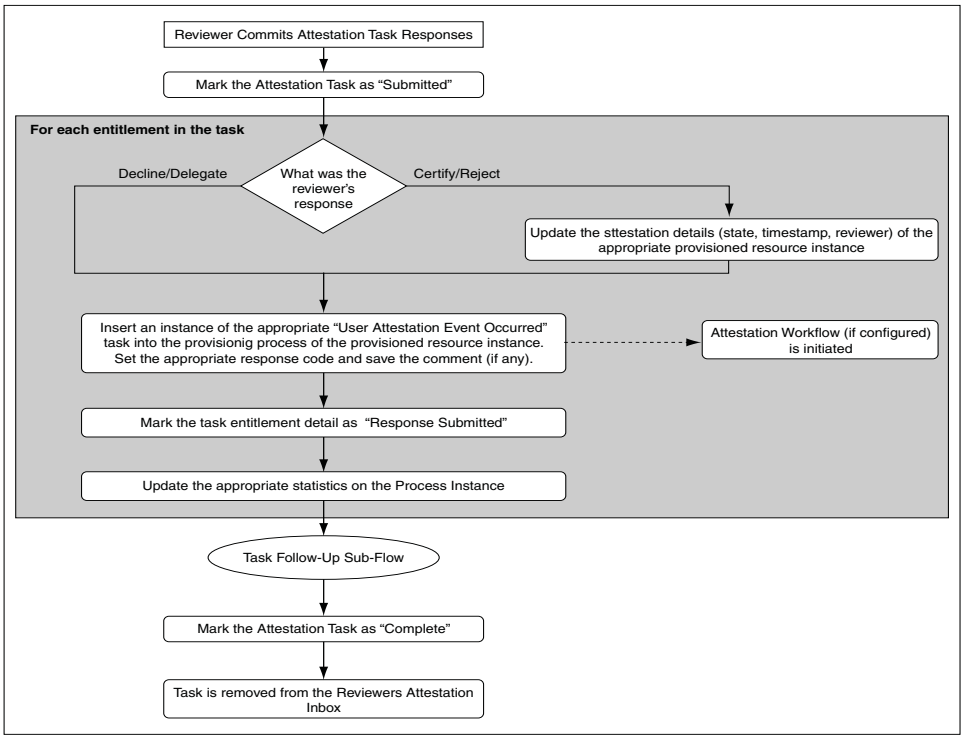
15.1.5.3 Stage 3: Processing a Submitted Attestation Task

The Attestation Task is marked as **Submitted**. At this point the attestation task is frozen, and cannot be acted on further. For each entitlement in the attestation task, the response is examined by the system. If the response is to either certify or reject, then the provisioned resource instance corresponding to that entitlement is updated accordingly. At the provisioned resource instance level, the last attestation result, the time at which last attestation occurred, and who the reviewer was are recorded. If the response is to decline or delegate, then the attestation detail at the provisioned resource level is not changed.

The **User Attestation Event Occurred** task is inserted into the provisioning process of the resource instance. This starts any attestation-driven workflows that may have been defined. Any comments are saved to the notes field of the task.

The attestation entitlement detail in the task is marked as **Response Submitted**. Figure 15–3 shows the flow of events after the attestation task response is submitted.

Figure 15–3 Flow of Events After Attestation Task Response Is Submitted



The following statistics are updated on the process instance:

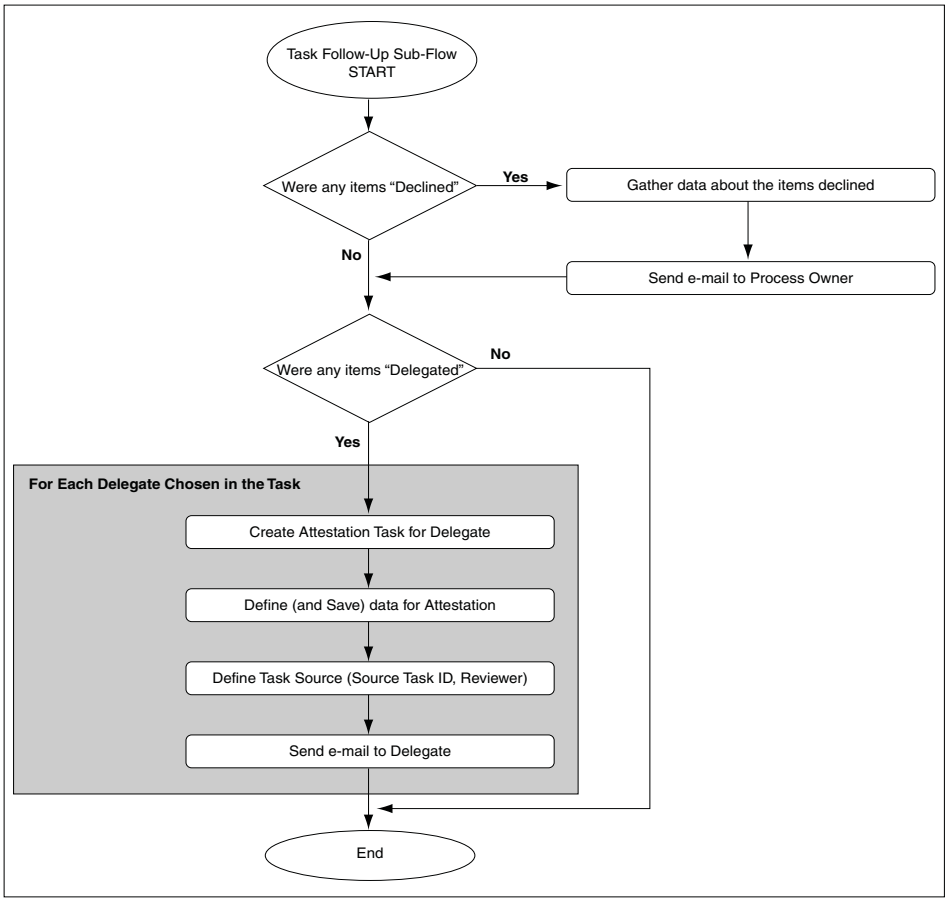
- Number of entitlements certified
- Number of entitlements rejected
- Number of entitlements declined
- Number of entitlements delegated

After all entitlements are covered, a subflow for follow-up action is initiated. In this flow, the process examines if the response for any of the entitlements in the task was declined. If there were any such entitlements, then the process sends e-mail to the Process Owner outlining the details of the decline action.

Next, the process examines if the response for any of the entitlements in the task was delegated. If there were any such entitlements, then the process identifies all the users that the reviewer selected as delegates and creates an attestation task for each. Each attestation task is only for the entitlements that the reviewer delegated to the user. The delegated user receives e-mail notification about the delegation.

After all the delegated attestation tasks are created, the subflow is completed and it merges back into the main flow. Figure 15–3 shows the flow of events of the follow-up action subflow.

Figure 15–4 Follow-Up Action Sub-Flow



With the follow-up subflow complete, the attestation task is marked as **Complete**.

15.1.6 Attestation Engine

The attestation engine implements the attestation lifecycle. It is a service in the Oracle Identity Manager architecture that exposes APIs to receive instructions to initiate a particular attestation process. The API is called from the attestation scheduled task as well as from the Run Now button on the Attestation Process Detail page to support on-demand execution. It supports both drivers for initiation of attestation processes.

The attestation engine uses the JMS messaging service to perform offline, queued processing. This feature ensures better performance.

Note: Attestation depends on the entry in the user profile audit data. If the audit entry is not generated for a user who is part of the attestation process, then the reviewer would not be able to see the user and process form information in attestation. To avoid such situations, ensure that the `Issue Audit Messages Task` scheduled task is run before performing the attestation run.

15.1.7 Attestation Scheduled Task

This new system scheduled task is responsible for examining the attestation processes defined in Oracle Identity Manager, and creating the necessary attestation tasks in the system.

Features of this scheduled task are:

- By default, this scheduled task is set to run every night. You can change the schedule according to your requirements.
- This scheduled task examines the attestation process definition table for all active (not system administrator) attestation processes
- If the scheduled task finds that the next scheduled start time of a process is in the past, then the task sends a call to the Attestation Engine to initiate the attestation process.

15.1.8 Attestation-Driven Workflow Capability

You can enhance the provisioning processes predefined in Oracle Identity Manager to listen to triggers coming from attestation activity. In this way, you can define custom workflows as part of the provisioning workflow that would respond to attestation taking place (or not taking place, in case of a refusal), and therefore be initiated when attestation takes place. This serves two purposes:

- The default attestation task in the flow, User Attestation Event Occurred, would provide the audit trail for the attestation history of the specific user entitlement.
  - There is one instance of this task for each time that resource instance is attested by the appropriate type of attestation process.
  - The response code set on the task indicates what the response provided by the reviewer is.
  - The user tagged as the person creating the task indicates who the reviewer is.
  - Any comment provided by the user is in the notes field for the task.
- Using response-generated tasks, the default task can start the workflow to respond to a particular attestation response received. Therefore, for a particular resource, you can specify that the Reject response must start the appropriate workflow tasks in the provisioning process for disabling the account, as an example.

15.1.9 Attestation E-Mail

As part of the attestation processes, the Attestation Engine sends out e-mail to various interested parties. To make the e-mail configurable with respect to the content, they are made available as e-mail templates of the General type in the Oracle Identity Manager Email Definition store. For context-sensitivity, the e-mail contain a set of variables that can be replaced with the required values.

15.1.9.1 Notify Attestation Reviewer

This template is used to build the e-mail to send to the reviewer when an attestation task is assigned to the reviewer.

15.1.9.1.1 Variables The following are variables in the Notify Attestation Reviewer template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task was assigned

15.1.9.1.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Attestation Reviewer template:

```
A new attestation task for attestation process Attestation Definition.Process Name
has been added to your attestation inbox
```

15.1.9.1.3 Body The body of the e-mail message contains the following information:

```
The attestation task details are as follows
Process Name: Attestation Definition.Process Name
Process Code: Attestation Definition.Process Code
Data Type: Access Rights
Assigned Date: Attestation Task.Task Assigned Date
```

15.1.9.2 Notify Delegated Reviewers

This template is used to build the e-mail to send to a reviewer when an attestation task is delegated to the reviewer.

15.1.9.2.1 Variables The following are variables in the Notify Delegated Reviewers template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task is assigned
Attestation Task.Delegated By First Name	First name of the reviewer who performed the delegation
Attestation Task.Delegated By Last Name	Last name of the reviewer who performed the delegation
Attestation Task.Delegated By User Id	User ID of the reviewer who performed the delegation action

15.1.9.2.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Delegated Reviewers template:

```
Attestation Task.Delegated By User Id has delegated to you an attestation task
from attestation process Attestation Definition.Process Name
```

15.1.9.2.3 Body The body of the message contains the following information:

```
The attestation task details are as follows
Process Name: Attestation Definition.Process Name
Process Code: Attestation Definition.Process Code
Data Type: Access Rights
Assigned Date: Attestation Task.Task Assigned Date
Delegated By: Attestation Task.Delegated By First Name Attestation Task.Delegated
By Last Name [Attestation Task.Delegated By User Id]
```

15.1.9.3 Notify Process Owner About Declined Attestation Entitlements

The Notify Declined Attestation Entitlements template is used to build the e-mail to send to process owners notifying them of any declined entitlement attestations.

15.1.9.3.1 Variables The following are variables in the Notify Process Owner about Declined Attestation Entitlements template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request
Attestation Definition.Process Name	Name of the attestation process
Attestation Task.Reviewer First Name	First name of the reviewer
Attestation Task.Reviewer Last Name	Last name of the reviewer
Attestation Task.Reviewer User Id	User ID of the reviewer
Attestation Data.Provisioned User First Name	First name of the user being attested
Attestation Data.Provisioned User Last Name	Last name of the user being attested
Attestation Data.Provisioned User User Id	User ID of the user being attested
Attestation Data.Resource Name	Name of the resource being attested
Attestation Data.Entitlement Descriptive Data	Descriptive data of the entitlement being attested

15.1.9.3.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Process Owner About Declined Attestation Entitlements template:

```
User access rights in attestation request Attestation Request.Request Id have been
declined by Attestation Task.Reviewer User Id
```

15.1.9.3.3 Body The following is displayed in the body of the message:

```
Attestation of the following user access rights were declined by the reviewer.
Reviewer: Attestation Task.Reviewer First Name Attestation Task.Reviewer Last Name
[Attestation Task.Reviewer User Id]
Attestation Process: Attestation Definition.Process Name
Attestation Request ID: request Attestation Request.Request Id
Access Rights Data: Attestation Data.Provisioned User First Name Attestation
Data.Provisioned User Last Name [Attestation Data.Provisioned User User Id] -
Attestation Data.Resource Name - Attestation Data.Entitlement Descriptive Data
```

15.1.9.3.4 Special Comments Each entitlement data item will appear on a new line.

15.1.9.4 Notify Process Owner About Reviewers with No E-Mail Defined

The Attestation Reviewers With No Email Defined template is used to build the e-mail to send to process owners notifying them of reviewers for whom there is no e-mail address defined.

15.1.9.4.1 Variables The following are variables in the Notify Process Owner About Reviewers with No Email Defined template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request
Attestation Definition.Process Name	Name of the attestation process
Attestation Request.Request Creation Date	Date when the attestation request was created
Attestation Task.Reviewer First Name	First name of the reviewer that is invalid
Attestation Task.Reviewer Last Name	Last name of the reviewer that is invalid
Attestation Task.Reviewer User Id	User ID of the reviewer that is invalid

15.1.9.4.2 Subject Line The following is the Subject line for e-mail defined by the Notify Process Owner About Reviewers with No Email Defined template:

```
E-mail address is not defined for some of the reviewers in attestation process
Attestation Definition.Process Name, request Attestation Request.Request Id
```

15.1.9.4.3 Body The following is the body of the message:

```
The following attestation reviewers do not have e-mail addresses defined.
Attestation requests have been generated for these reviewers and can be accessed
by logging in to Oracle Identity Manager. However, notification e-mails were not
sent.
Attestation process: Attestation Definition.Process Name
Attestation Request ID: request Attestation Request.Request Id
Request date: Attestation Request.Request Creation Date
Reviewers Without Email: Attestation Task.Reviewer First Name Attestation
Task.Reviewer Last Name [Attestation Task.Reviewer User Id]
```

15.1.9.4.4 Special Comments Each reviewer detail appears on a new line.

15.2 Attestation Process Configuration

A menu item in the Administrative and User Console provides access to the Attestation Process Configuration pages. Oracle Identity Manager administrators can use these pages to:

- Define new attestation processes.
- Manage existing processes.
- Initiate ad-hoc attestation processes.

15.2.1 Menu Structure

The top-level Attestation menu contains the following links:

- Create
- Manage
- Dashboard

These menu items are governed by the same delegated administration permissions that govern all menu items in the Administrative and User Console.

These menu items are defined but not assigned to any group in Oracle Identity Manager. They will be assigned to the System Administrators group in Oracle Identity Manager if audit compliance components are installed.

15.2.2 System Control

Attestation has the following dependencies:

- The User Profile Audit feature must be enabled.
- Historical data must be collected at least up to the Process Form level.

If the auditing level is set below the required levels, then clicking menu item links related to attestation generates the Attestation Feature Not Available page, and prevents the user from defining any attestation processes.

Audit levels are controlled by the system property called `XL.UserProfileAuditDataCollection` and the attestation feature expects this value to be set to at least `Resource Form`.

15.3 Creating Attestation Processes

Note: The Oracle Identity Manager Permission model applies to the procedure described in this section. This model restricts any list of targets (for example, users) to only those targets for which the logged-in user has read access.

To create an attestation process:

1. In the left navigation pane, expand the **Attestation** menu, and then click **Create**.

   The Step1: Define Process page is displayed.

2. Enter values for the fields described in the following table, and then click **Continue**:

Field	Description
Name	A unique name for the attestation process. The name must be unique across system administrator and deleted attestation processes.
Code	An identifying code (up to 32 characters) for the process. The code must be unique across system administrator and deleted attestation processes. **Note:** A code enhances the identification of the attestation process definition. However, if you do not specify a value in the Code field, then the attestation process is identified by the unique name.
Description	Detailed description of the attestation process.

3. On the Step 2: Define User Scope page:

   a. Select an attribute from the **Attribute** list. The Attribute list displays the user attributes given in the `FormMetaData.xml` file and the user-defined attributes from the user form. The attribute that you select is used to specify the criteria that must be met by users on whom the attestation process is applied.

b. From the **Condition** list, select a condition. The Condition list of values will change based on the type of attribute selected. For example, if you select User ID in the Attribute field, then the conditions displayed are Contains, Does Not Contain, Is Exactly, and Is Not Exactly. If you select the Start Date attribute, then the conditions displayed are Before, After, and Between.

c. In the **Value** field, enter a value for the user attribute.

d. Select the **Recursive** option. The Recursive check box is used for the entities for which you want to include the child entities while defining user scope. For example, if you select **Organization** in the user scope and then select **Recursive**, then the operation also includes all the suborganizations.

e. Click **Add** to add a new row to the user scope table, and click **Continue**.

4. On the Step 3: Define Resource Scope page, select a resource for the attestation process as follows:

a. From the **Attribute** list, select one of the resource attributes listed in the following table:

Attribute	Expression	Description
Name	Full text or wildcard	The name of the resource.
Type	Lookup values with the option to select all or a subset	The type of resource.
Resource Audit Objectives	Lookup values with the option to select all or a subset	The audit objectives assigned for a resource, which is provisioned. For example, whether or not the resource is financially significant. For more information about Resource Audit Objectives, see "Viewing Resource Details" on page 12-1.
Administrator User Groups	Lookup values with the option to select all or a subset	The user groups that have administrative permissions for a resource.
Authorized User Groups	Lookup values with the option to select all or a subset	The user groups that are authorizers or approvers for the resources.
Resource Status	Full text or wildcard	The status displayed when a resource is provisioned to a user, such as Certify, Reject, Open, or Closed.

b. From the **Condition** list, select a search condition.

c. In the **Value** field, enter a value for the resource attribute.

d. Click **Add** to add a new row to the resource scope table, and then click **Continue**.

5. On the Step 4: Define Administration Details page, define the reviewer to attest data, the attestation process schedule, and the process owner by performing the following steps:

a. From the **Reviewer** list, select the type of reviewer for the attestation process, such as a single specific user or resource administrator with highest priority. Then, select the reviewer from the adjoining lookup field.

b. Specify the attestation process schedule to run the attestation process once or repeatedly after a specific number of days, months, or years.

c. In the **Starting on** field, specify a start date for the attestation process.

d. In the **Process owner group lookup** field, specify a group that is the process owner for the attestation process.

e. If you want the process owner to be notified by e-mail if the reviewer refuses the attestation process, select **Email process owner if reviewer refuses attestation request**. Then, click **Continue**.

6. On the Step 5: Verify Info page, review the details of the attestation process, and then click **Create Process**.

   You are redirected to a page with a message that you have successfully created an attestation process definition. Clicking the process name takes you to the Attestation Process Detail page. To create another attestation process, click **Create Another Attestation Process Definition**.

   The Attestation Process Detail page is described in the "Managing Attestation Processes" section.

15.4 Managing Attestation Processes

To manage attestation processes:

1. In the left navigation pane, expand the **Attestation** menu, and then click **Manage.** The Manage Attestation Process page is displayed.

2. On the Manage Attestation Process page, enter the search criteria for the attestation process you want to manage. You can search by attestation process name, process code, reviewer type, or process owner. After you enter your search criteria, click **Search.** The Attestation Process Details page is displayed with the attestation processes that match your search criteria. The attestation processes displayed are the ones that the logged-in administrator is allowed to view based on permissions, or by virtue of being a member of the Process Owner group. This page does not show any deleted processes. The columns displayed on the page are listed in the following table:

Column	Description
Names	Specifies the name of the process.
Code	Specifies the attestation process code.
Description	Specifies a description for the process.
Status	Indicates whether the attestation process is active or system administrator.
Type	Specifies the type of resource.
User Scope	Specifies the scope of the user who will be a part of the attestation process.
Resource Scope	Specifies the resources that are within the scope of the attestation process.
Reviewer Type	Indicates the type of the reviewer.
Reviewer Name	Indicates the name of the reviewer.
Schedule	Indicates if the process is scheduled to run only once, or on a daily, monthly, or yearly basis.
Last Start	Specifies the last time an attestation process was run.

Column	Description
Next Start	Specifies when the process is scheduled to run next.
Process Owner Group	Indicates the process owner group. In addition, it specifies whether or not the process owner will be notified by e-mail if the reviewer refuses the attestation request.
Last Completion	Specifies the last time an instance of this process was completed.

The rest of this section discusses the following topics:

- Editing Attestation Processes
- Disabling Attestation Processes
- Enabling Attestation Processes
- Deleting Attestation Processes
- Running Attestation Processes
- Managing Attestation Process Administrators
- Viewing Attestation Process Execution History

15.4.1 Editing Attestation Processes

To edit an attestation process:

1. On the Attestation Process Detail page, click **Edit.**
2. On the Edit Attestation Process page, make the required changes to the attestation process, and then click **Save**.

   The fields on the Edit Attestation Process page are the same as those displayed in the "Creating Attestation Processes" section.

15.4.2 Disabling Attestation Processes

To disable an active attestation process:

1. On the Attestation Process Detail page, click **Disable.**

   Note that the Disable button is displayed only when a process is active.
2. On the Disable Attestation Confirmation page, click **Confirm Disable**.

15.4.3 Enabling Attestation Processes

An attestation process can be enabled only if its next start time is in the future and if the process is disabled.

To enable an attestation process:

1. On the Attestation Process Detail page, click **Enable.**

   Note that the Enable button is displayed only when the process is disabled.
2. On the Enable Attestation Confirmation page, click **Confirm Enable**.

15.4.4 Deleting Attestation Processes

You can edit, disable, or delete an attestation process only as a process administrator with the required permissions.

To delete an attestation process:

1. On the Attestation Process Detail page, click **Delete.**
2. On the page, click Confirm **Delete**.

15.4.5 Running Attestation Processes

This feature enables you to run unscheduled attestation processes. To run an attestation process, click **Run Now** on the Attestation Process Detail page. This starts the attestation process independent of the attestation schedule.

Only users in the process owner group can start unscheduled attestation processes.

15.4.6 Managing Attestation Process Administrators

The tasks of adding, deleting, and updating administrative groups for attestation processes are similar to the tasks of adding, deleting, and updating administrative groups for users and organizations.

To manage the administrators of an attestation process, select **Administrators** from the Additional Details list on the Attestation Process Detail page. The Administrative Groups page is displayed. You can use this page to add and remove administrators for an attestation process and update administrator permissions.

The permission model for an attestation process definition is as follows:

- To view the attestation process definition, the user must be either of the following:
  - A member of a group that has the appropriate read permissions in the administrators group
  - A member of the group that is the process owner
- To edit the attestation process definition, the user must be a member of a group that has the required write permissions in the administrators group.
- To delete the attestation process definition, the user must be a member of a group that has the required delete permissions in the administrators group.

15.4.7 Viewing Attestation Process Execution History

To view the execution history of an attestation process, select **Execution History** from the Additional Details list on the Attestation Process Detail page. The Attestation Process Execution History page is displayed.

The following are the columns in the Attestation Process Execution History table:

Column	Description
Request ID	ID for the attestation process instance that was run
Reviewer	Name of the reviewer for the attestation process
Initiated On	Date and time when the request was started
Completed On	Date and time when the request was completed If the request is still pending, then it shows Not Completed.

On the Attestation Process Execution History page, click the request ID link to open the Request Detail page. On this page, you can filter the requests according to the certified, rejected, open, and closed state.

15.5 Using the Attestation Dashboard

You use the Attestation Dashboard to view the state of attestation processes that are owned by any group of which you are a member. To use the Attestation Dashboard, expand the **Attestation** menu, and then click **Attestation Dashboard.** The Attestation Dashboard page displays a table listing the state of attestation processes that are owned by any group of which you are a member. The Attestation Dashboard table contains the columns listed in the following table:

Column	Description
Process Code	The attestation process code.
Process Names	The name of the process. The Attestation Process Detail page is displayed when the link for an attestation process name is clicked.
Last Completion	The date and time when the instance was run before the latest one was completed. If it does not exist, then the value must be None. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Request Date	The date and time when the last instance of this Process was run. If it has never been run, then the value is New. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Completion	The date and time when the last instance run was completed. If it has not been completed, then the value is Pending.
Total Records	The total number of entitlements identified for attestation and covered by an attestation task as part of the last process instance.
Certified	The number of entitlements certified in the last attestation process instance.
Rejected	The number of entitlements rejected in the last attestation process instance.
Open	All the open records for which no responses have been provided by the reviewers.

15.5.1 Viewing Attestation Request Details

You can access the drill-down page from the Attestation Dashboard page. The drill-down page displays the attestation details of all entitlements covered by a particular run of the Attestation Process.

To view attestation request details:

1. Click the link for the Last Completion or Current Request Page fields listed in the table on the Attestation Dashboard page.

   The Attestation Request Detail page displays the request details for the selected attestation process, along with a table that contains the following columns:

Column	Description
User	User whose entitlement is being attested. The data is displayed as a link. When you click the link, the user profile page is displayed with the user details for the attestation date.

Column	Description
Resource	Resource that is the basis for the entitlement being attested. The data is displayed as a link. When you click the link, a page is displayed with the process form data of the entitlement for the attestation date.
Descriptive Data	Description of the provisioned resource instance.
Comments	Comment or status of the request. The value can be one of the following: ■ Certify ■ Reject ■ Open ■ Closed
Attestation Result	Last response that was provided for the attestation.
Reviewer	User who provided the response. The data is displayed as a link. When you click the link, the user profile page is displayed with the current user details.
Delegation Path	If the attestation of an entitlement goes through any delegation, then you can use the View link in this column to see the Delegation Path Detail page. If no delegation has taken place, then `None` is displayed.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

2. Any attestation requests that require delegation include a link in the Delegation Path column.

   Clicking the link displays a Delegation Path page that provides information about the delegation path of the attestation request.

   The Data Attested field shows details about the entitlement being attested. It constructs the value by putting together user information, the resource name, and descriptive data in the following format:

   ```
   User_First_Name User_Last_Name [User_ID] - Resource_Name - Descriptive_Data
   ```

   The table on the Delegation Path page contains the following fields:

Column	Description
Reviewer	The reviewer to whom the entitlement for attestation is assigned. The data is displayed as a link. When you click the link, the current user profile data is displayed.
Attestation Result	Action supplied by the reviewer. Except for the first record, the value is always Delegated.
Attestation Date	The date and time of the attestation response of the reviewer.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

15.5.2 E-Mail Notification

As part of the attestation process, the attestation engine sends e-mail to concerned parties at various stages. You can configure e-mail content by using e-mail templates of the General type in the Oracle Identity Manager Email Definition store.

In the templates, the form user is defined as XELSYSADM. You can change it to a different user. You must ensure that the e-mail address is defined for the user selected

to use these templates. Otherwise, the system may not be able to send out notifications.

The following e-mail notification templates are available:

- **Notify Attestation Reviewer:** Used for sending e-mail when an attestation task is assigned to a reviewer.
- **Notify Delegated Reviewers:** Used for sending e-mail to reviewers when an attestation task is delegated to them.
- **Notify Declined Attestation Entitlements:** Used for sending e-mail to users in the Process Owner group if a reviewer declines any entitlements.
- **Attestation Reviewers With No E-Mail Defined:** Used for sending e-mail to users in the Process Owner group if an e-mail address is not defined for any of the reviewers.

15.5.3 Attestation Grace Period Expiry Checker Scheduled Task

A system scheduled task called `Attestation Grace Period Expiry Checker` is used to examine the attestation processes defined in Oracle Identity Manager and to create the required attestation tasks.

The features of the `Attestation Grace Period Expiry Checker` scheduled task are:

- The scheduled task is set to run every 30 minutes by default. You can change this according to your requirement.
- The scheduled task examines all active attestation processes.
- The scheduled task checks for attestation processes whose expiry date is within one, two, or three days and sends warning e-mail to the corresponding reviewers. If the attestation process has already expired, then it removes the actions provided by the reviewers and assigns it to the next priority member in the process owner group.

16

Working with the Diagnostic Dashboard

This chapter describes the Diagnostic Dashboard utility shipped with Oracle Identity Manager and includes the following topics:

16.1 Introduction to the Diagnostic Dashboard

You use the Diagnostic Dashboard to validate some of the Oracle Identity Manager prerequisites and to verify the installation.

You must have the appropriate system administrator permissions for your Application Server and Oracle Identity Manager environments to use this tool. Some database-related tests require DBA-level permissions.

The list of tests available and displayed depends on whether or not Oracle Identity Manager is installed and on what application server this tool and Oracle Identity Manager will be or are installed on.

The Diagnostic Dashboard utility and Oracle Identity Manager should be installed on the same application server.

16.1.1 Installation Tests

You use the Diagnostic Dashboard utility before installing Oracle Identity Manager, right after Oracle Identity Manager installation to verify that the installation is fine, and subsequently to check the status of the installation.

The following tests are performed before Oracle Identity Manager installation:

- Microsoft SQL Server JDBC Libraries Availability Check
- Microsoft SQL Server Prerequisites Check
- Oracle Prerequisites Check
- Embedded JMS Server Status

In addition, the following reports are available:

- Java VM System Properties Report
- WebSphere Version Report

The following tests are available only after the Oracle Identity Manager installation is available on the application server:

- Database Connectivity Check
- Account Lock Status
- Data Encryption Key Verification
- Scheduler Service Status
- Remote Manager Status
- JMS Messaging Verification
- Target System SSL Trust Verification
- SSL Diagnostic Information

The following reports are also available only after an Oracle Identity Manager installation is available:

- Oracle Identity Manager Libraries and Extensions Version Report
- Oracle Identity Manager Libraries and Extensions Manifest Report

You can run the following tests at any time to check the status of the Oracle Identity Manager installation:

- Display Version Number
- JVM Version Verification
- Fresh Oracle Identity Manager Installation Verification
- Database Verification
- WebSphere Embedded JMS Installation Verification
- Database Encryption Key Generation

16.1.2 Postinstallation Tests

The following are postinstallation tests:

- Database Encryption Key Verification
- Truststore verification
- SSO Diagnostics or Verification
- JMS Server availability on IBM WebSphere Application Server
- Messaging Verification
- Scheduler Verification
- Remote Manager Verification
- Reporting Version numbers
- Packaging

16.2 Installing the Diagnostic Dashboard

The Diagnostic Dashboard utility is distributed on the installation CD with the Oracle Identity Manager Installer. It is available as a WAR file in the `Diagnostic Dashboard` directory on the CD-ROM.

Oracle recommends that you deploy the Diagnostic Dashboard utility on the application server before installing Oracle Identity Manager.

This section discusses the following topics:

- Installing the Diagnostic Dashboard on Oracle Application Server
- Installing the Diagnostic Dashboard on JBoss Application Server
- Installing the Diagnostic Dashboard on IBM WebSphere Application Server
- Installing the Diagnostic Dashboard on Oracle WebLogic Server
- Launching the Diagnostic Dashboard

16.2.1 Installing the Diagnostic Dashboard on Oracle Application Server

This section describes how to install the Diagnostic Dashboard on Oracle Application Server.

> **Note:** For clustered installations, you must install Diagnostic Dashboard on each node in the cluster.

To install the Diagnostic Dashboard on Oracle Application Server:

1. Log in to the Administrative and User Console.
2. Click **Log on to Oracle Enterprise Manager 10g Application Server Control**.
3. Log in by using your Oracle Application Server administrator account.
4. For all nonclustered deployments, select the appropriate instance name from within the **All Application Servers**, **Application Server Name**.
5. Click **Application** on the Oracle Application Server home page.
6. Click **Deploy**.
7. Select the **Archive is present on local host. Upload the archive to the server where Application Server Control is running:** option.
8. Click **Browse** and select `XIMDD.war` from the following directory:

   PATCH`/Diagnostic Dashboard/`

   Click **Next**.
9. In Step 2 of the wizard, specify a name for the application (for example, `XIMDD`), and then click **Deploy** in Step 3 of the wizard.
10. Open the following file in a text editor:

    ORACLE_HOME`/j2ee/`*OAS_INSTANCE_NAME*`/application-deployments/XIMDD/orion-application.xml`

11. In this file, search for the following lines:

```
<imported-shared-libraries>
</imported-shared-libraries>
```

12. Replace these lines with the following lines:

```
<imported-shared-libraries>
<import-shared-library name="oim.xml.parser"/>
<remove-inherited name="apache.commons.logging"/>
```

```
</imported-shared-libraries>
```

13. Save and close the file.
14. Restart the server by using the opmnctl utility.

You can access the Diagnostic Dashboard at the following location:

`http://OIM_server_host_ip:port/XIMDD`

> **Note:** If you want the Scheduler test to run successfully, you must access `XIMDD` from each node of the cluster. However, if you try to access `XIMDD` from the Web server, it will fail.

16.2.2 Installing the Diagnostic Dashboard on JBoss Application Server

To deploy the Diagnostic Dashboard on JBoss Application Server, copy the *PATCH*`/Diagnostic Dashboard/jboss/XIMDD.war` file to the following location:

JBOSS_HOME`/server/default/deploy`

> **Note:** Here, *PATCH* is the name given to the root directory in the deployment package for Oracle Identity Manager release 9.1.0.2

16.2.3 Installing the Diagnostic Dashboard on IBM WebSphere Application Server

To deploy the Diagnostic Dashboard on IBM WebSphere Application Server:

1. Log in to the administrator console for the application server.
2. On the WebSphere main page, click **Applications** on the left menu pane, and then click **Install New Application**.

   The Preparing for the Application Installation page is displayed.
3. Specify the location of the XIMDD.war file as the value of the Path attribute and `XIMDD` as the Context root.
4. Click **Next** to proceed, and then click **Next** on the Generate Default Bindings page.

   The Install New Application page is displayed.
5. Change the application name to `XIMDD`. Click **Next** twice.
6. Select the cluster or server, select **XIMDD.war**, and then click **Apply.**
7. Confirm that the selected cluster or server is displayed under the Server column, and then click **Next**.
8. Click **Finish**.

   The Installing page is displayed. After the application installs successfully, the following message is displayed:

   ```
   Application XIMDD installed successfully
   ```
9. Click **Save to Master Configuration**, then click **Save**.
10. Click **Applications** > **Enterprise Applications** in the left menu pane.
11. Select **XIMDD**, and then click **Start**.

    A status is displayed, for example, whether or not the installed application has been started successfully.

In addition, perform the following steps:

1. Copy the XIMDD.war file from the *PATCH*/Diagnostic Dashboard directory to a temporary directory.
2. Extract the contents of the XIMDD.war file.
3. Extract the xlDataobjectBeans.jar file from the xellerate.ear file deployed on the application server host computer. To do so:
   a. Log in to the WebSphere Admin console.
   b. From the Application menu, select Enterprise Application.
   c. Select xellerate.ear, click Extract, and then provide a path for the directory into which you want to extract the file.
4. Copy the xlDataobjectBeans.jar file into the XIMDD/WEB-INF/lib directory.
5. Re-create the XIMDD.war file.
6. Deploy the XIMDD.war file by using the administrative console of the application server.

16.2.4 Installing the Diagnostic Dashboard on Oracle WebLogic Server

To deploy the Diagnostic Dashboard on Oracle WebLogic Server:

1. Log in to the administrative console of the application server.
2. In the Change Center region, click **Lock & Edit**.
3. In the Domain Structure region, click **Deployments**.
4. In the Deployments region on the right pane, click **Install**.
5. Click the **Upload your file(s)** link.
6. In the **Deployment Archive** field, enter the full path of the XIMDD.war file. This file is in the *PATCH*/DiagnosticDashboard directory.
7. Click **Next** and then click **Next** again.
8. Ensure that the **Install this deployment as an application** option is selected, and then click **Next**.
9. On the Optional Settings page, ensure that:
   - **XIMDD** is shown as the name of the application
   - The **DD Only: Use only roles and policies that are defined in the deployment descriptors** option is selected.
   - The **Use the defaults defined by the deployment's targets** option is selected.
10. Click **Finish**.
11. In the Change center region, click **Activate changes**.
12. In the Summary of Deployments region, select the check box for the XIMDD deployment.
13. From the **Start List** (after the table), select **Servicing all requests**.
14. Click **Yes** to confirm that you want the XIMDD deployment to be started.

    At this stage, the State column of the Deployments table shows `Active`.

You can now use a browser and connect to the Diagnostic Dashboard.

16.2.5 Launching the Diagnostic Dashboard

After the Diagnostic Dashboard is deployed, you can access it by using a URL of the following format:

`http://host:port/XIMDD`

In a clustered installation, you must connect to the individual cluster members directly with their corresponding host and port numbers. Click the **Diagnostic Dashboard** link on the left menu pane to display the main Diagnostic Dashboard main page.

The Diagnostic Dashboard utility indicates on which application server the tool is deployed. It also indicates whether or not Oracle Identity Manager is already installed on that application server. The tests displayed in the following table may vary, depending on whether or not Oracle Identity Manager is installed and which application server is used. Table 16–1 also shows the availability of these tests.

Table 16–1 Diagnostic Dashboard Tests

Test	Availability When Oracle Identity Manager Is Not Installed	Application Servers
Microsoft SQL Server JDBC Libraries Availability Check	Yes	JBoss Application Server
Microsoft SQL Server Prerequisites Check	Yes	JBoss Application Server
Oracle Prerequisites Check	Yes	All
WebSphere Embedded JMS Server Status	Yes	IBM WebSphere Application Server
Database Connectivity Check	No	All
Account Lock Status	No	All
Data Encryption Key Verification	No	All
Scheduler Service Status	No	All
Remote Manager Status	No	All
JMS Messaging Verification	No	All
Target System SSL Trust Verification	No	All
Java VM System Properties Report	Yes	All
WebSphere Version Report	Yes	IBM WebSphere Application Server
Oracle Identity Manager Libraries and Extensions Version Report	No	All
Oracle Identity Manager Libraries and Extensions Manifest Report	No	All
SSO Diagnostic Information	No	All
Test Basic Connectivity	No	All
Test Provisioning	No	All

Table 16–1 (Cont.) Diagnostic Dashboard Tests

Test	Availability When Oracle Identity Manager Is Not Installed	Application Servers
Test Reconciliation	No	All

16.3 Using the Diagnostic Dashboard

The Diagnostic Dashboard main page includes the sections listed in the following table:

Section	Description
System Information Application Server	Displays the name of the application server
Oracle Identity Manager Installation	Displays installation details such as product version, build number, host, and location of the product
Test Details Test Name	Displays the test name
Description	Displays the description of the test
Test Parameters	Displays testing parameters if required for verifying the test

To run a test:

1. Select the test by selecting the option on the Diagnostic Dashboard main page.
2. Enter the required parameters.
3. Click **Verify** to see the result.

   The Diagnostic Dashboard Test Result page is displayed with the status information listed in the following table.

Test Result	Description
Result Summary	Shows all the selected tests with icons (pass or fail) indicating the result. The test name is a Web link that allows the user to jump to the result details directly.
Test Name	Displays the name of the test
Description	Displays the description of the test
Input Parameters	Displays the parameters of the test
Result	Displays the outcome of the test
Details	Displays details about the outcome of the test

4. Click **Diagnostic Dashboard** on the left menu pane to return to the previous test page.

16.4 Test Details and Parameters

The following tests are available for different application servers:

- Microsoft SQL Server JDBC Libraries Availability Check

- Microsoft SQL Server Prerequisites Check
- Oracle Database Prerequisites Check
- WebSphere Embedded JMS Server Status
- Database Connectivity Check
- Account Lock Status
- Data Encryption Key Verification
- Scheduler Service Status
- Remote Manager Status
- JMS Messaging Verification
- Target System SSL Trust Verification
- Java VM System Properties Report
- WebSphere Version Report
- Oracle Identity Manager Libraries and Extensions Version Report
- Oracle Identity Manager Libraries and Extensions Manifest Report
- SSO Diagnostic Information
- Test Basic Connectivity
- Test Provisioning
- Test Reconciliation

16.4.1 Microsoft SQL Server JDBC Libraries Availability Check

Prerequisite: None

Description: Oracle Identity Manager needs JDBC drivers in the CLASSPATH to work with Microsoft SQL Server. This test verifies if the drivers are available in the CLASSPATH.

Result: Microsoft SQL Server Driver should be found.

16.4.2 Microsoft SQL Server Prerequisites Check

Application Server: JBoss Application Server

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Database Server	Enter the location for the database server.
Port	Enter the port number.
Database Name	Enter the database name.
Oracle Identity Manager Database User Name	Enter the Oracle Identity Manager database user name.
Oracle Identity Manager Database User Password	Enter the Oracle Identity Manager database user password.

Description: Checks if the specified Microsoft SQL server instance meets the prerequisites for Oracle Identity Manager installation

Result: It will display the following information:

- Necessary permissions for user
- XA support should be enabled
- Microsoft SQL Server Version

16.4.3 Oracle Database Prerequisites Check

Application Server: JBoss Application Server or IBM WebSphere Application Server / Oracle WebLogic Server / Oracle Application Server

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Database Server	Enter the location of the database server.
Port	Enter the port number.
Database Name (SID)	Enter the database name (SID).
Oracle Identity Manager Database User Name	Enter the Oracle Identity Manager database user name.
System User Name	Enter the system user name.
System User Password	Enter system user password.

Description: Checks if the specified Oracle instance meets the prerequisites for Oracle Identity Manager installation. This test requires SYSTEM permissions.

Result: It will display the following information:

- Necessary permissions for user
- XA support enabled
- JVM enabled
- Oracle version Information

16.4.4 WebSphere Embedded JMS Server Status

Application Server: IBM WebSphere Application Server

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Host	Enter the host name.
Port	Enter the port number.
User Name	Enter the user name.
Password	Enter the password.

Description: Checks the status of JMS Server. This test is valid for IBM WebSphere Application Server only and requires Oracle Identity Manager to be installed.

Result: Displays the status of JSM Server.

16.4.5 Database Connectivity Check

Application Server: All

Prerequisite: None

Description: Run this test to verify whether or not Oracle Identity Manager is able to connect to the database. This test verifies the direct database connection as well as the J2EE data sources (XA and non-XA).

Result: It will display the following information:

- Direct database connectivity
- XA and non-XA execution

16.4.6 Account Lock Status

Application Server: All

Prerequisite: The following is the prerequisite for verifying this test:

Prerequisite	Description
User Name	Enter the user name.

Description: Oracle Identity Manager locks an account when there are successive multiple invalid login attempts. This test checks whether or not a specified account is locked.

Result: Checks for locked or unlocked accounts in the database.

16.4.7 Data Encryption Key Verification

Application Server: All

Prerequisite: None

Description: The data encryption key in an Oracle Identity Manager installation should be the same as the one used to encrypt the data in the Oracle Identity Manager database. This may not be the case when an Oracle Identity Manager installation is pointed to a database schema created for a different Oracle Identity Manager installation. This can also happen when a database dump from one Oracle Identity Manager installation is imported for a different Oracle Identity Manager installation without copying the corresponding key.

Result: Checks if the database key is present in the Oracle Identity Manager configuration directory.

16.4.8 Scheduler Service Status

Application Server: All

Prerequisite: None

Description: Checks the status of the Oracle Identity Manager Scheduler Service running on the server.

Result: Displays the status of the scheduler service.

16.4.9 Remote Manager Status

Application Server: All

Prerequisite: None

Description: Reports the status of the Remote Managers that this Oracle Identity Manager installation is set to work with.

Result: Displays the status of the Remote Manager.

16.4.10 JMS Messaging Verification

Application Server: All

Prerequisite: None

Description: The purpose of this test is to verify that Oracle Identity Manager will be able to submit a JMS message and process it.

Result: Displays if Oracle Identity Manager is able to submit and process a JMS message.

16.4.11 Target System SSL Trust Verification

Application Server: All

Prerequisite: The following are the prerequisites for running this test:

Prerequisite	Description
Host	Enter the host name.
Port	Enter the port number.
Truststore Location	Enter the location for storage.
Truststore Password	Enter the password for storage.

Description: Oracle Identity Manager must be set up to trust the target system certificates if the connectivity is over Secure Sockets Layer (SSL). Enter the host name and the port where a target system is listening for SSL connections.

Result: It displays the following information:

- Valid and invalid host and port address
- Trusted certificates

16.4.12 Java VM System Properties Report

Application Server: All

Prerequisite: None

Description: Displays all the Java VM system properties.

Result: Displays all the Java VM system properties.

16.4.13 WebSphere Version Report

Application Server: IBM WebSphere Application Server

Prerequisite: None

Description: Obtains the IBM WebSphere Application Server version information along with a list of all the installed fix packs and components of the application server.

Result: Displays WebSphere version information

16.4.14 Oracle Identity Manager Libraries and Extensions Version Report

Application Server: All

Prerequisite: None

Description: Reports all the versions of the Oracle Identity Manager libraries and extensions.

Result: Displays the versions of the Oracle Identity Manager libraries and extensions.

16.4.15 Oracle Identity Manager Libraries and Extensions Manifest Report

Application Server: All

Prerequisite: None

Description: Reports the manifest information of the Oracle Identity Manager libraries and extensions.

Result: Displays the manifest information of the Oracle Identity Manager libraries and extensions.

16.4.16 SSO Diagnostic Information

Application Server: All

Prerequisite: None

Description: Provides information pertaining to SSO setup. In addition, provides instructions needed for setting up Oracle Identity Manager to enable retrieving run-time diagnostic information related to SSO logins.

Result: Displays whether or not the SSO setup is enabled for the Oracle Identity Manager installation.

16.4.17 Test Basic Connectivity

Application Server: All

Prerequisite: IT resource type and IT resource name

Description: Tests the connection to the target system by using the IT resource for the target system.

> **Note:** If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the connectivity test. If the test fails, then the cause of the error is also displayed.

16.4.18 Test Provisioning

Application Server: All

Prerequisite: IT resource type and IT resource name

Description: Performs a basic Create User operation on the target system.

> **Note:** If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the provisioning test. Test data created on the target system during the test is deleted at the end of the test.

16.4.19 Test Reconciliation

Application Server: All

Prerequisite: IT resource type and IT resource name

Description: Performs a basic reconciliation operation on the target system.

> **Note:** If the specified IT resource type was created when you deployed a predefined connector, then see the Oracle Identity Manager Connector Pack release notes and documentation to determine whether or not this test can be applied for the release of the connector that you deployed.

Result: Displays the results of the reconciliation test. Test data reconciled into Oracle Identity Manager during the test is deleted at the end of the test.

Part II

Integration Solutions Features

Part II is divided into the following chapters:

17

Installing Predefined Connectors

You use a predefined connector to integrate Oracle Identity Manager with a specific third-party application. This chapter discusses the procedure to install predefined connectors.

> **Note:** The predefined connectors are distributed in the Oracle Identity Manager Connector Pack, independent from the Oracle Identity Manager core server release.
>
> See the Oracle Identity Manager Connector Pack documentation to determine whether or not you can install the required release of the connector by using the Connector Installer feature of the Administrative and User Console.

This chapter is divided into the following sections:

17.1 Overview of the Connector Installation Process

The installation of most predefined connectors requires you to perform some or all of the following tasks:

1. Verify the installation requirements.
2. Configure the target system.
3. Copy the connector files and external code files to directories on the Oracle Identity Manager server.
4. Configure the Oracle Identity Manager server.
5. Import the connector XML files.
6. Configure reconciliation.
7. Configure provisioning.
8. Configure Secure Sockets Layer (SSL).

Of these tasks, the Administrative and User Console can be used to perform the following:

- Copying the connector files and external code files to directories on the Oracle Identity Manager server
- Importing the connector XML files
- Compiling adapters (which is part of the procedure to configure provisioning)

Note: You must manually perform the remaining tasks. For instructions on performing these tasks, see the connector-specific documentation in the Oracle Identity Manager Connector Pack documentation library.

17.2 Creating the User Account for Installing Connectors

All users belonging to the `SYSTEM ADMINISTRATORS` group of Oracle Identity Manager can install connectors. Alternatively, members of a group to which you assign the required menu items and permissions can install connectors.

See Also: Chapter 10, "Creating and Managing User Groups" for information about creating groups and assigning menu items and permissions to them

The required permissions are the following:

- Form Designer (Allow Insert, Write Access, Delete Access)
- Structure Utility.Additional Column (Allow Insert, Write Access, Delete Access)
- Meta-Table Hierarchy (Allow Insert, Write Access, Delete Access)

The required menu item is Deployment Management Install Connector.

To install a connector, if you want to use a user account that does not belong to the `SYSTEM ADMINISTRATORS` group, then you must apply these permissions and menu item to one of the groups to which the user account belongs.

17.3 Installing a Predefined Connector

To install a predefined connector:

1. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section on page 17-2.
2. Click **Deployment Management**, and then click **Install Connector**.
3. From the Connector List list, select the connector that you want to install. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

   OIM_HOME`/xellerate/ConnectorDefaultDirectory`

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

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select the connector that you want to install.

4. Click **Load**.

   Information about the following is displayed:

   - Connector installation history

     The connector installation history is information about previously installed releases of the same connector.

   - Connector dependency details

     There are some connectors that require the installation of some other connectors before you can start using them. For example, before you use the Novell GroupWise connector, you must install the Novell eDirectory connector. Novell eDirectory is called the **dependency connector** for Novell GroupWise.

     The connector dependency details include the list of connectors that must be installed before you install the selected connector. These details also include information about any dependency connectors that are already installed, and whether or not any of the installed dependency connectors must be upgraded.

     You must ensure that the correct versions of dependency connectors are installed before you proceed with the connector installation.

5. 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)

   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.

   One of the reasons for installation failure could be a mismatch between information about files and directory paths in the configuration XML file and the actual files and directory paths. If this happens, then an error message is displayed.

   For example, suppose the actual name of the JAR file for reconciliation is `recon.jar`. If the name is provided as `recon1.jar` in the configuration XML file, then an error message is displayed.

   If such an error message is displayed, then perform *any one* of the following steps:

   - Make the change in the configuration XML file, and then retry installation from the Step 1: Select Connector to Install page onward.

     In the example described earlier, change the name of the JAR file to `recon.jar` in the configuration XML file, and then retry installation from the Step 1: Select Connector to Install page onward.

   - Make the change in the actual name or path of the file or directory, and then use the Retry option.

In the example described earlier, change the name of the JAR file to `recon1.jar` and then click the **Retry** button.

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

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

   Note: At this stage, run the PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See *Oracle Identity Manager Best Practices Guide* for information about running the `PurgeCache` utility.

   There are no prerequisites for some predefined connectors.

   b. Creating an IT resource for the connector

   The IT resource type is displayed. You must create an IT resource of the specified type.

   See Also: The "Creating IT Resources" section on page 12-46

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

   The names of the scheduled tasks that are created during the XML file import process are displayed. You must configure these scheduled tasks.

   See Also: The "Managing Scheduled Tasks" section on page 12-52

   Note: You can also access links to the Administrative and User Console pages for creating the IT resource and configuring the scheduled tasks by expanding the **Resource Management** menu on the left navigation pane of the console.

18

Configuring Connectors for Installation and Testing

The guidelines explained in this chapter are aimed at ensuring that your custom connectors meet the compatibility requirements for using the connector installer and the Diagnostic Dashboard. These guidelines apply only to specific areas of custom connector development.

This chapter contains the following sections:

18.1 Structure of the Configuration XML File

This section discusses the structure of the configuration XML file that is used during the connector installation process. Use the information in this section to create configuration XML files for your custom connectors.

The following is the recommended path for copying the installation files for the predefined connectors:

OIM_HOME/xellerate/ConnectorDefaultDirectory

When you install Oracle Identity Manager, the following files are copied into the ConnectorDefaultDirectory directory:

- ConnectorConfigTemplate.xml

  This is a template of the configuration XML file. Use a copy of this file to create the configuration XML file.

- ConnectorSchema.xsd

  This is the XML schema document (XSD) against which you must validate the configuration XML file that you create.

Table 18–1 lists the elements in the configuration XML file. Use the links in this table to access sections on each element.

Table 18–1 Elements in the Configuration XML File

Root Element	Level 1 Element	Level 2 Element	Level 3 Element
connector Element			
	connector-name Element		

Table 18–1 (Cont.) Elements in the Configuration XML File

Root Element	Level 1 Element	Level 2 Element	Level 3 Element
	connector-version Element		
	filecopy Element	destination Element	file Element
	configuration Element	source Element	file Element
	pre-Install Element	title Element	step Element
	dependency-connector Element	dependency-connector-name Element	
		dependency-connector-version Element	

See "Sample Configuration XML File" for the contents of a sample configuration XML file.

18.1.1 connector Element

The following table summarizes the properties of the `connector` element:

Property	Value
Parent Element	NA
Attributes	NA In the template XML file, do not change the values of attributes of this element.
Child Elements	`connector-name`, `connector-version`, `filecopy`, `configuration`, `pre-Install`, and `dependency-connector`
Number of Occurrences	One
Element Value	NA

The `connector` element is the root element in the configuration XML file. See the following sections for information about the child elements of the `connector` element:

- connector-name Element
- connector-version Element
- filecopy Element
- configuration Element
- pre-Install Element
- dependency-connector Element

18.1.2 connector-name Element

The following table summarizes the properties of the `connector-name` element:

Property	Value
Parent Element	`connector`

Property	Value
Attributes	None
Child Elements	None
Number of Occurrences	One
Element Value	Name of the connector

Use the `connector-name` element to specify the name of the target system of the connector. The connector name value is displayed on most of the connector installation pages.

Sample usage:

```
<connector-name>Active Directory</connector-name>
```

18.1.3 connector-version Element

The following table summarizes the properties of the `connector-version` element:

Property	Value
Parent Element	`connector`
Attributes	None
Child Elements	None
Number of Occurrences	One
Element Value	Release number of the connector

Use the `connector-version` element to specify the connector release number. The release number is displayed along with the name of the connector. It is also used to compare releases and provide upgrade guidelines to users.

Sample usage:

```
<connector-version>9.1.0</connector-version>
```

Apply the following guidelines whenever you specify a value for the `connector-version` element:

- Use only numerals and periods (.) to specify the connector release number.
- Ensure that there are no spaces in the connector release number.
- Trailing zeros in the connector release number are discarded when the release number of a connector is compared with the release number of another connector. For example, the values `9.1.0` and `9.1.0.0` are considered the same by the code that compares release numbers.

18.1.4 filecopy Element

The following table summarizes the properties of the `filecopy` element:

Property	Value
Parent Element	`connector`
Attributes	None

Property	Value
Child Elements	`destination`
Number of Occurrences	One
Element Value	NA

The `filecopy` element serves as the container for `destination` elements, which hold details of the files to be copied from specific directories in the connector installation media directory.

The "destination Element" section discusses the child element of the `filecopy` element.

18.1.5 destination Element

The following table summarizes the properties of the `destination` element:

Property	Value
Parent Element	`filecopy`
Attributes	`folder`
Child Elements	`file`
Number of Occurrences	One for each type of file to be copied
Element Value	The value can be `JavaTasks`, `ScheduleTask`, `connectorResources`, or `ThirdParty`.

Use the `folder` attribute of the `destination` element to specify the name of the folder on the Oracle Identity Manager server into which a certain type of connector files must be copied. As mentioned in the table, you can specify any one of the following folders:

- `connectorResources`: Specify this folder if the connector installation media contains resource bundles.
- `JavaTasks`: Specify this folder if the connector installation media contains JAR files for provisioning.
- `ScheduleTask`: Specify this folder if the connector installation media contains JAR files for reconciliation.
- `ThirdParty`: Specify this folder if the connector installation media contains external code files that the connector requires for provisioning or reconciliation.

The "file Element" section discusses the child elements of the `filecopy` element.

18.1.6 file Element

The following table summarizes the properties of the `file` element:

Property	Value
Parent Element	`destination` or `source` **Note:** The `source` element is described later in this chapter.
Attributes	None

Property	Value
Child Elements	None
Number of Occurrences	At least one
Element Value	Name of file to be copied

Use the `file` element to specify the name of the file that must be copied into the folder specified by the parent `destination` element. The case of the file name (uppercase and lowercase) that you specify must be the same as that of the actual name. For a given file name, the installation program searches the entire connector installation media directory to locate the file and then copies the file into the folder specified by the parent `destination` element.

Sample usage:

```
<file>ActiveDirectory.properties</file>
```

If you want the same file to be copied into multiple directories, then you must specify the file name in `file` elements under the required `destination` elements. For example, suppose you want the `connector.jar` file to be copied into both the `JavaTasks` and `ScheduleTask` directories, then add the following lines in the XML file:

```
<destination folder="JavaTasks">
  <file>connector.jar</file>
</destination>
<destination folder="ScheduleTask">
  <file>connector.jar</file>
</destination>
```

18.1.7 configuration Element

The following table summarizes the properties of the `configuration` element:

Property	Value
Parent Element	`connector`
Attributes	None
Child Elements	`destination`
Number of Occurrences	One
Element Value	NA

The `configuration` element is used to hold information about the XML files that are to be imported during the installation process.

The "source Element" section discusses the child element of the `configuration` element.

18.1.8 source Element

The following table summarizes the properties of the `source` element:

Property	Value
Parent Element	`configuration`

Property	Value
Attributes	`folder`
Child Elements	`file` **Note:** The `file` element is described earlier in this chapter.
Number of Occurrences	One
Element Value	`xml`

The `source` element is used to specify the `xml` folder in the connector installation media directory in which the connector XML files are stored. During the installation process, the Deployment Manager is called to import these XML files.

The following sample code lines show how the `configuration`, `source`, and `file` elements must be used:

```
<configuration>
  <source folder="xml">
    <file>xliADResourceObject.xml</file>
    <file>xliADXLResourceObject.xml</file>
  </source>
</configuration>
```

18.1.9 pre-Install Element

The following table summarizes the properties of the `pre-Install` element:

Property	Value
Parent Element	`connector`
Attributes	None
Child Elements	`title`
Number of Occurrences	One
Element Value	NA

You might need to perform certain tasks before you can start using some connectors. For example, the Microsoft Active Directory connector requires you to configure Secure Sockets Layer (SSL) to secure communication between Oracle Identity Manager and the target system. These prerequisite tasks can be displayed at the end of the connector installation process by using the child elements of the `pre-Install` element.

If you do not want to display prerequisite tasks at the end of the connector installation process, then do not include the `pre-Install` element in the XML file.

The "title Element" section discusses the child element of the `pre-Install` element.

18.1.10 title Element

The following table summarizes the properties of the `title` element:

Property	Value
Parent Element	`pre-Install`

Property	Value
Attributes	`description`
Child Elements	`step`
Number of Occurrences	At least one
Element Value	Key value of the resource bundle line that contains the text to be displayed

In the resource bundle, there is a line that specifies the title of the section containing prerequisite tasks for the connector. Use the `description` attribute of the `title` element to specify the key value of this resource bundle line.

> **Note:** The key value of a resource bundle line is the text to the left of the equal sign (=) in the resource bundle. See *Oracle Identity Manager Globalization Guide* for more information about resource bundles.

The "step Element" section discusses the child element of the `title` element. The example in that section illustrates how you must use this element.

18.1.11 step Element

The following table summarizes the properties of the `step` element:

Property	Value
Parent Element	`title`
Attributes	None
Child Elements	None
Number of Occurrences	One
Element Value	Key value of the resource bundle line that contains the text to be displayed

Use the `step` element to specify the key value of the resource bundle line that describes a single prerequisite task for the connector.

The following example uses the Microsoft Active Directory connector to illustrate how you must use the `pre-Install`, `title`, and `step` elements:

The following is a partial listing of the prerequisite tasks that are displayed after the installation of the Microsoft Active Directory connector:

```
Enabling LDAPS
- Ensure that Certificate Services are installed on the server.
- Open the default group policy for the Domain Controller on the server (in Active
Directory Users and Computers).
- Right-click the domain node, and select Properties.Click the Group Policy tab.
- Select Default Domain Policy.
 . . .

Setting Up the Microsoft Active Directory Certificate as a Trusted Certificate
- To make the Microsoft Active Directory certificate a trusted certificate, export
the certificate and import it into the keystore of the Oracle Xellerate Identity
Provisioning server as a trusted CA certificate.
```

. . .

The following is a partial listing of the resource bundle lines that contain the prerequisite tasks that appear after the installation of the Microsoft Active Directory connector:

```
AD-connector.prerequisite.enablingldaps=Enabling LDAPS

AD-connector.prerequisite.enablingldapsteps=<ul><li>Ensure that Certificate
Services are installed on the server</li><li>Open the default group policy for the
Domain Controller on the server (in Active Directory Users and
Computers).</li><li>Right-click the domain node, and select
Properties.</li><li>Click the Group Policy tab.</li><li>Select Default Domain
Policy.</li>. . . </ul>

AD-connector.prerequisite.setupad=Setting Up the Microsoft Active Directory
Certificate as a Trusted Certificate

AD-connector.prerequisite.setupadsteps=<ul><li>To make the Microsoft Active
Directory certificate a trusted certificate, export the certificate and import it
into the keystore of the Oracle Xellerate Identity Provisioning server as a
trusted CA certificate.</li> . . .</ul>
```

To enable the display of these resource bundle lines at the end of the installation process, you must add the following lines in the configuration XML file:

```
<pre-Install>
  <title description="AD-connector.prerequisite.enablingldaps">
    <step>AD-connector.prerequisite.enablingldapsteps</step>
  </title>
  <title description="AD-connector.prerequisite.setupad">
    <step>AD-connector.prerequisite.setupadsteps</step>
  </title>
</pre-Install>
```

18.1.12 dependency-connector Element

The following table summarizes the properties of the `dependency-connector` element:

Property	Value
Parent Element	`connector`
Attributes	None
Child Elements	`dependency-connector-name`, `dependency-connector-version`
Number of Occurrences	At least one
Element Value	NA

You can start using certain connectors only after the installation of certain other connectors. For example, you can start using the Novell GroupWise connector only after you install the Novell eDirectory connector. In the Oracle Identity Manager context, the connector whose installation is a prerequisite is called the **dependent connector.** For example, the Novell eDirectory connector is the dependent (required) connector for the Novell GroupWise connector.

The dependency-connector element is used to hold information about dependent connectors for your connector. If your connector has multiple dependent connectors, then add one dependency-connector element in the XML file for each dependent connector.

The following sections discuss the child elements of the dependency-connector element:

- dependency-connector-name Element
- dependency-connector-version Element

18.1.13 dependency-connector-name Element

The following table summarizes the properties of the dependency-connector-name element:

Property	Value
Parent Element	dependency-connector
Attributes	None
Child Elements	None
Number of Occurrences	At least one
Element Value	Name of the dependent connector

Use the dependency-connector-name element to specify the name of the dependent connector for your connector. The name that you specify must be the same as the name that is specified in the connector-name element of the XML file for the dependent connector.

The "dependency-connector-version Element" section contains an example that illustrates how you must use the dependency-connector-name element.

18.1.14 dependency-connector-version Element

The following table summarizes the properties of the dependency-connector-version element.

Property	Value
Parent Element	dependency-connector
Attributes	None
Child Elements	None
Number of Occurrences	One for each occurrence of the dependency-connector-name element
Element Value	Release number of the dependent connector

Use the dependency-connector-version element to specify the release number of the dependent connector for your connector. The release number that you specify must be the same as the release number that is specified in the connector-version element of the configuration XML file for the dependent connector. Ensure that there are no spaces in the connector version value that you specify.

The following example illustrates how to use the `dependency-connector`, `dependency-connector-name`, and `dependency-connector-version` elements.

`DepConn1` and `DepConn2` are dependent connectors for your connector. Their release numbers are 9.0.3 and 9.0.4.1, respectively. For these dependent connectors, you must add the following lines in the configuration XML file of your connector:

```
<dependency-connector>
  <dependency-connector-name>DepConn1<dependency-connector-name>
  <dependency-connector-version>9.0.3<dependency-connector-version>
</dependency-connector>
<dependency-connector>
  <dependency-connector-name>DepConn2</dependency-connector-name>
  <dependency-connector-version>9.0.4.1<dependency-connector-version>
</dependency-connector>
```

If your connector has no dependent connectors, then you need not add the `dependency-connector` element.

18.1.15 Sample Configuration XML File

The following are the contents of a sample configuration XML file:

```
<?xml version="1.0" encoding="UTF-8" ?>
<connector orderid="1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation=".\ConnectorSchema.xsd">
<connector-name>Active Directory</connector-name>
<connector-version>9.1.0</connector-version>
<filecopy>
<destination folder="ConnectorResources">
  <file>ActiveDirectory.properties</file>
<destination folder="JavaTasks">
  <file>connector.jar</file>
</destination>
<destination folder="ScheduleTask">
  <file>connector.jar</file>
</destination>
</filecopy>
<configuration>
  <source folder="xml">
    <file>ActiveDirectory.xml</file>
  </source>
</configuration>
<pre-Install>
  <title description="AD-connector.prerequisite.enablingldaps">
    <step>AD-connector.prerequisite.enablingldapsteps</step>
  </title>
  <title description="AD-connector.prerequisite.setupad">
    <step>AD-connector.prerequisite.setupadsteps</step>
  </title>
</pre-Install>
<dependency-connector>
  <dependency-connector-name>DepConn1<dependency-connector-name>
  <dependency-connector-version>9.0.3<dependency-connector-version>
</dependency-connector>
<dependency-connector>
  <dependency-connector-name>DepConn2</dependency-connector-name>
  <dependency-connector-version>9.0.4.1<dependency-connector-version>
</dependency-connector>
```

18.2 Developing the Test Class for the Connector

You must develop a test class for the connector. When you use the Diagnostic Dashboard to test connectivity, reconciliation, or provisioning, this class is used to run the test.

The following are guidelines on creating the test class:

- The test class must implement the `testBasicConnectivity`, `testProvisioning`, and `testReconciliation` methods. These methods must accept a hashmap parameter.
- The name of the test class must be in the following format:

  connector_name`ConnectorTest.java`

  To apply this format, replace *connector_name* with the value of the `ITResourceDef` attribute of the `SPD_KEY` element in the following file:

  Connector_Pack_Directory`/xml/xli`*connector_name*`ResourceObject.xml`

  Remove spaces, if there are any, from the value of the `ITResourceDef` attribute. For example, suppose the `SPD_KEY` element in the XML file is as follows:

  ```
  <SPD_KEY ITResourceDef="AD Server"/>
  ```

  In this case, set the name of the test class to `ADServerConnectorTest.java`.
- Include the test class file in the connector JAR file, and then copy the JAR file into the `lib` directory inside the connector pack directory.

18.3 Structure of the Connector Pack Directory

After you create the connector files, you must place them in the directories described in Table 18–2. These directories are placed in the connector pack directory for your connector. For example, the connector pack directory for the Microsoft Active Directory connector is `ActiveDirectory`.

Table 18–2 Structure of the Connector Pack Directory

Directory	Description
`configuration`	In this directory, place the configuration XML file to be used during the installation process. For example: `ActiveDirectorConnectorConfig.xml`
`ext`	In this directory, place all third-party JAR files. During the installation process, files in this directory are copied into the `ThirdParty` directory. For example, the `ldap.jar` file is required for using the Sun Java System Directory connector.
`lib`	In this directory, place the JAR files required for reconciliation and provisioning operations. During the installation process, JAR files for reconciliation are copied into the `ScheduleTask` directory and JAR files for provisioning are copied into the `JavaTasks` directory. For example: `xliActiveDirectory.jar`
`resources`	In this directory, place the resource bundles. During the installation process, these resource bundles are copied into the `connectorResources` directory. For example: `ActiveDirectory_en.properties`

Table 18–2 (Cont.) Structure of the Connector Pack Directory

Directory	Description
`scripts`	In this directory, place the scripts that must be run as part of the manual connector configuration process. These scripts are not used during the installation process performed by using the Administrative and User Console.
`xml`	In this directory, place the connector XML files for trusted source and target resource reconciliation. During the installation process, the connector XML files mentioned in the configuration XML file are imported by the Deployment Manager. For example: `ActiveDirectorConnectorConfig.xml`

19

Introduction to Generic Technology Connectors

This chapter introduces the generic technology connector concept and the features that Oracle Identity Manager provides for working with generic technology connectors.

This chapter is divided into the following sections:

19.1 Requirement for Generic Technology Connectors

Predefined Oracle Identity Manager connectors are designed for commonly used target systems such as Microsoft Active Directory and PeopleSoft Enterprise Applications. A predefined connector is developed using the Adapter Factory approach, and its architecture is based on either the APIs that the target system supports or the data repository type and schema in which the target system stores user data. Because they are developed using the Adapter Factory, predefined connectors offer extensive workflow and adapter customization capabilities. The use of a predefined connector is the recommended integration method if such a connector is available for the target system.

There may be scenarios in which you want to integrate Oracle Identity Manager with a target system that has no corresponding predefined connector. The following are examples of such scenarios:

Scenario 1: All employees of Acme Inc. are allotted disk space on a backup server. Employees send requests to the system administrator for managing their accounts on the backup server. The system administrator has developed a Web-based application to capture, review, and act on requests from employees. The front end of this application is a Web service that accepts and stores data in CSV format. Employee account data stored in the back end can be exported as XML files to a specified location.

Scenario 2: Ceeam Travels Inc. owns a custom Web-based application that its customers use to request airline fare quotes. Agents, who are also employees of Ceeam Travels, respond to these requests by using the same application. Customers self-register themselves to create accounts in this application. However, Ceeam Travels employees need to have accounts auto-provisioned based on their HR job title.

Account management functions (such as create, update, and delete) of the application are available through Java APIs.

In both Scenario 1 and 2, you would need to create a custom connector to link the target system and Oracle Identity Manager. If you are looking for a simple and easy way to create your custom connector and you do not need the customization features of the Adapter Factory, then you can create the connector by using the Generic Technology Connector feature of Oracle Identity Manager. As described in the "Functional Architecture of Generic Technology Connectors" section on page 19-2, providers are the building blocks of generic technology connectors. In Scenario 1, you can use the predefined Shared Drive Reconciliation Transport Provider and CSV Reconciliation Format Provider to create a generic technology connector that reconciles data stored in a flat file into Oracle Identity Manager. For Scenario 2, there is no predefined provider available to integrate the custom application with Oracle Identity Manager. In this case, you can use the instructions provided in Chapter 21 to create the custom providers that call the Java APIs exposed by the target application.

19.2 Functional Architecture of Generic Technology Connectors

Like a predefined connector, a generic technology connector acts as the bridge for reconciliation and provisioning operations between Oracle Identity Manager and a target system. In terms of functionality, a generic technology connector can be divided into a reconciliation module and provisioning module. When you create a generic technology connector, you can specify whether you want to include both modules or only the reconciliation or provisioning module.

A predefined connector provides reconciliation and provisioning functionality in the context of the same target. In contrast, the reconciliation and provisioning modules of a generic technology connector are composed of reusable components that you select. Each component performs a specific function during provisioning or reconciliation. For example, you can create a connector that performs trusted source reconciliation from flat files and provides target resource provisioning using the SPML protocol to an SPML-enabled target.

In this guide, the components that constitute a generic technology connector are called **providers.**

Each provider performs a transport, format change, validation, or transformation function on the data that it receives as input. In other words, data items processed by a provider are moved to a new location, validated against specified criteria, or undergo modification in structure or value. In this guide, the term **data sets** is used to describe data structures arranged in the form of layers, with data flowing from one layer to another during provisioning and reconciliation.

While creating a generic technology connector, you can specify the fields (user identity metadata) that must be included in each data set. You can also define mappings between fields of different data sets. A mapping serves one of the following purposes:

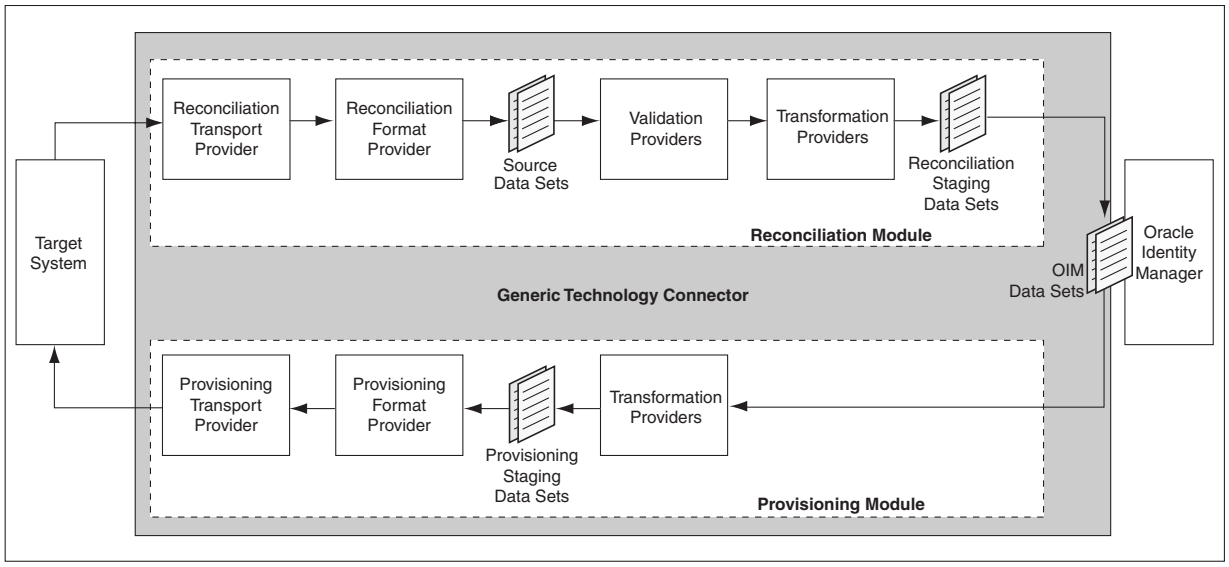
- Establishes a data flow path between fields of two data sets, for either provisioning or reconciliation

  A mapping of this type forms the basis for validations or transformations to be performed on data that is fetched from the target system.

- Creates a basis for comparing (matching) field values of two data sets

Figure 19–1 shows the functional architecture of a generic technology connector.

Figure 19–1 Functional Architecture of a Generic Technology Connector



The following sections describe the providers and data sets that constitute a generic technology connector:

- Providers and Data Sets of the Reconciliation Module
- Providers and Data Sets of the Provisioning Module
- OIM Data Sets

19.2.1 Providers and Data Sets of the Reconciliation Module

The reconciliation module consists of the following providers and data sets:

- Reconciliation Transport Provider

  A Reconciliation Transport Provider carries reconciliation data from the target system to Oracle Identity Manager. The manner in which this provider carries reconciliation data depends on the implementation of the provider. For example, a Reconciliation Transport Provider can read data from a file, accept data from a Web service, or query a database.

- Reconciliation Format Provider

  A Reconciliation Format Provider parses the reconciliation data fetched by the Reconciliation Transport Provider and converts this data into data structures that can be stored in Oracle Identity Manager.

- Source

  A Source data set holds the data processed by the Reconciliation Format Provider. This data set can have child data sets.

- Validation Provider

  A Validation Provider checks the data in the Source data sets against criteria you specify before passing the data to the reconciliation engine of Oracle Identity Manager.

Note: You can include more than one Validation Provider in a generic technology connector.

- Transformation Provider

  A Transformation Provider included in the reconciliation module modifies data received from the Validation Providers before passing on the data for the creation of reconciliation events in Oracle Identity Manager.

  The following is an example of a Transformation Provider function:

  Suppose the following are the values of two fields in the target system

  First Name: `John`

  Last Name: `Doe`

  A Transformation Provider can be used to create the following reconciliation field output:

  Login ID: `John.Doe`

- Reconciliation Staging

  A Reconciliation Staging data set holds user data that has been processed by the Validation Providers and Transformation Providers. This data set can have child data sets.

19.2.2 Providers and Data Sets of the Provisioning Module

The provisioning module consists of the following providers and data sets:

- Transformation Provider

  A Transformation Provider can be used to modify data items at the following stages:

  – During reconciliation, data can be modified before reconciliation events are created in Oracle Identity Manager.

  – During provisioning, data entered in Oracle Identity Manager process forms can be modified before it is sent to the target system.

  The following is an example of a Transformation Provider function:

  Suppose the following are the values of two fields in the target system:

  First Name: `John`

  Last Name: `Doe`

  A Transformation Provider can be used to create the following reconciliation field output:

  Login ID: `john.doe`

- Provisioning Staging

  A Provisioning Staging data set holds user data before it is sent to the Provisioning Format Provider. This data is the output of the transformation functions that are run on the user data or account data stored in Oracle Identity Manager. This data set can have child data sets.

- Provisioning Format Provider

  A Provisioning Format Provider converts Oracle Identity Manager provisioning data (received from the Transformation Provider) into a format that is supported by the target system.

- Provisioning Transport Provider

A Provisioning Transport Provider carries provisioning data from the Provisioning Format Provider to the target system. The manner in which this provider carries reconciliation data depends on the implementation of the provider. For example, a provider can copy data into a file, send data to a Web service, or post data to a database.

19.2.3 OIM Data Sets

The OIM data sets represent data that is stored in Oracle Identity Manager. Although these data sets are not part of the reconciliation or provisioning module, they are considered part of the generic technology connector because you can add fields to these data sets and create mappings between fields of these data sets and other data sets. The following are the OIM data sets:

- OIM - User

  The OIM - User data set holds the metadata (set of identity fields) that defines the OIM User. In trusted source reconciliation, this data set receives newly created or modified user account information from the Reconciliation Staging data set. In target resource reconciliation, the fields of the OIM - User data set can be used to establish a match between target system user accounts and existing OIM Users. This data set does not have child data sets.

- OIM - Account

  The OIM - Account data set holds the user account information that is stored in the process form fields of Oracle Identity Manager. This user account information is received from the Reconciliation Staging data sets. The OIM - Account data set can have child data sets.

19.3 Features of Generic Technology Connectors

The following sections discuss the features of generic technology connectors:

- Features Specific to the Reconciliation Module
- Other Features

19.3.1 Features Specific to the Reconciliation Module

The following features are specific to the reconciliation module:

- Trusted Source Reconciliation
- Account Status Reconciliation
- Full and Incremental Reconciliation
- Batched Reconciliation
- Reconciliation of Multivalued Attribute Data (Child Data) Deletion
- Failure Threshold for Stopping Reconciliation

19.3.1.1 Trusted Source Reconciliation

A generic technology connector can be used for trusted source reconciliation. During reconciliation in trusted mode:

- If the reconciliation engine detects new target system accounts, then it creates corresponding OIM Users.

- If the reconciliation engine detects changes to existing target system accounts, then the same changes are made in the corresponding OIM Users.

> **Note:** While creating a generic technology connector, if you do not select the Trusted Source Reconciliation option, then target resource reconciliation is enabled. In target resource reconciliation, only modifications to target system accounts are reconciled. New target system accounts detected during reconciliation are *not* automatically created in Oracle Identity Manager.

A generic technology connector that is used for trusted source reconciliation cannot be used for provisioning. This design feature was incorporated to ensure that you do not create or modify through Oracle Identity Manager user account information on a target system that is designated as a trusted source.

Connector objects, such as IT resources and resource objects, are created automatically at the end of the generic technology connector creation process. By default, the resource object of a generic technology connector is a trusted resource object. In other words, a generic technology connector is already compatible with the Multiple Trusted Source Reconciliation feature. This feature is discussed in the "Multiple Trusted Source Reconciliation" section of *Oracle Identity Manager Design Console Guide*.

> **Note:** In trusted source reconciliation, the reconciliation of multivalued (child) data is not supported.

19.3.1.2 Account Status Reconciliation

User account status information is used to track whether or not the owner of a target system account is to be allowed to access and use the account. If the target system does not store account status information in the format in which it is stored in Oracle Identity Manager, then you can use the predefined Translation Transformation Provider to implement account status reconciliation.

> **Note:**
>
> User account status reconciliation can be implemented independently of whether you select trusted source or target resource reconciliation.
>
> The Design Console offers features for implementing account status reconciliation, without using the Translation Transformation Provider. For more information, see "Account Status Reconciliation" in *Oracle Identity Manager Design Console Guide*.

19.3.1.3 Full and Incremental Reconciliation

While creating a generic technology connector, you can specify that you want to use the connector for full or incremental reconciliation.

You select incremental reconciliation if the target system supports a method for the reconciliation engine to identify records that have changed since the last reconciliation run. For example, if the target system time stamps the creation of or changes made to user records, then the reconciliation engine can identify records that have been added or modified since the last reconciliation run. In incremental reconciliation, only target system records that have changed after the last reconciliation run are reconciled (stored) into Oracle Identity Manager.

You select full reconciliation if any one of the following conditions is true:

- The target system does not support any method for the reconciliation engine to identify records that have changed since the last reconciliation run.
- You want to perform first-time reconciliation of all user account records in the target system.

In full reconciliation, all the reconciliation records are extracted from the target system. However, the optimized reconciliation feature identifies and ignores records that have already been reconciled in Oracle Identity Manager. This helps reduce the space occupied by reconciliation data. If this feature were not present, then the amount of data stored in the Oracle Identity Manager database would increase rapidly with each reconciliation run.

Note: The outcome of both full and incremental reconciliation is the same:

- All the target system records are reconciled during the first reconciliation run.
- From the second reconciliation run onward, target system records that are created or updated after the last reconciliation run are reconciled into Oracle Identity Manager.

19.3.1.4 Batched Reconciliation

You can specify a batch size for reconciliation. By doing this, you can break into batches the total number of records that the reconciliation engine fetches from the target system during each reconciliation run. This feature provides more control over the reconciliation process.

19.3.1.5 Reconciliation of Multivalued Attribute Data (Child Data) Deletion

You can specify whether or not you want to reconcile into Oracle Identity Manager the deletion of multivalued attribute data on the target system.

Note: Generic technology connectors do not support the reconciliation of parent data deletion. For example, if the account of user `John Doe` is deleted from the target system, then you cannot use a generic technology connector to reconcile this user account deletion into Oracle Identity Manager. This is also mentioned in the "General Known Issues" section on page 26-9.

19.3.1.6 Failure Threshold for Stopping Reconciliation

During reconciliation, Validation Providers can be used to run checks on target system data before it is stored in Oracle Identity Manager. You can set a failure threshold to automatically stop a reconciliation run if the percentage of records that fail the validation checks to the total number of records processed exceeds the specified threshold percentage.

19.3.2 Other Features

The following features are not specific to the reconciliation or provisioning module:

- Custom Data Fields and Field Mappings

- Custom Providers
- Multilanguage Support
- Custom Date Formats
- Propagation of Changes in OIM User Attributes to Target Systems

19.3.2.1 Custom Data Fields and Field Mappings

While creating a generic technology connector, you can specify the identity fields and field mappings (data flow paths) that must be used during reconciliation and provisioning.

19.3.2.2 Custom Providers

You can create custom providers if the predefined providers shipped with Oracle Identity Manager do not address the transport, format change, validation, or transformation requirements of your operating environment.

19.3.2.3 Multilanguage Support

Generic technology connectors can handle both ASCII and non-ASCII user data.

19.3.2.4 Custom Date Formats

While creating a generic technology connector, you can specify:

- The format of date values in target system records that are extracted during reconciliation
- The format in which date values must be sent to the target system during provisioning

19.3.2.5 Propagation of Changes in OIM User Attributes to Target Systems

While creating a generic technology connector, you can enable the automatic propagation of changes in OIM User attributes to the target system.

19.4 Roadmap for Information on Generic Technology Connectors in This Guide

The following is an overview of the remaining chapters and appendixes on generic technology connectors:

- Chapter 20, "Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager"

  This chapter describes the predefined providers that are shipped with Oracle Identity Manager.

- Chapter 21, "Creating Custom Providers for Generic Technology Connectors"

  This chapter describes the procedure to create custom providers.

- Chapter 22, "Creating Generic Technology Connectors"

  This chapter describes the procedure to create generic technology connectors.

- Chapter 23, "Managing Generic Technology Connectors"

  This chapter provides procedural information about modifying, exporting, and importing generic technology connectors.

- Chapter 24, "Best Practices for Creating and Using Generic Technology Connectors"

  This chapter discusses best practices that you must apply while creating and using generic technology connectors. Some of these guidelines have been repeated at appropriate places in this guide.

- Chapter 25, "Troubleshooting Generic Technology Connector Errors"

  This chapter provides solutions to some commonly encountered problems associated with using generic technology connectors for reconciliation and provisioning.

- Chapter 26, "Known Issues of Generic Technology Connectors"

  This chapter explains the limitations of the generic technology connector framework in this release of Oracle Identity Manager. Most of these limitations are also covered at appropriate places in the rest of the guide.

- Chapter 27, "Using Oracle Identity Manager As a Target System for Provisioning Operations"

  This chapter discusses instructions specific to creating a generic technology connector for use as the provisioning link to a target Oracle Identity Manager installation.

- Chapter 28, "Connector Objects Created by the Generic Technology Connector Framework"

  This chapter provides information about the connector objects that are automatically created by the generic technology connector framework.

Related Documentation on Connectors

The following guides provide additional information about connectors and the features that Oracle Identity Manager provides for working with connectors:

- *Oracle Identity Manager Design Console Guide*

  See this guide for additional information about Design Console procedures related to using generic technology connectors.

- *Oracle Identity Manager Globalization Guide*

  This guide contains information related to understanding globalized portions of the product, and working with resource bundles to localize user-configurable strings. This guide also provides instructions on developing resource bundles for generic technology connectors that you create.

20

Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager

The following predefined providers are shipped with the current release of Oracle Identity Manager:

> **Note:** You must determine the values of parameters for providers that you decide to use. You would need to use these values while creating the generic technology connector by using the Administrative and User Console.

20.1 Shared Drive Reconciliation Transport Provider

The Shared Drive Reconciliation Transport Provider reads data from flat files stored in staging directories and moves the files to an archiving directory. The staging and archiving directories must be shared for access from the Oracle Identity Manager server.

The following are parameters of this provider:

- **Staging Directory (Parent identity data)**

  Use this parameter to specify the path of the directory in which files containing parent data is stored. It is mandatory to specify a value for this parameter. This is a run-time parameter.

  In this guide, **parent data** means the user account information that is stored in the target system.

  Sample value for this parameter:

  ```
  T:/TargetSystemDirectory/ParentData
  ```

Note: If the staging directory is not on the server on which Oracle Identity Manager is installed, then it must be shared and mapped as a network drive on the Oracle Identity Manager server.

Data stored in the parent data files must conform to the following conventions:

– First line of the file

  The first line of the parent data file must be the file header that describes the contents of the file.

  The file header can be preceded by number signs (#). These are ignored while the file is read. However, you must ensure that there are no spaces at the start of the header. If you are using a language other than English, then you must not enter non-ASCII characters on this line.

  Note: There are no checks to stop you from entering non-ASCII characters on the first line. In addition, the generic technology connector framework can parse such characters. However, the use of non-ASCII characters would result in problems at the time when the connector objects are automatically created for the generic technology connector that you create. See the "Multilanguage Support" section on page 26-5 of the "Known Issues" chapter for more information about this limitation.

– Second line of the file

  The second line of the parent data file must contain the field names (metadata) for the data in the file.

  Note: In the generic technology connector context, the term **metadata** refers to the set of identity fields that constitute the user account information.

  If you are using a language other than English, then you must not enter non-ASCII characters on this line. See the Note in the preceding point for more information about this limitation.

– Third line of the file onward

  From the third line onward, the parent data file can contain data in the language that you have selected for Oracle Identity Manager. This language can have an ASCII or non-ASCII character set.

  Even if there is no data from the third line onward, reconciliation will take place and the files are archived.

The following are contents of a sample parent data file:

```
##Active Directory user
Name TD,Address TD,User ID TD
John Doe,Park Street,jodoe
Jane Doe,Mark Street,jadoe
```

See Also: The "Permissions to Be Set on the Staging and Archiving Directories" section on page 20-6

- **Staging Directory (Multivalued identity data)**

  Use this parameter to specify the path of the directory in which files containing multivalued (or child) user data (for example, role or group membership data) are stored. It is *not* mandatory to specify a value for this parameter. This is a run-time parameter.

  Note: In this guide, the terms **multivalued user data** and **child data** have been used interchangeably.

  Sample value for this parameter:

  ```
  T:/TargetSystemDirectory/ChildData
  ```

  Note:

  - The staging directory for parent data files cannot be the same as the staging directory for multivalued user data files. In addition, if the staging directory is not on the same server on which Oracle Identity Manager is installed, then it must be shared and mapped as a network drive on the Oracle Identity Manager server.
  - If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then you must not specify a value for the Staging Directory (Multivalued Identity Data) parameter. This is because the reconciliation of multivalued (child) data is not supported in trusted source reconciliation.

  For each type of multivalued user data, there must be a different file in the shared directory. For example, if the multivalued user data for a particular target system is group membership data and role data, then there must be one file for group membership data and a different file for role data.

  Data stored in the child data files must conform to the conventions (first line, second line, and remaining lines) that are specified for the parent data files.

  In addition, the same unique field must be present in the parent data file and each child data file. This field is used to uniquely link each record in the child data files with a single record in the parent data file. This structure is similar to the concept of integrity constraints (primary key-foreign key) in RDBMSs.

  Note: The unique field must be the first field in the child data files.

  The following are contents of a sample child data file holding role information that is linked to the sample parent data file listed earlier:

  ```
  ###Role
  User ID TD,Role Name TD,Role Type TD
  jodoe,admin1,admin
  jadoe,admin2,admin
  ```

The following are contents of a sample child data file holding group membership information that is linked to the sample parent data file listed earlier:

```
###Group Membership
User ID TD,Group Name TD,Group Type TD
jodoe,OracleDev1,OracleDev
jadoe,OracleDev2,OracleDev
jadoe,OracleDev3,OracleDev
jadoe,OracleDev4,OracleDev
jadoe,OracleDev5,ConnectorDev
```

Note that the name of the unique field, `User ID TD`, is the same in the child data files and the parent data file.

On the Step 3: Modify Connector Configuration page, the name of a child data set is the same as the header that you provide in the child data file. For these sample child data files, the child data sets would be labeled `Role` and `Group Membership`. In addition, on the Step 4: Verify Connector Form Names page, the default names displayed for forms corresponding to the child data sets would be `Role` and `Group Membership`. As mentioned in the "Step 4: Verify Connector Form Names Page" section on page 22-30, you can either accept the default form names or change them.

> **See Also:** The "Permissions to Be Set on the Staging and Archiving Directories" section on page 20-6

- **Archiving Directory**

  Use this parameter to specify the path of the directory in which parent and child data files that have already been reconciled are to be stored. This is a run-time parameter.

  It is mandatory to specify a value for this parameter.

  At the end of the reconciliation run, the data files are copied into the archiving directory and deleted from the staging directory.

  The files moved to the archiving directory are not time stamped or marked in any way. Therefore, while specifying the path of the archiving directory, bear in mind the following guidelines:

  – The archiving directory path that you specify must not be the same as the staging directory path. If you specify the same path, then the existing files in the archiving directory are deleted at the end of the reconciliation run.

  – If data files with the same names as the files used in the last reconciliation run are placed in the staging directory, then the existing files in the archiving directory are overwritten by the new files from the staging directory at the end of the current reconciliation run.

  These points are also mentioned in the "Step 2: Specify Parameter Values Page" section on page 24-2.

  > **See Also:** The "Permissions to Be Set on the Staging and Archiving Directories" section

- **File Prefix**

  Use this parameter to specify the prefix added to the names of files in the staging directories for both parent and child data files. During reconciliation, all files (in

the staging directories) with names that start with the specified prefix are processed, regardless of the file extension. This is a run-time parameter.

For example:

If you specify `usrdata` as the value of the File Prefix parameter, then data is parsed from the following files placed in the staging directory for multivalued (child) user data files:

```
usrdataRoleData.csv
usrdataGroupMembershipData.txt
```

Data is not extracted from the following files in the same directory, because the file names do not begin with `usrdata`:

```
RoleData.csv
GroupMembershipData.txt
```

- **Specified Delimiter**

  Use this parameter to specify the character that is used as the delimiter character in the parent and child data files. You can specify only a single character as the value of this parameter. This is a run-time parameter.

  Note: You cannot use the space character ( ) as a delimiter.

  In addition, you must ensure that the character you specify is used only as the delimiter in the data files. If this character is also used inside the data itself, then the data row (or record) is not parsed correctly. For example, you cannot use the comma (,) as the delimiter if it is also displayed inside the data itself.

- **Tab Delimiter**

  Use this parameter to specify whether or not the file is tab delimited. This is a run-time parameter. This parameter is ignored if you specify a value for the Specified Delimiter parameter.

- **Fixed Column Width**

  If the input file contains fixed-width data, then use this parameter to specify the character width of the data columns. This is a run-time parameter.

  Note: In this context, the term "fixed-width" refers to the number of characters in the data field, not the byte length of the field. This means that, for example, four characters of single-byte data and four characters of multibyte data are the same in terms of width.

  This parameter is ignored if you specify a value for the Specified Delimiter or Tab Delimiter parameter.

- **Unique Attribute (Parent Data)**

  For multivalued user data, use this parameter to specify the field that is common to both the parent data and child data files. In the examples described earlier, the requirement for a unique attribute is fulfilled by the `User ID TD` field, which is present in both the parent and child data files. This is a run-time parameter.

Note: If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then you must not specify a value for the Unique Attribute (Parent Data) parameter. This is because the reconciliation of multivalued (child) data is not supported in trusted source reconciliation.

- **File Encoding**

  Use this parameter to specify the character set encoding used in the parent and data files. This is a design parameter.

  Specify `Cp1251` for data files stored on a computer running an operating system with the English-language setting. This is the canonical name for the `java.io` API that is supported by the generic technology connector framework. For any other language that you select from the list given in the "Multilanguage Support" section on page 19-8, you must specify the canonical name for the corresponding `java.io` API listed on the following Web page:

  `http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html`

  Note: The canonical name that you specify for the API must be entered exactly the way it is displayed on this Web page. You must not change the case (uppercase or lowercase) of the canonical name.

  For example, if you want to specify the encoding set for the Traditional Chinese language on a Microsoft Windows computer, then you specify `MS950` as the value of the File Encoding parameter.

Permissions to Be Set on the Staging and Archiving Directories

You must ensure that the required permissions are set on the staging and archiving directories. The following table describes the effect of the various permissions on the shared directories that are used to hold staging and archiving data files.

Storage Entity	Access Permission	Reason for Access Permission Requirement
Staging directory for parent data files	Read	This permission is required for reconciliation to take place. An error message is logged if this permission is not applied.
Staging directory for parent data files	Write	This permission is required for the deletion of data files from the parent staging directory at the end of the archive process.
Staging directory for parent data files	Execute	Not applicable
Staging directory for child data files	Read	This permission is required for the reconciliation of child data. An error message is logged if this permission is not applied.
Staging directory for child data files	Write	This permission is required for the deletion of data files from the child staging directory at the end of the archive process.
Staging directory for child data files	Execute	Not applicable

Storage Entity	Access Permission	Reason for Access Permission Requirement
Archiving directory	Write	This permission is required for the copying of parent and child data files to the archiving directory during the archive process. Even if this permission is not applied: ■ Parent and child data reconciliation takes place. ■ Files are deleted from the parent and child staging directories if the required permissions have been set on those directories.
Archiving directory	Execute	Not applicable
Parent or child data file in staging directory	Read	This permission is required for the reconciliation of the data in the file. An error message is logged if this permission is not applied.
Parent or child data file in staging directory	Write	This permission is required for the deletion of the data file at the end of the archive process. An error message is logged if this permission is not applied. However, data in this file is reconciled.
Parent or child data file in staging directory	Execute	Not applicable

Note: Data files in the staging directory cannot be deleted if they are open in any editor.

20.2 CSV Reconciliation Format Provider

The CSV Reconciliation Format Provider converts reconciliation data that is in character-delimited, tab-delimited, or fixed-length format into a format that is supported by Oracle Identity Manager.

Although the CSV Reconciliation Format Provider is packaged as a standalone provider, all of its parameters are bundled with the Shared Drive Transport Provider. If you select the Shared Drive Transport Provider on the Step 1: Provide Basic Information page, then you must select the CSV Format Provider. When you select this provider, its parameters are displayed along with the Shared Drive Transport Provider parameters.

20.3 SPML Provisioning Format Provider

The SPML Provisioning Format Provider converts the provisioning data generated during a provisioning operation on Oracle Identity Manager into an SPML request that can be processed by an SPML-compatible target system.

Note: Each SPML request is sent in a SOAP message. The SOAP header carries authentication information for the request. The actual SPML request data is the SOAP message body.

See "SPML Web Service" in *Oracle Identity Manager Tools Reference* for information about the structure of the SPML-SOAP message.

You can access sample SOAP messages in the following directory:

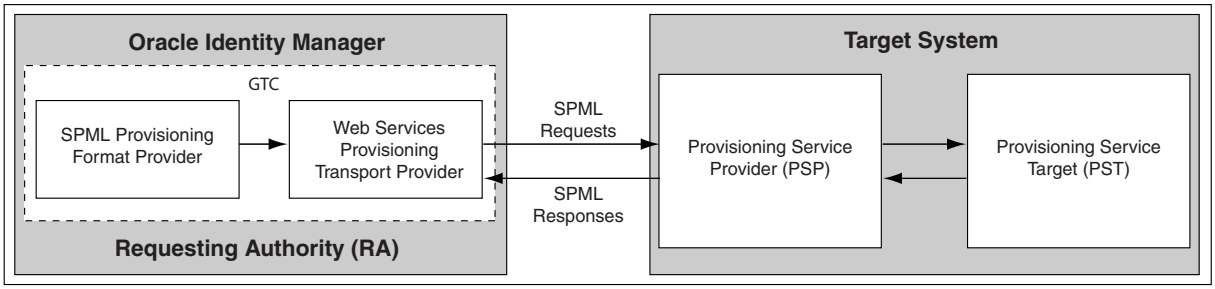
OIM_HOME/xellerate/GTC/Samples/spml

For information about the SPML specification, see the following Web page on the OASIS Web site at

http://www.oasis-open.org/specs/index.php#spmlv2.0

Figure 20–1 shows the setup of the system in which the SPML Provisioning Format Provider acts as the requesting authority (RA), and the target system provides the provisioning service provider (PSP) and the provisioning service target (PST).

Figure 20–1 Communication Between the SPML Provisioning Format Provider and the Target System



During actual provisioning, a Velocity template engine is used to create the SOAP-SPML requests. For the following processes, the provider generates SOAP requests based on the SPML 2.0 DSML profile:

- Add request
- Modify request for the following Oracle Identity Manager process tasks:
  - Field updated
  - Add child data
  - Modify child data
  - Delete child data
- Suspend request (for Disable Oracle Identity Manager process tasks)
- Resume request (for Enable Oracle Identity Manager process tasks)
- Delete request

The Create Organization, Update Organization, and Delete Organization are not supported. This is because the resource object created for a generic technology connector does not support provisioning operations for organizations. The Create Group, Update Group, and Delete Group operations are not supported. This is because group provisioning operations are not supported in Oracle Identity Manager.

When you select this provider, the following identity fields are displayed by default on the Step 3: Modify Connector Configuration page along with the `ID` field:

- `objectClass`
- `containerID`

For each provisioning task (for example, Create User and Modify User), the provider generates a request in a predefined format.

The following sections discuss the parameters of this provider:

- Run-Time Parameters
- Design Parameters

Depending on the application server that you use, some of the run-time and design parameters are mandatory and some have fixed values. The following sections discuss these parameters:

- Nonmandatory Parameters
- Parameters with Predetermined Values

20.3.1 Run-Time Parameters

The following are run-time parameters of the SPML Provisioning Format Provider:

- **Target ID**

  This value uniquely identifies the target system for provisioning operations.

- **User Name (authentication)**

  This is the user name of the account required to connect to the target system (PST) through the Web service interface (PSP).

- **User Password (authentication)**

  This is the password of the user account required to connect to the target system (PST) through the Web service interface (PSP).

20.3.2 Design Parameters

The following are design parameters of the SPML Provisioning Format Provider:

> **See Also:** For more information about the SOAP elements and attributes mentioned in this section, visit the following Web site
>
> `http://www.w3.org/TR/wsdl20/`

- **Web Service SOAP Action**

  In the WSDL file, this is the value of the `soapAction` attribute of the `operation` element.

- **WSSE Configured for SPML Web Service?**

  Select this check box if the Web service is configured to authenticate incoming requests by using WS-Security credentials.

- **Custom Authentication Credentials Namespace**

> **Note:** You need not specify a value for this parameter if you select the SPML Web Service WSSE Configured? check box.

This is the name of the credentials namespace that you have defined for the Web service. In most cases, this namespace is the same as the target namespace.

- **Custom Authentication Header Element**

  Note: You need not specify a value for this parameter if you select the SPML Web Service WSSE Configured? check box.

  This is the name of the element that will contain the credentials of the user account used to connect to the target system. In other words, this is the parent element in the custom authentication section of the SOAP message header.

- **Custom Element to Store User Name**

  Note: You need not specify a value for this parameter if you select the SPML Web Service WSSE Configured? check box.

  This is the name of the element in the custom authentication section that will contain the user name you specify as the value of the User Name (authentication) parameter.

- **Custom Element to Store Password**

  Note: You need not specify a value for this parameter if you select the SPML Web Service WSSE Configured? check box.

  This is the name of the element in the custom authentication section that will contain the user name you specify as the value of the User Password (authentication) parameter.

- **SPML Web Service Binding Style (DOCUMENT or RPC)**

  In the WSDL file, this is the value of the `style` attribute of the `binding` element. You must enter either `DOCUMENT` or `RPC`.

  Note: You must enter the value `DOCUMENT` or `RPC`. Do not use lowercase letters in the value that you specify.

- **SPML Web Service Complex Data Type**

  In the WSDL file, this is the value of the `name` attribute of the `complexType` element. This parameter is applicable only if the binding style is `DOCUMENT`. You must specify a value for this parameter if the target Web service is running on Oracle Application Server.

- **SPML Web Service Operation Name**

  In the WSDL file, this is the value of the `name` attribute of the `operation` element. This parameter is applicable only if the binding style is `RPC`.

- **SPML Web Service Target Namespace**

  In the WSDL file, this is the value of the `targetNamespace` attribute of the `definition` element.

- **SPML Web Service Soap Message Body Prefix**

This is the name of the custom prefix element that contains the SOAP message body. If the target Web service is running on Oracle WebLogic Server, IBM WebSphere Application Server, JBoss Application Server, or Oracle Application Server, then you need not specify a value for this parameter. However, if you are using a different application server, then you must enter the name of the custom prefix element. The following is the prefix element if the Web service is running on Oracle Application Server:

```
<SPMLv2Document xmlns="http://xmlns.oracle.com/OIM/provisioning">
```

- **ID Attribute for Child Dataset Holding Group Membership Information**

  This is the name of the unique identifier field for a Provisioning Staging child data set that holds group membership information. For provisioning operations on the child data set that contains this field, the SOAP packet will contain SPML code for group operations. The following is an SPML code block for this type of group operation:

```
<modification modificationMode="add">
  <capabilityData capabilityURI="urn:oasis:names:tc:SPML:2:0:reference"
mustUnderstand="true">
    <reference typeOfReference="memberOf"
xmlns="urn:oasis:names:tc:SPML:2:0:reference">
    <toPsoID ID="Groups:1" targeted="120"/>
</reference>
  </capabilityData>
</modification>
```

  For provisioning operations on the child data sets that do not contain this field, the SOAP packet will contain ordinary SPML code. The following is an SPML code block for this type of group operation:

```
<modification>
  <dsml:modification name="Group Membership" operation="add">
    <dsml:value>AdminOra, System Admins, USA</dsml:value>
  </dsml:modification>
</modification>
```

20.3.3 Nonmandatory Parameters

Depending on the application server you use, you need not specify values for the following parameters:

- **Oracle WebLogic Server**
  - SPML Web Service Complex Data Type
  - SPML Web Service Soap Message Body Prefix
  - ID Attribute for Child Dataset Holding Group Membership Information
- **IBM WebSphere Application Server**
  - SPML Web Service Complex Data Type
  - SPML Web Service Soap Message Body Prefix
  - ID Attribute for Child Dataset Holding Group Membership Information
- **JBoss Application Server**
  - SPML Web Service Complex Data Type

  - SPML Web Service Soap Message Body Prefix
  - ID Attribute for Child Dataset Holding Group Membership Information
- **Oracle Application Server**
  - SPML Web Service Soap Message Body Prefix
  - ID Attribute for Child Dataset Holding Group Membership Information

20.3.4 Parameters with Predetermined Values

Depending on the application server you use, you can specify predetermined values for the following parameters:

- **Oracle WebLogic Server**
  - Web Service URL:
    `http://`*`IP_address`*`:`*`port_number`*`/spmlws/OIMProvisioning`
  - SPML Web Service Binding style (DOCUMENT or RPC): `RPC`
  - SPML Web Service Operation Name: `processRequest`
- **IBM WebSphere Application Server**
  - Web Service URL:
    `http://`*`IP_address`*`:`*`port_number`*`/spmlws/HttpSoap11`
  - SPML Web Service Binding style (DOCUMENT or RPC): `DOCUMENT`
  - SPML Web Service Operation Name: `processRequest`
- **JBoss Application Server**
  - Web Service URL:
    `http://`*`IP_address`*`:`*`port_number`*`/spmlws/services/HttpSoap11`
  - SPML Web Service Binding style (DOCUMENT or RPC): `RPC`
  - SPML Web Service Operation Name: `processRequest`
- **Oracle Application Server**
  - Web Service URL:
    `http://`*`IP_address`*`:`*`port_number`*`/spmlws/HttpSoap11`
  - SPML Web Service Binding style (DOCUMENT or RPC): `DOCUMENT`
  - SPML Web Service Complex Data Type: `SPMLv2Document`
  - SPML Web Service Operation Name: `processRequest`

20.4 Web Services Provisioning Transport Provider

The Web Services Provisioning Transport Provider acts as a Web service client and carries provisioning request data from Oracle Identity Manager to the target system Web service.

The following types of target system Web services are supported:

- RPC-literal
- RPC-encoded
- DOCUMENT-literal

The following is the parameter of the Web Services Provisioning Transport Provider:

Web Service URL

Use this parameter to specify the URL of the Web service that you want to use for sending a provisioning request to the target system. This is a run-time parameter. In the WSDL file, the Web service URL is the value of the `location` attribute of the `wsdlsoap:address` element.

If you include the Web Services Provisioning Transport Provider in the generic technology connector that you create, then you may want to configure Secure Sockets Layer (SSL) communication between the target system and Oracle Identity Manager. The following section provides information about this procedure.

20.4.1 Configuring SSL Communication Between Oracle Identity Manager and the Target System Web Service

This section describes the procedure to configure the application server on which Oracle Identity Manager is installed for SSL communication.

You can perform the procedure described in this section only if all of the following conditions are true:

- You want to include the Web Services Provisioning Transport Provider in the generic technology connector that you plan to create.
- The target Web service is running on an SSL-enabled application server.

To configure SSL communication between Oracle Identity Manager and the target system Web service:

> **Note:** You can perform this procedure even before you create the generic technology connector.

1. Export the target application server certificate as follows:
   - For a target system Web service deployed on JBoss Application Server, Oracle WebLogic Server, or Oracle Application Server, run the following command:

     ```
     JAVA_HOME/jre/bin/keytool -export -alias default -file
     exported-certificate-file -keystore app-server-specific-keystore
     -storetype jks -storepass keystore-password -provider
     sun.security.provider.Sun
     ```

     In this command:
     * Replace *JAVA_HOME* with the full path to the SUN JDK directory.
     * Replace *exported-certificate-file* with the name of the file in which you want the exported certificate to be stored.
     * Replace *app-server-specific-keystore* with the path to the keystore on the application server.
     * Replace *keystore-password* with the password for the keystore.
   - For a target system Web service deployed on IBM WebSphere Application Server or Oracle Application Server on AIX, run the following command:

     ```
     JAVA_HOME/jre/bin/keytool -export -alias default -file
     exported-certificate-file -keystore app-server-specific-keystore -storetype
     jks -storepass keystore-password -provider com.ibm.crypto.provider.IBMJCE
     ```

In this command:

* Replace *JAVA_HOME* with the full path to the IBM JDK directory.
* Replace *exported-certificate-file* with the name of the file in which you want the exported certificate to be stored.
* Replace *app-server-specific-keystore* with path to the keystore on the application server.
* Replace *keystore-password* with the password for the keystore.

When the command is run, the exported certificate file is stored in the file that you specify as the value of *exported-certificate-file*.

2. Import the certificate file exported in the preceding step into the Oracle Identity Manager truststore as follows:

   a. Copy the certificate file exported in the preceding step into a temporary directory on the Oracle Identity Manager server.

   b. Run the following command:

```
JAVA_HOME/jre/bin/keytool -import -trustcacerts -alias servercert -noprompt
-keystore OIM_HOME\config\.xlkeystore -file certificate_file
```

   In this command:

   * Replace *JAVA_HOME* with full path to the JDK directory. For Oracle Identity Management Server deployed on IBM WebSphere Application Server, the path must be that of the IBM JDK directory. For Oracle Identity Manager deployed on JBoss Application Server, Oracle WebLogic Server, or Oracle Application Server, the path must be that of the SUN JDK directory.
   * Replace *OIM_HOME* with the full path of the Oracle Identity Manager home directory
   * Replace *certificate_file* with the path of the temporary directory into which you copy the certificate file.

   Note: If the application server is enabled for one-way SSL communication, then you need not perform the rest of this procedure.

3. Import the Oracle Identity Manager certificate into the target system application server truststore as follows:

   Note: Perform the following steps only if the application server is enabled for two-way SSL communication.

   a. Export the Oracle Identity Manager certificate file.

   For Oracle Identity Manager deployed on JBoss Application Server, Oracle WebLogic Server, or Oracle Application Server, run the following command:

```
JAVA_HOME/jre/bin/keytool -export -alias xell -file
OIM_HOME\config\xell.cert -keystore OIM_HOME\config\.xlkeystore -storetype
jks -provider sun.security.provider.Sun
```

   In this command:

- Replace *JAVA_HOME* with the full path to the SUN JDK directory.

- Replace *OIM_HOME* with the full path of the Oracle Identity Manager home directory.

For Oracle Identity Manager deployed on IBM WebSphere Application Server, run the following command:

```
JAVA_HOME/jre/bin/keytool -export -alias xell -file
OIM_HOME\config\xell.cert -keystore OIM_HOME\config\.xlkeystore -storetype
jks -provider com.ibm.crypto.provider.IBMJCE
```

In this command:

- Replace *JAVA_HOME* with the full path to the IBM JDK directory.

- Replace *OIM_HOME* with the full path of the Oracle Identity Manager home directory.

b. Import the certificate file that you export in Step 3.a into the truststore of the application server as follows:

Copy the exported Oracle Identity Manager certificate file to a temporary directory on the target application server.

Then, run the following command on the target application server:

– If the target application server is JBoss Application Server, Oracle WebLogic Server, or Oracle Application Server, then run the following command:

```
JAVA_HOME/jre/bin/keytool -import -alias alias -trustcacerts  -file
OIM-certificate-file -keystore app-server-specific-truststore
-storetype jks -storepass truststore-password -provider
sun.security.provider.Sun
```

In this command:

* Replace *JAVA_HOME* with the full path to the SUN JDK directory.

* Replace *alias* with an alias for the certificate in the truststore of the target application server.

* Replace *OIM-certificate-file* with the name of the exported Oracle Identity Manager certificate file.

* Replace *app-server-specific-truststore* with path to the truststore on the target application server.

* Replace *truststore-password* with the password for the truststore on the target application server.

– If the target application server is IBM WebSphere Application Server, then run the following command:

```
JAVA_HOME/jre/bin/keytool -import -alias alias -trustcacerts -file
OIM-certificate-file -keystore app-server-specific-truststore
-storetype pkcs12 -storepass truststore-password -provider
com.ibm.crypto.provider.IBMJCE
```

In this command:

* Replace *JAVA_HOME* with the full path to the SUN JDK directory.

* Replace *alias* with an alias for the certificate in the target truststore.

* Replace *OIM-certificate-file* with the name of the exported Oracle Identity Manager certificate file.

* Replace *app-server-specific-truststore* with the path to the truststore on the target application server.

* Replace *truststore-password* with the password for the truststore on the target application server.

See Also: SSL configuration documentation for the target application server

20.5 Transformation Providers

Note: Use the information provided in this section while performing the instructions given in the "Step 3: Modify Connector Configuration Page" section on page 22-15.

A Transformation Provider is used to transform user data while it is in transit between the source and destination data sets listed in the following table.

Source Data Set	Destination Data Set	Purpose of the Transformation
Source	Reconciliation Staging	Data is transformed before it is used to create reconciliation events.
OIM	Provisioning Staging	Data is transformed before it is used to create the provisioning request to be sent to the target system.

The following predefined Transformation Providers are included in the current release of Oracle Identity Manager:

- Concatenation Transformation Provider
- Translation Transformation Provider

20.5.1 Concatenation Transformation Provider

You use the Concatenation Transformation Provider to concatenate the values of two fields of data sets to create the input for a single field of another data set.

The following example explains the output format of this provider:

Suppose the input values are the following fields of the Source data set:

- First Name: `John`
- Last Name: `Doe`

When the Concatenation Transformation Provider is applied to these two fields, the output value is as follows:

```
John Doe
```

Note: As shown in the preceding example, the Concatenation Transformation Provider adds a space between the values of the two input fields.

The following procedure describes how to add a Concatenation Transformation Provider while creating a generic technology connector:

> **Note:** This procedure explains in detail the instruction given in Step 5 of the "Adding or Editing Fields in Data Sets" section on page 22-21. It is assumed that you have already selected the **Concatenation** option from the **Mapping Action** list on the Step 1: Field Information page and that you have performed Steps 2 and 3 given in that section.

On the Step 2: Mapping page in the pop-up window, perform the following steps:

1. From the **Dataset** list in the Input 1 region, select the data set containing the first field that you want to concatenate. Then, from the **Field Name** list, select the first field. Alternatively, you can use the **Literal** option to specify a literal (or fixed) value as the first concatenation input.

   For the example described earlier, from the **Dataset** list in the Input 1 region, select the data set containing the **First Name** field. Then, from the **Field Name** list, select **First Name**.

2. From the **Dataset** list in the Input 2 region, select the data set containing the second field that you want to concatenate. Then, from the **Field Name** list, select the second field. Alternatively, you can use the **Literal** option to specify a literal (or fixed) value as the second concatenation input.

   For the example described earlier, from the **Dataset** list in the Input 2 region, select the data set containing the **Last Name** field. Then, from the **Field Name** list, select **Last Name**.

20.5.2 Translation Transformation Provider

A translation operation involves accepting a certain (literal) value as input and converting it into another value.

The following example illustrates a translation operation:

Suppose the Source data set contains the Country field and data values stored in this field can take one of the following values:

- Austria
- France
- Germany
- India
- Japan

When these values are propagated to the Reconciliation Staging data set, you want to convert these values to the following:

- AT
- FR
- DE
- IN
- JP

To automate this translation, you can use the Translation Transformation Provider.

To use the Translation Transformation Provider:

1. Use the Design Console to create a lookup definition that stores the input and decoded values.

   See Also: *Oracle Identity Manager Design Console Guide* for detailed information about creating a lookup definition

   Note: While creating a lookup definition in the Lookup Definition form, you must select the Lookup Type option, and not the Field Type option.

   For the Country field example described earlier, the Code Key and Decode values are as shown in the following table.

Code Key	Decode
Austria	AT
France	FR
Germany	DE
India	IN
Japan	JP

2. Define a transformation (translation) mapping between the input field and output field for the translation. As mentioned earlier, a transformation can be set up between the following pairs of data sets:

   - Source and Reconciliation Staging
   - OIM and Provisioning Staging

   Note: This procedure explains in detail the instruction given in Step 5 of the "Adding or Editing Fields in Data Sets" section on page 22-21. It is assumed that you have already selected the **Concatenation** option from the **Mapping Action** list on the Step 1: Field Information page and that you have performed Steps 2 and 3 given in that section.

   a. On the Step 3: Mapping page, from the **Dataset** list in the Input region, select the data set containing the field that will provide the input value for the translation operation. Then, from the **Field Name** list, select the field itself.

      For the Country field example described earlier, select the data set containing the Country field and then select the Country field.

   b. In the Lookup Code Name region, select **Literal** and enter the name of the lookup definition that you create in the preceding step.

Note: You must not specify a data set name and field in the Lookup Code Name region. Although there is no validation to stop you from selecting a data set name and field, the translation operation would fail during actual reconciliation or provisioning operations.

This point is also mentioned in the "Mappings" section on page 24-5.

For the Country field example described earlier, select **Literal** then select the lookup definition you create in Step 1.

20.5.2.1 Configuring Account Status Reconciliation

User account status information is used to track whether or not the owner of a target system account is to be allowed to access and use the account. If required, you can use the Translation Transformation Provider to reconcile account status information.

Note: The Design Console offers an alternative method to configure account status reconciliation. This method does not involve the use of a generic technology connector. The "Account Status Reconciliation" section in *Oracle Identity Manager Design Console Guide* describes this method.

You need to use the Translation Transformation Provider only if account status values used in the target system are not the same as the values used in Oracle Identity Manager. For a target resource, Oracle Identity Manager uses the following values:

- Enabled state: `Enabled`
- Disabled state: `Disabled`

For a trusted source, Oracle Identity Manager uses the following values:

- Enabled state: `Active`
- Disabled state: `Disabled`

The procedure to configure account status reconciliation can be summarized as follows:

Note: Detailed instructions to perform these steps are provided later in this section.

1. Create a lookup definition that maps the status values used in the target system with the values used in Oracle Identity Manager.
2. While creating the generic technology connector, use the Translation Transformation Provider to create a transformation mapping between the fields that hold account status values in the Source data set and the Reconciliation Staging data set.

   The following example describes the action that you must perform:

   Suppose the following fields are used to hold account status values:

   - The User Status field of the Source data set holds the values `True` (for a user in the Enabled state) and `False` (for a user in the Disabled state).

- The User Status field of the Reconciliation Staging data set must hold one of the following pairs of values:
  - For target resource reconciliation, the field must hold `Enabled` or `Disabled`.
  - For trusted source reconciliation, the field must hold `Active` or `Disabled`.

  You must create a transformation mapping that converts the `True/False` values in the User Status field of the Source data set into corresponding `Enabled/Disabled` or `Active/Disabled` values. During reconciliation, these converted values are sent to the User Status field of the Reconciliation Staging data set.

3. Create a mapping between the field that holds account status values in the Reconciliation Staging data set and one of the following fields:
   - The OIM Object Status field of the OIM – Account data set, for target resource reconciliation
   - The Status field of the OIM – User data set, for trusted source reconciliation

   During reconciliation, this mapping is used to propagate status values from the Reconciliation Staging data set to the OIM – Account or OIM – User data set.

Detailed steps to configure account status reconciliation are as follows:

1. Create a lookup definition that maps the status values used in the target system with the values used in Oracle Identity Manager.

   See Also: The "Lookup Definition Form" section in *Oracle Identity Manager Design Console Guide*

   The Code Key values in the lookup definition must be the same as the values used to represent the account status in the target system. The Code Key and Decode values for both trusted and target resource reconciliation are as shown in the following table:

Code Key	Decode (for Trusted Source Reconciliation)	Decode (for Target Resource Reconciliation)
Target system status value for a user account that is in the Enabled state	`Active`	`Enabled`
Target system status value for a user account that is in the Disabled state	`Disabled`	`Disabled`

   Examples of Code Key values are `True/False`, `Yes/No`, and `1/0`. The Decode values must be set to the exact value, including the case (uppercase and lowercase), shown in the table.

   Note: While creating the lookup definition in the Lookup Definition form, you must select the Lookup Type option, and not the Field Type option.

2. The procedure to create the generic technology connector is described in Chapter 22. While creating the generic technology connector, perform the following steps on the Step 3: Modify Connector Configuration page:

   Note: These steps are a condensed version of the procedure described in the "Adding or Editing Fields in Data Sets" section on page 22-21. Refer to that section for a description of the terms and GUI elements mentioned in the following steps.

   a. If the target system status field is displayed on the Step 3: Modify Connector Configuration page, then click the Edit icon for the field in the Reconciliation Staging data set.

      If the field is not displayed, then click the Add icon of the Reconciliation Staging data set.

   b. On the Step 1: Field Information page, specify values for the following GUI elements:

      - **Field Name**: If you are adding the field, then specify a name for it. The field name that you specify must contain only ASCII characters, because non-ASCII characters are not allowed.
      - Mapping Action: Select **Create Mapping With Translation** from this list.
      - **Matching Only**: Ensure that this check box is deselected.
      - **Create End-to-End Mapping**: If you are adding the field, then select this check box.
      - **Multi-Valued Field**: Ensure that this check box is deselected.
      - **Data Type**: Select the data type of the field.
      - **Length**: Specify the character length of the field.
      - **Required**: Select this check box if you want to ensure that the field always contains a value.
      - **Encrypted**: Ensure that this check box is deselected.
      - **Password Field**: Ensure that this check box is deselected.

   c. Click **Continue**.

   d. On the Step 3: Provide Mapping Information page, perform the following steps:

      In the Input region:

      - From the **Dataset** list, select **Source**.
      - From the **Field Name** list, select the field that stores status values.

      In the Lookup Code Name region, select **Literal** and enter the name of the lookup definition that you create in Step 1.

   e. If required, select a validation check for the field and then click **Add**. In other words, select the Validation Provider that you want to use.

   f. Click **Continue**, and then click **Close**.

3. Create a mapping between the status field of the Reconciliation Staging data set and either the OIM Object Status field of the OIM - Account data set or the Status field of the OIM - User data set as follows:

   Note: These steps are a condensed version of the procedure described in the "Adding or Editing Fields in Data Sets" section on page 22-21.

   a. For target resource reconciliation, click the edit icon for the OIM Object Status field of the OIM - Account data set.

      For target resource reconciliation, click the edit icon for the Status field of the OIM - User data set.

      Note: If a mapping already exists between the status field of the Reconciliation Staging data set and the OIM Object Status field or Status field, then apply the instructions given in this step only where required.

   b. On the Step 1: Field Information page, specify values for the following GUI elements:

      – Mapping Action: Select **Create Mapping Without Transformation** from this list.

      – **Matching Only**: Ensure that this check box is deselected.

   c. Click **Continue**.

   d. In the Input region on the Step 3: Mapping page, select the status field of the Reconciliation Staging data set.

   e. Click **Continue**, **Continue**, and then click **Close**.

   f. To add or edit other fields displayed on the Step 3: Modify Connector Configuration page, continue with the procedure described in the "Adding or Editing Fields in Data Sets" section on page 22-21.

20.6 Validation Providers

Table 20–1 describes the Validation Providers that are shipped with this release of Oracle Identity Manager.

Note: Except for the Validate Date Format Provider, all the providers in this table are implementations of methods of the `GenericValidator` class in the Apache Jakarta Commons API.

Table 20–1 Validation Providers

Validation Provider	Description
IsNotBlankOrNull	Checks if the field value is null or blank

Table 20–1 (Cont.) Validation Providers

Validation Provider	Description
IsValidDate	Checks if the field value is a valid date for the locale that is in use **Note:** Date formats are different for different locales. When you select this provider, you also specify the locale whose date formats must be used for the validation.
IsInRange	Checks if the field value is within a range specified by a minimum and maximum value pair
IsByte	Checks if the field value can be converted to a byte primitive
IsDouble	Checks if the field value can be converted to a double primitive
IsFloat	Checks if the field value can be converted to a float primitive
IsInteger	Checks if the field value can be converted to an integer primitive
IsLong	Checks if the field value can be converted to a long primitive
IsShort	Checks if the field value can be converted to a short primitive
MatchRegexp	Checks if the field value matches the specified regular expression **Note:** A regular expression is a string that is used to describe or match a set of strings according to specific syntax rules.
MaxLength	Checks if the length of the field value is less than or equal to the specified value
MinLength	Checks if the length of the field value is greater than or equal to the specified value
Validate Date Format	Validates date values in target system records before these records are reconciled into Oracle Identity Manager The value of the Source Date Format parameter is used as the basis for validation. This Validation Provider is applied if you specify a value for the Source Date Format parameter on the Step 2: Specify Parameter Values page, regardless of whether or not you select this provider on the Step 3: Modify Connector Configuration page. **Note:** Unlike the other providers in this table, the Validate Date Format is not an implementation of a method of the `GenericValidator` class in the Apache Jakarta Commons API.

21

Creating Custom Providers for Generic Technology Connectors

You must create custom providers to address provider requirements that cannot be addressed by the predefined providers. This chapter discusses the procedure to create custom providers.

> **Note:** This is an optional step of the procedure. If the predefined providers address all your provider requirements, then you need not create custom providers.

The information in this chapter is divided into the following sections:

- Role of Providers
- Creating Custom Providers
- Reusing Providers

21.1 Role of Providers

The following sections discuss the role of providers during generic technology connector creation and use:

- Role of Providers During Generic Technology Connector Creation
- Role of Providers During Reconciliation
- Role of Providers During Provisioning

21.1.1 Role of Providers During Generic Technology Connector Creation

You create a generic technology connector by using the Administrative and User Console. Defining data sets and the flow of data between these data sets is one of the tasks of the connector creation procedure. The metadata detection process facilitates this task.

In the generic technology connector context, the term **metadata** refers to the set of identity fields that constitute the user account information. The term **metadata detection** refers to the reading and parsing of target system metadata by the providers.

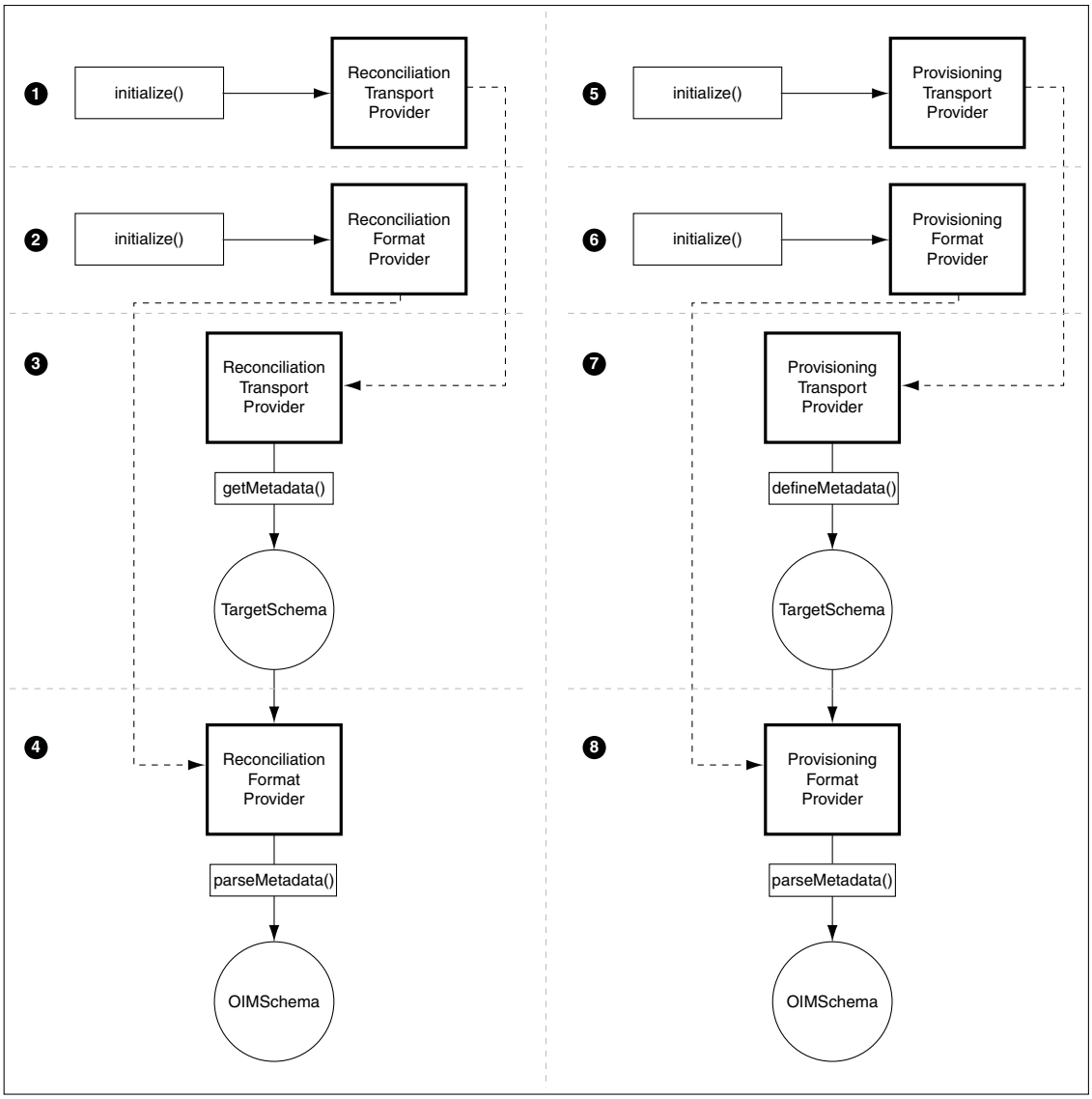
> **See Also:** The "Step 3: Modify Connector Configuration Page" section on page 22-15

The metadata detection feature is supported for all the provider types. In other words, when you create a custom provider, you can incorporate in the provider the capability to read metadata.

Note: In the Javadocs, the term **metadata definition** has been used instead of **metadata detection**.

Figure 21–1 shows the metadata detection process.

Figure 21–1 Metadata Detection Process



The following sequence of steps describe how metadata detection is performed. This sequence of steps is based on the assumption that you select both the Reconciliation and Provisioning options while creating the generic technology connector. If you do not select either the Reconciliation or the Provisioning option, then the corresponding steps are not performed.

See Also: The Javadocs for detailed information about the SPI methods and value objects mentioned in the following steps.

You can access the Javadocs at the following location:

OIM_HOME/documentation/SDK/javadocs/gc/index.html

In the Javadocs, the terms **metadata detection** and **metadata definition** have been used interchangeably.

1. The `initialize` method of the Reconciliation Transport Provider is called to create an instance of that provider.
2. The `initialize` method of the Reconciliation Format Provider is called to create an instance of that provider.
3. The `getMetadata` method of the Reconciliation Transport Provider is called to fetch metadata from the target system. The output of this method is the `TargetSchema` value object containing metadata fetched from the target system.
4. The `parseMetadata` method of the Reconciliation Format Provider is called to parse metadata fetched from the target system. The output of this method is the `OIMSchema` value object containing metadata fetched from the target system.

Note: The `OIMSchema` value object corresponds to the Source data sets discussed in the "Providers and Data Sets of the Reconciliation Module" section on page 19-3.

5. The `initialize` method of the Provisioning Transport Provider is called to create an instance of that provider.
6. The `initialize` method of the Provisioning Format Provider is called to create an instance of that provider.
7. If the Reconciliation Transport Provider and Reconciliation Format Provider are not able to detect metadata, then Steps 1 through 4 are repeated for the Provisioning Transport Provider and Provisioning Format Provider.

Note: After a provider is initialized, it is stored in the Oracle Identity Manager cache until any one of the following events occurs:

- Cache is purged.
- Oracle Identity Manager is restarted.
- The generic technology connector is modified after it is created.

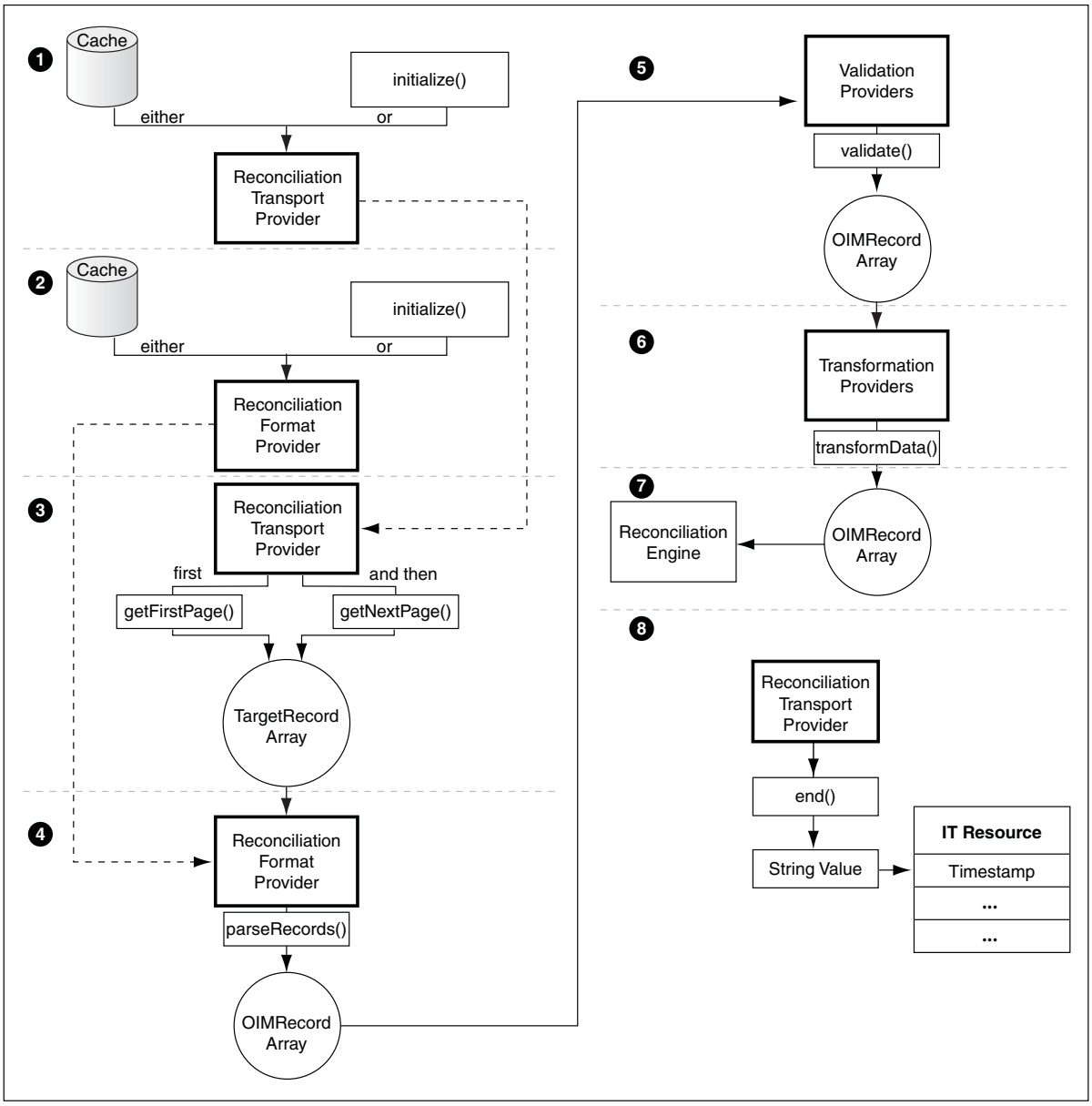
The Validation Providers and Transformation Providers are instantiated only when they are needed. They are not stored in cache.

The Shared Drive Reconciliation Transport Provider and CSV Reconciliation Format Provider can detect metadata from the target system. However, this function is not supported for the Web Services Provisioning Transport Provider and SPML Provisioning Format Provider.

21.1.2 Role of Providers During Reconciliation

Figure 21–2 shows the role of providers during reconciliation.

Figure 21–2 Role of Providers During Reconciliation



The following steps describe the role of providers during reconciliation:

1. If an instance of the Reconciliation Transport Provider is not available in cache, then the `initialize` method is called to create an instance of that provider.
2. If an instance of the Reconciliation Format Provider is not available in cache, then the `initialize` method is called to create an instance of that provider.
3. While using the Administrative and User Console to create a generic technology connector, you can specify a batch size for the reconciliation run. By using this parameter, you break into batches the total number of records that the reconciliation engine fetches from the target system during each reconciliation run. The default value of this parameter is `All`.

   If you had not specified a batch size, then at this stage of reconciliation, the `getFirstPage` method of the Reconciliation Transport Provider is called to fetch the entire set of target system records that are ready for reconciliation.

If you specified a batch size, then the `getFirstPage` method of the Reconciliation Transport Provider is called to fetch the first batch of target system records for reconciliation. The `getNextPage` method of the same provider is called (multiple times, if required) if there are more batches of target system records for reconciliation.

4. The `parseRecords` method of the Reconciliation Format Provider is called to process each record of the `TargetRecord` value objects array. The output of this method is an array of `OIMRecord` value objects.
5. While creating the generic technology connector, if you selected Validation Providers to validate data while it is in transit from the Source data sets to the Reconciliation Staging data sets, then:
   a. An instance of the Validation Provider is created.
   b. The `validate` method of each Validation Provider is run on the specified attribute of each record of the `OIMRecord` value objects array.

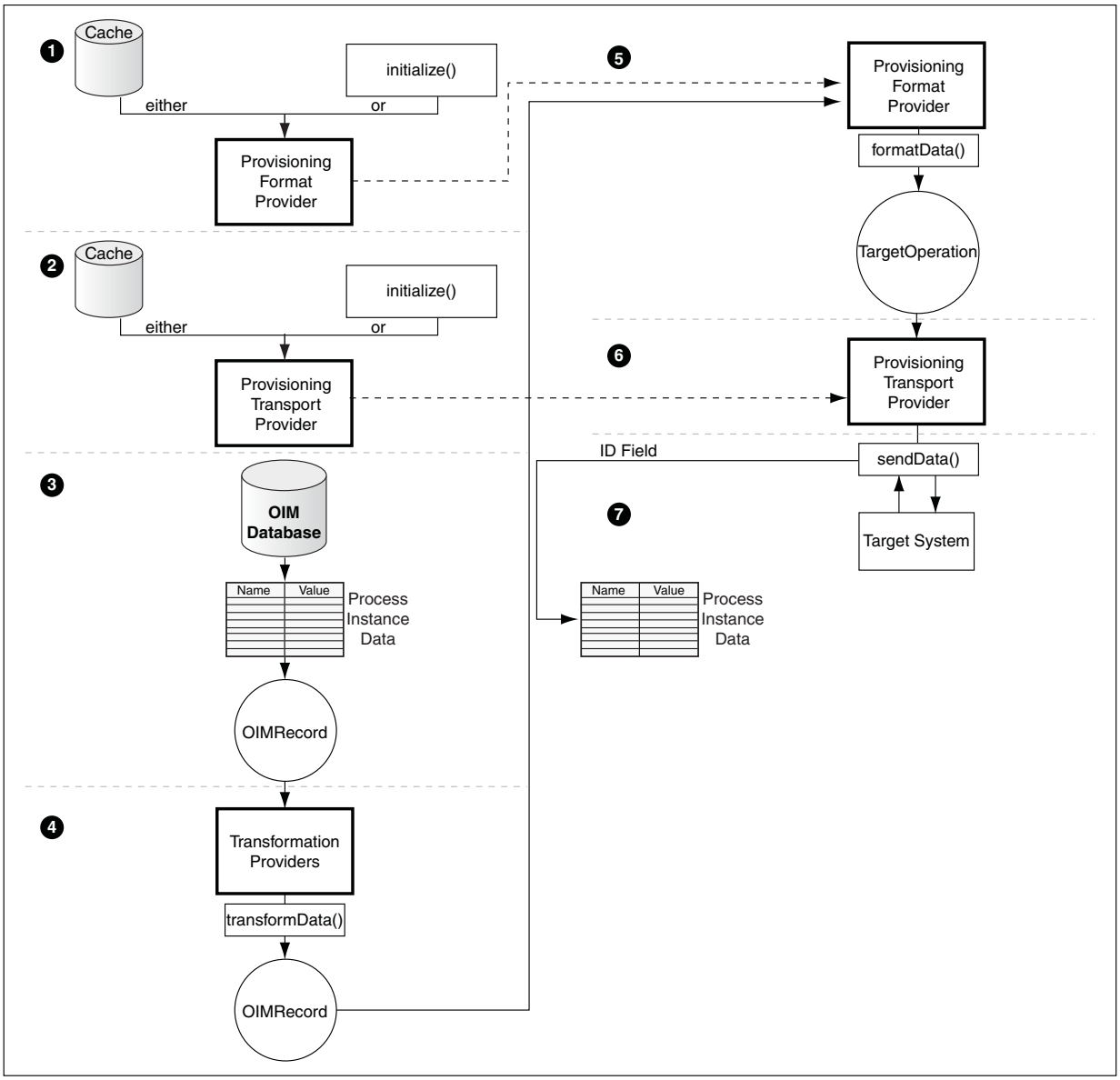
   If you did not select Validation Providers while creating the generic technology connector, then Step 5 is not performed and each element of the `OIMRecord` value objects array is passed on to Step 6.
6. While creating the generic technology connector, if you selected Transformation Providers to modify data that is in transit from the Source data sets to the Reconciliation Staging data sets, then:
   a. An instance of the Transformation Provider is created.
   b. The `transformData` method of the Transformation Providers processes the `OIMRecord` value objects array that was generated as the output of one of the following:
      – The `validate` method of each Validation Provider (if you selected Validation Providers)
      – The `parseRecords` method of the Reconciliation Format Provider (if you did not select Validation Providers)

   If you did not select Transformation Providers while creating the generic technology connector, then Step 6 is not performed and each element of the `OIMRecord` value objects array from the previous step (Step 4 or 5) is passed on to Step 7.
7. At this stage, the `OIMRecord` value objects array corresponds to the Reconciliation Staging data sets discussed in the "Providers and Data Sets of the Reconciliation Module" section on page 19-3. Each element of the `OIMRecord` value objects array is passed on to the reconciliation engine.
8. At the end of the reconciliation procedure, the `end` method of the Reconciliation Transport Provider is called. This method returns a string value, which the generic technology connector framework stores in the `Timestamp` parameter of the IT resource. The framework uses the `Timestamp` parameter to track the stage at which the reconciliation run was completed.

21.1.3 Role of Providers During Provisioning

Figure 21–3 shows the role of providers during provisioning.

Figure 21–3 Role of Providers During Provisioning



The following steps describe the role of providers during provisioning:

1. If an instance of the Provisioning Transport Provider is not available in cache, then the `initialize` method is called to create an instance of that provider.
2. If an instance of the Provisioning Format Provider is not available in cache, then the `initialize` method is called to create an instance of that provider.
3. The generic technology connector adapter is one of the connector objects created when you create the generic technology connector. This adapter converts the provisioning data record into a hashmap of name-value pairs. This hashmap contains process instance data. Each hashmap is then converted into an element of the `OIMRecord` value object. At this stage, the `OIMRecord` value object corresponds to the OIM data sets discussed in the "OIM Data Sets" section on page 19-5.

4. While creating the generic technology connector, if you selected Transformation Providers to modify data that is in transit from the OIM data sets to the Provisioning Staging data sets, then:
   a. An instance of the Transformation Provider is created.
   b. The `transformData` method of the Transformation Providers processes the specified attributes of the input `OIMRecord` value object and converts these records into an output `OIMRecord` value object. At this stage, the `OIMRecord` value object corresponds to the Provisioning Staging data sets discussed in the "Providers and Data Sets of the Provisioning Module" section on page 19-4.
5. The `formatData` method of the Provisioning Format Provider is called to process the `OIMRecord` value object. The output of this process is the `TargetOperation` value object.
6. The `sendData` method of the Provisioning Transport Provider is called to send the `TargetOperation` value object to the target system.
7. If the provisioning operation is a Create request, then the outcome is one of the following events:
   - On successful completion of the Create operation on the target system, the ID field value assigned to the newly created user account is returned by the `sendData` method. This value is then passed on to the generic technology connector framework, which posts this value to the database.
   - If the ID field value is not returned, then it is assumed that the Create operation has failed. An error message is then displayed on the Administrative and User Console.
   - If the operation fails at any stage after the name-value pairs are created, then an error message is displayed on the Administrative and User Console.

   If the provisioning operation is an Update or Delete request, then the ID field is one of the name-value pairs. When this type of provisioning request is sent, the outcome is one of the following events:
   - If the operation fails at any stage after the name-value pairs are created, then an error message is displayed on the Administrative and User Console.
   - On successful completion of the Update or Delete operation, the ID field value may or may not be returned depending on the implementation of the Provisioning Transport Provider.

     In either case, the generic technology connector framework does not need the ID field value.

21.2 Creating Custom Providers

The procedure to create custom providers can be divided into the following steps:

1. Determining Provider Requirements
2. Identifying the Provider Parameters
3. Developing Java Code Implementations of the Value Objects
4. Developing Java Code Implementations of the Provider SPI Methods
5. Developing Java Code for Logging and Exception Handling
6. Creating the Provider XML File

7. Creating Resource Bundle Entries for the Provider
8. Deploying the Provider

21.2.1 Determining Provider Requirements

Guidelines for determining provider requirements are divided into the following sections:

- Determining the Reconciliation Provider Requirements
- Determining the Provisioning Provider Requirements

21.2.1.1 Determining the Reconciliation Provider Requirements

Apply the following guidelines to determine the reconciliation provider requirements:

- If you want to use the target system only as a source of user account information for Oracle Identity Manager, then you need only the Reconciliation Transport Provider and Reconciliation Format Provider. You do not need the Provisioning Transport Provider and Provisioning Format Provider.

  If you are going to include the reconciliation module in the generic technology connector, then you must include both the Reconciliation Transport Provider and the Reconciliation Format Provider, even if you do not need any one of these providers. This guideline is illustrated by the following example:

  The function of the Reconciliation Format Provider is to convert target system data into a format that is supported by Oracle Identity Manager. Even if the target system generates data in a format supported by Oracle Identity Manager, you must include the Reconciliation Format Provider when you create the generic technology connector.

- You must create custom providers only to address provider requirements that are not addressed by the predefined providers.

  The types of providers you must include in the generic technology connector depend on the data formats and data transport mechanisms that your target system supports. If any combination of the data formats and data transport mechanisms are compatible with any combination of the predefined providers, then you need not create custom providers.

  For example, if your target system can generate reconciliation data files in comma-delimited format, then you can use the Shared Drive Reconciliation Transport Provider and CSV Reconciliation Format Provider. You need not create custom reconciliation providers.

  See Also: Reusing Providers on page 21-16

21.2.1.2 Determining the Provisioning Provider Requirements

Apply the following guidelines to determine the provisioning provider requirements for the provisioning module:

- If you want to use the target system only as a target for provisioning operations initiated on Oracle Identity Manager, then you need only the Provisioning Transport Provider and Provisioning Format Provider. You do not need the Reconciliation Transport Provider and Reconciliation Format Provider.

  If you are going to include the provisioning module in the generic technology connector, then you must include both the Provisioning Transport Provider and

the Provisioning Format Provider, even if you do not need any one of these providers. This guideline is illustrated by the following example:

The function of the Provisioning Format Provider is to convert Oracle Identity Manager data into a format that is supported by the target system. Even if the target system supports the output data format of Oracle Identity Manager, you must include the Provisioning Format Provider when you create the generic technology connector.

- You must create custom providers only to address provider requirements that are not addressed by the predefined providers.

  The types of providers you must include in the generic technology connector depend on the data formats and data transport mechanisms that your target system supports. If any combination of the data formats and data transport mechanisms are compatible with any combination of the predefined providers, then you need not create custom providers.

  For example, if your target system is a Web service that can accept and parse SPML-based provisioning requests packaged in SOAP messages, then you can use the SPML Provisioning Format Provider and Web Services Provisioning Transport Provider. You need not create custom provisioning providers.

See Also: Reusing Providers on page 21-16

21.2.2 Identifying the Provider Parameters

Provider parameters are the values that a provider must perform its intended function. For example, a Provisioning Transport Provider that copies provisioning request files to the target system server would need the connection parameters required to connect to the target system.

While creating a generic technology connector, you specify values for the parameters of the providers that you select for the generic technology connector.

For the custom provider that you are creating, you must identify all the parameters required for the provider to function. You must also categorize these parameters as run-time and design parameters.

A run-time parameter represents a value that is not constrained by the design of the provider. For example, the location of the directories containing data files that you want to reconcile is a run-time parameter. A design parameter represents a value or set of values that is defined as part of the provider design. For example, the character set encoding formats that can be parsed by a Reconciliation Format Provider is a design parameter for that provider.

21.2.3 Developing Java Code Implementations of the Value Objects

Develop the Java code implementations of the value objects listed in Table 21–1. As described earlier in this chapter, these value objects are used at various stages of provider operations.

Note:

- You need not develop Java code implementations of the value objects that you are not going to include in the generic technology connector.
- You can access the Javadocs at the following location:

  OIM_HOME/documentation/SDK/javadocs/gc/index.html

Table 21–1 Value Objects Used During Provider Operations

Area of Use	Value Object	Javadocs Package
Metadata Detection	`TargetSchema`	`com.thortech.xl.gc.vo.designtime`
	`OIMSchema`	`com.thortech.xl.gc.vo.designtime`
Provisioning	`TargetOperation`	`com.thortech.xl.gc.vo.runtime`
Reconciliation	`TargetRecord`	`com.thortech.xl.gc.vo.runtime`
	`OIMRecord`	`com.thortech.xl.gc.vo.runtime`

You can access sample code files for each provider type in the respective provider type directory at the following location:

OIM_HOME/xellerate/GTC/Samples

For example, if you are creating an implementation of the `TargetOperation` value object, then see the following sample code file:

OIM_HOME/xellerate/GTC/Samples/provisioningTransportProvider/MapProvInput.java

21.2.4 Developing Java Code Implementations of the Provider SPI Methods

Develop the Java code implementations of the SPI methods that are used during provider operations. As described earlier in this chapter, these SPI methods are called at various stages of provider operations. See the `Package com.thortech.xl.gc.spi` page of the Javadocs for links to information about the SPI methods of each provider.

You can access sample code files for each provider type in the respective provider type directory at the following location:

OIM_HOME/xellerate/GTC/Samples

For example, if you are creating a Provisioning Format Provider, then see the following sample code file:

OIM_HOME/xellerate/GTC/Samples/provisioningFormatProvider/PrepareDataHMap.java

Note: You need not develop Java code implementations of SPI methods for the providers that you are not going to include in the generic technology connector.

21.2.5 Developing Java Code for Logging and Exception Handling

Oracle recommends that you to incorporate logging in the Java code implementations of the value objects and SPI methods. By doing this, you can simplify the process of troubleshooting errors that may occur when you use the providers.

The logging modules for the generic technology connector framework are an extension of the logging functionality of Oracle Identity Manager. Table 21–2 lists the modules that are specific to the supported provider types.

Table 21–2 Logging Modules Specific to the Supported Provider Types

Logging Module	Functional Module of the Generic Technology Connector Framework
`XELLERATE.GC.PROVIDER.PROVISIONINGFORMAT`	Provisioning Format Provider
`XELLERATE.GC.PROVIDER.PROVISIONINGTRANSPORT`	Provisioning Transport Provider
`XELLERATE.GC.PROVIDER.RECONCILIATIONTRANSPORT`	Reconciliation Transport Provider
`XELLERATE.GC.PROVIDER.RECONCILIATIONFORMAT`	Reconciliation Format Provider
`XELLERATE.GC.PROVIDER.TRANSFORMATION`	Transformation Provider
`XELLERATE.GC.PROVIDER.VALIDATION`	Validation Provider

You can use the sample code files as a reference for using these modules to incorporate logging in the custom provider.

See the Javadocs and sample code files for information about incorporating exception handling in the custom provider.

21.2.6 Creating the Provider XML File

The provider XML file contains the data required to register the provider with the generic technology connector framework. You must create the provider XML file. Table 21–3 describes the elements that you can include in the provider XML files for custom providers.

> **Note:** You can use a single provider XML file to define any number of providers. Alternatively, you can create a provider XML file for each provider that you create.

You must ensure that the provider XML file adheres to the schema definition provided in the following file:

OIM_HOME`/xellerate/GTC/Schema/Providers-def.xsd`

Table 21–3 Elements of the Provider XML File

Element	Description
`Provider`	Root element of the provider XML file
`Reconciliation`	Parent element of the configuration elements that are used to describe Reconciliation Providers
`Provisioning`	Parent element of the configuration elements that are used to describe Provisioning Providers

Table 21–3 (Cont.) Elements of the Provider XML File

Element	Description
`Transformation`	Parent element of the configuration elements that are used to describe Transformation Providers
`Validation`	Parent element of the configuration elements that are used to describe Validation Providers
`ReconTransportProvider`	Parent element of the configuration elements that are used to describe a Reconciliation Transport Provider This element has the following attributes: `name`: Name of the provider `class`: Name of the Java class of the provider implementation
`ReconFormatProvider`	Parent element of the configuration elements that are used to describe a Reconciliation Format Provider This element has the following attributes: `name`: Name of the provider `class`: Name of the Java class of the provider implementation
`ProvFormatProvider`	Parent element of the configuration elements that are used to describe a Provisioning Format Provider This element has the following attributes: ■ `name`: Name of the provider ■ `class`: Name of the Java class of the provider implementation
`ProvTransportProvider`	Parent element of the configuration elements that are used to describe a Provisioning Transport Provider This element has the following attributes: ■ `name`: Name of the provider ■ `class`: Name of the Java class of the provider implementation
`TransformationProvider`	Parent element of the configuration elements that are used to describe a Transformation Provider This element has the following attributes: ■ `name`: Name of the provider ■ `class`: Name of the Java class of the provider implementation
`ValidationProvider`	Parent element of the configuration elements that are used to describe a Validation Provider This element has the following attributes: ■ `name`: Name of the provider ■ `class`: Name of the Java class of the provider implementation
`Configuration`	Parent element of the configuration elements of any type of provider

Table 21–3 (Cont.) Elements of the Provider XML File

Element	Description
`Parameter`	Element that provides information about a parameter of a provider The `Parameter` element has the following attributes: ■ `type`: Type of parameter, either `Runtime` or `Designtime` ■ `datatype`: Data type of parameter, either `String` or `Boolean`. Any parameter whose data type is not Boolean must be represented as a string. ■ `required`: Specifies whether or not the parameter is mandatory ■ `encrypted`: Specifies whether or not the parameter display must be encrypted ■ `name`: Name of the parameter ■ `datalength`: Character length of the parameter value
`DefaultAttribute`	Child element of the `Configuration` element This element must be included only in the `ProvFormatProvider` element. It has the following attributes: ■ `datatype`: Data type of parameter, either `String` or `Boolean`. Any parameter whose data type is not Boolean must be represented as a string. ■ `name`: Name of the parameter ■ `encrypted`: Specifies whether or not the parameter display must be encrypted ■ `size`: Size of the default attribute Some data attributes included in the provisioning request are essential for the provisioning operation to be successfully completed. Because the Provisioning Format Provider generates the final provisioning input data format, the definition of this provider must include these mandatory data attributes. Therefore, if such attributes are required by a target system, then they must be defined by using the `DefaultAttribute` element in the Provisioning Format Provider XML file.
`Response`	Child element of the `Configuration` element This element must be included only in the `ProvFormatProvider`, `ProvTransportProvider`, `TransformationProvider`, and `ValidationProvider` elements. It represents the response returned from the providers that are called by the provisioning engine. This response is displayed on the Oracle Identity Manager Administrative and User Console. This element has the following attributes: ■ `code`: Corresponds to the Oracle Identity Manager process task response code to be generated ■ `description`: Corresponds to the description of the Oracle Identity Manager process task response code to be generated **Note:** For a Provisioning Format Provider or Provisioning Transport Provider, you must ensure that the sum of the number of characters of the `name` attribute of the `ProvFormatProvider` or `ProvTransportProvider` element and the number of characters of the `Response` element is less than or equal to 70. If the sum of the number of characters exceeds 70, then the response code cannot be stored in the database and an error is thrown.

If required, you can view the contents of sample XML files for each provider type in the respective provider type directory at the following location:

OIM_HOME`/xellerate/GTC/Samples`

For example, if you want to create a Provisioning Format Provider, then see the following sample XML file:

OIM_HOME/xellerate/GTC/Samples/provisioningFormatProvider/PrepareDataHMapProvFormat.xml

21.2.7 Creating Resource Bundle Entries for the Provider

A resource bundle is a file containing locale-specific text strings. At run time, Oracle Identity Manager reads these text strings and displays them as GUI element labels and messages on the Administrative and User Console. The file extension of a resource bundle is `.properties`.

During installation of Oracle Identity Manager, resource bundles for each of the supported languages are copied to the Oracle Identity Manager server. These include the resource bundles for the predefined providers.

For a custom provider, you must create resource bundle entries for each locale that you plan to use. The following is a summary of the steps involved in creating a resource bundle:

> **See Also:** *Oracle Identity Manager Globalization Guide* for detailed information about creating resource bundle entries
>
> Guidelines on, for example, the resource bundle file naming convention are explained in this guide.

1. Open a new file in a text editor.
2. In this file, create entries for the following text strings:

> **Note:**
> - In the resource bundle file, you must provide localized text for the part of each line that follows the equal sign (=).
> - The `Provider_Type`, `Parameter_Name`, and `RESPONSE_CODE` values mentioned in this section must be the same as the values you specify in the provider XML file while performing the procedure described in the "Creating the Provider XML File" section on page 21-11.

- Provider names

  The format for provider names is as follows:

  gc.provider.*Provider_Type*.*Provider_Name*=*Label_string_in_the_required_language*

  The following is an English-language example of the provider name entry for a Provisioning Format Provider:

  gc.provider.ProvFormatProvider.SPML=SPML

- Provider parameter labels and description

  The format for provider parameter labels and parameter descriptions is as follows:

  gc.*Provider_Type*.*Provider_Name*.*Parameter_Name*.label=*Parameter_label_in_the_required_language*
  gc.*Provider_Type*.*Provider_Name*.*Parameter_Name*.description=*Parameter_descrip*

tion_in_the_required_language

The following is an English-language example of the provider parameter label and parameter description entries for a Provisioning Format Provider:

```
gc.ProvFormatProvider.SPML.targetID.label=Target ID
gc.ProvFormatProvider.SPML.targetID.description=Target ID of the
provisioning target
```

- Response codes and descriptions

  The format for response codes and descriptions is as follows:

  ```
  GC.GCPROV.PROVIDER_TYPE.PROVIDER_NAME.RESPONSE_CODE=Response_code_in_the_re
  quired_language
  GC.GCPROV.PROVIDER_TYPE.PROVIDER_NAME.RESPONSE_CODE.description=Description
  _in_the_required_language
  ```

  The following is an English-language example of the response code and description entries for a Provisioning Format Provider:

  ```
  GC.GCPROV.ProvFormatProvider.SPML.SPML_VELOCITY_PROPERTIES_NOT_READ=SPML
  Velocity Properties Not Read
  GC.GCPROV.ProvFormatProvider.SPML.SPML_VELOCITY_PROPERTIES_NOT_READ.descrip
  tion=Necessary SPML template properties could not be read.
  ```

- Metadata detection error messages

  The format for metadata detection error messages is as follows:

  ```
  gc.error.Provider_Type.Provider_Name.ERROR_CODE=Error_Description
  ```

  Here, *ERROR_CODE* must be the same as the value of the `errorCode` string passed as an argument to the constructor of the exception class. For example, the following is one of the constructors of the `ReconciliationTransportException` class:

  ```
  ReconciliationTransportException(java.lang.String errorCode,
  java.lang.String isMessage)
  ```

  You must add lines in the resource bundle for all possible values of the `errorCode` string.

  The following is an English-language example of the metadata detection error message for a Reconciliation Transport Provider:

  ```
  gc.error.ReconTransportProvider.SharedDrive.NO_READ_FILE=There are no
  readable files to detect metadata.
  ```

3. Save and close the resource bundle.

21.2.8 Deploying the Provider

To deploy the provider:

1. Deploy the JAR files as follows:

   a. Compile and package all the Java code files in a JAR file.

      The following JAR file contains the code files for all the sample code files:

      OIM_HOME/xellerate/GTC/Samples/xliGTCProviderSamples.jar

   b. Copy the JAR file into the following directory:

OIM_HOME/xellerate/JavaTasks

Note: In a clustered environment, you must copy each file that you create to the corresponding directory on each node of the cluster.

2. Deploy the provider XML files as follows:
   a. Copy the provider XML file into the following directory:

      OIM_HOME/xellerate/GTC/ProviderDefinitions

      Note: In a clustered environment, you must copy each file that you create to the corresponding directory on each node of the cluster.

   b. Restart Oracle Identity Manager.
   c. To check if the provider XML file has been correctly registered:

      i. Log in to the Administrative and User Console.

      ii. Expand **Generic Technology Connector**, and then click **Create**. If there are any errors in the provider XML file, then an error message is displayed.

      If an error message is displayed, then fix the problem in the XML file, restart Oracle Identity Manager, and repeat Steps i and ii.

      Repeat this procedure until no error messages are displayed when you click Create.
3. Deploy the provider resource bundles as follows:
   a. Copy the resource bundles into the following directory:

      OIM_HOME/xellerate/connectorResources

      Note: In a clustered environment, you must copy each file that you create to the corresponding directory on each node of the cluster.

   b. For the new resource bundle entries to take effect, either run the `PurgeCache` script or restart the application server. See *Oracle Identity Manager Best Practices Guide* for information about running the `PurgeCache` utility.

21.3 Reusing Providers

Format Providers and Transport Providers work in pairs. During reconciliation, the output of the Reconciliation Transport Provider is passed on to the Reconciliation Format Provider. During provisioning, the output of the Provisioning Format Provider is passed on to the Provisioning Transport Provider. This means that the implementation of the Transport Providers and Format Providers is linked through the implementation of the value objects that are passed between them. This dependency forms the basis of guidelines on reusing Format Providers and Transport Providers.

In contrast, a Validation Provider or Transformation Provider does not have any such dependency on other providers. Therefore, there are no guidelines on reusing Validation Providers and Transformation Providers. You can reuse both predefined and custom Transformation and Validation providers, because their action is not specific to the data format or data transport mechanism of the target system.

Guidelines on reusing Format Providers and Transport Providers are dividing into the following sections:

- Reusing Reconciliation Providers
- Reusing Provisioning Providers

21.3.1 Reusing Reconciliation Providers

As described in the "Role of Providers During Reconciliation" section on page 21-3, the `TargetRecord` value object is used to exchange data between the Reconciliation Transport Provider and the Reconciliation Format Provider. The Reconciliation Transport Provider creates an array of `TargetRecord` value objects for the target system records fetched during reconciliation. The Reconciliation Format Provider then processes the data in the value objects array and passes it on to the reconciliation engine.

Suppose the operating environment of your organization contains two target systems, `TS1` and `TS2`. `TS1` offers a Web-based interface for extracting data during reconciliation. `TS2` provides APIs for enabling other applications to read data from its identity store. Both target systems support the same data format. If you want to reconcile user data from both target systems, then you must create one generic technology connector for each target system. For each generic technology connector, you must create a Reconciliation Transport Provider. However, instead of creating a Reconciliation Format Provider for each generic technology connector, you can create and reuse a single Reconciliation Format Provider. Similarly, if `TS1` and `TS2` supported the same data transport mechanism (even if they do not support the same data format), then you can reuse the Reconciliation Transport Provider and create different Reconciliation Format Providers.

If you want to reuse a Reconciliation Transport Provider, then you must ensure that the implementation of the `TargetRecord` value object does not contain code that is specific to the function performed by the Reconciliation Format Provider. If you want to reuse a Reconciliation Format Provider, then you must ensure that the implementation of the `TargetRecord` value object does not contain code that is specific to the function performed by the Reconciliation Transport Provider.

Reusing the Predefined Reconciliation Providers

The implementation of the Shared Drive Reconciliation Transport Provider and CSV Reconciliation Format Provider is such that these predefined providers are built for a fixed combination of data formats and a single data transport mechanism. The Shared Drive Reconciliation Transport Provider reads data from flat files and passes an array of `TargetRecord` value objects to the CSV Reconciliation Format Provider. Paged reconciliation and multivalued (child) data reconciliation are two of the factors on which the implementation of the Shared Drive Reconciliation Transport Provider is based. These factors require the provider to be able to parse target system data before it can create an array of `TargetRecord` value objects. In other words, the ability of the Shared Drive Reconciliation Transport Provider to parse certain types of target system data and the ability of the CSV Reconciliation Format Provider to use only the output provided by the Shared Drive Reconciliation Transport Provider makes them interdependent. Therefore, the parameters of the CSV Reconciliation Format Provider are bundled along with those of the Shared Drive Reconciliation Transport Provider.

For this reason, you cannot use the Shared Drive Reconciliation Transport Provider with a custom Reconciliation Format Provider and you cannot use the CSV Format Provider with a custom Reconciliation Transport Provider.

21.3.2 Reusing Provisioning Providers

As described in the "Role of Providers During Provisioning" section on page 21-5, the `TargetOperation` value object is used to exchange data between the Provisioning Transport Provider and the Provisioning Format Provider. The Provisioning Format Provider creates a `TargetOperation` value object out of the provisioning data to be sent to the target system. The Provisioning Transport Provider then passes this value object to the target system.

Suppose the operating environment of your organization contains two target systems, `TS1` and `TS2`. `TS1` offers a Web-based interface for accepting provisioning request data. `TS2` provides APIs for enabling provisioning data to be written to the identity store. Both target systems support the same data format. If you want to perform provisioning operations on both target systems, then you must create one generic technology connector for each target system. For each generic technology connector, you must create a Provisioning Transport Provider. However, instead of creating a Provisioning Format Provider for each generic technology connector, you can create and reuse a single Provisioning Format Provider.

If `TS1` and `TS2` supported the same data transport mechanism but different data formats, then you can reuse the Provisioning Transport Provider and create different Provisioning Format Providers.

If you want to reuse the Provisioning Transport Provider, then you must ensure that the implementation of the `TargetOperation` value object does not contain code that is specific to the function performed by the Provisioning Format Provider. If you want to reuse the Provisioning Format Provider, then you must ensure that the implementation of the `TargetOperation` value object does not contain code that is specific to the function performed by the Provisioning Transport Provider.

Reusing the Predefined Provisioning Providers

If the target system is a Web service, then you can use the Web Services Provisioning Transport Provider along with any custom Provisioning Format Provider that you create. This is illustrated by the following example:

As mentioned earlier in this guide, the SPML Provisioning Format Provider supports only a subset of the provisioning operations that are described in the SPML specification. You can develop a custom Provisioning Format Provider that supports all the SPML provisioning operations. If the target system is a Web service, then you can use the Web Services Provisioning Transport Provider to carry SPML requests from your custom Provisioning Format Provider to the target system.

Similarly, you can use the SPML Provisioning Format Provider along with a custom Provisioning Transport Provider to send SPML requests to an SPML-based target system.

The following is the implementation of the `TargetOperation` value object that is created by the SPML Provisioning Format provider and used as an input for the Web Services Provisioning Transport Provider:

```
com.thortech.xl.gc.impl.prov.WSTransportTargetOperation
```

See the Javadocs for information about this class.

If you want to reuse the SPML Provisioning Format Provider, then you must create a custom Transport Provider that can accept an instance of this class as input and call the relevant `set` method. Similarly, if you want to reuse the Web Services Provisioning Transport Provider, then you must create a custom Provisioning Format Provider that can create an instance of this class and call the relevant `get` method.

22

Creating Generic Technology Connectors

The procedure to create a generic technology connector is composed of the following steps:

- Determining Provider Requirements
- Selecting the Providers to Be Included in the Generic Technology Connector
- Addressing the Prerequisites for Creating the Generic Technology Connector
- Using the Administrative and User Console to Create the Generic Technology Connector
- Configuring Reconciliation
- Configuring Provisioning
- Enabling Logging for the Generic Technology Connector

22.1 Determining Provider Requirements

As mentioned earlier in this guide, the following providers can be used as the building blocks of the generic technology connectors you create:

- Reconciliation Transport Provider
- Reconciliation Format Provider
- Provisioning Transport Provider
- Provisioning Format Provider
- Transformation Provider
- Validation Provider

See the "Functional Architecture of Generic Technology Connectors" section on page 19-2 for the definitions of these providers. Then, based on your knowledge of the data formats and data transport mechanisms supported by the target system, identify the providers that must be included in the generic technology connector that you create. If the target system supports multiple data formats and data transport mechanisms, then you must select a single combination of the transport and format providers discussed in the first chapter. You cannot include, for example, multiple Reconciliation Format Providers in a single generic technology connector.

See Also: Determining Provider Requirements on page 21-8

22.2 Selecting the Providers to Be Included in the Generic Technology Connector

Identify the predefined providers that can be used to meet your provider requirements. See Chapter 20 for information about the predefined providers.

If all your provider requirements are addressed by the predefined providers, then you need not create custom providers. You must create custom providers to address only the requirements that are not addressed by the predefined providers. See Chapter 21 for information about creating custom providers.

22.3 Addressing the Prerequisites for Creating the Generic Technology Connector

You must address the following prerequisites:

- If you are creating the generic technology connector on a production server, then enable the cache for the following cache categories:
  - `GenericConnector`
  - `GenericConnectorProviders`

  See "Optimal Cache Configuration for a Production Environment" in *Oracle Identity Manager Best Practices Guide* for more information.
- Testing connectivity between the target system server and the Oracle Identity Manager server

  You must take steps to ensure that connectivity can be established between the target system server and the Oracle Identity Manager server. For example, in a LINUX environment, you must enter the fully qualified host name of the Oracle Identity Manager server in the `/etc/hosts` file on the target system server.
- Creating the user account to be used for creating the generic technology connector

  All users belonging to the `SYSTEM ADMINISTRATORS` group of Oracle Identity Manager can create generic technology connectors. Alternatively, members of a group to which you assign the required menu items and permissions can create generic technology connectors.

  > **See Also:** Chapter 10, "Creating and Managing User Groups" for information about creating groups and assigning menu items and permissions to them

  The required menu items are as follows:
  - Create Generic Technology Connector menu item
  - Manage Generic Technology Connector menu item

  The required permissions are as follows:
  - Form Designer (Allow Insert, Write Access, Delete Access)
  - Structure Utility.Additional Column (Allow Insert, Write Access, Delete Access)
  - Meta-Table Hierarchy (Allow Insert, Write Access, Delete Access)

If these permissions are not correctly assigned to the group, then an error is thrown when the user clicks the Create button on the final Administrative and User Console page for creating generic technology connectors.

22.4 Using the Administrative and User Console to Create the Generic Technology Connector

To navigate to the first Administrative and User Console page for creating a generic technology connector, open the Administrative and User Console, expand **Generic Technology Connector**, and then click **Create**.

From this point onward, page-wise instructions are provided in the following sections:

- Step 1: Provide Basic Information Page
- Step 2: Specify Parameter Values Page
- Step 3: Modify Connector Configuration Page
- Step 4: Verify Connector Form Names Page
- Step 5: Verify Connector Information Page

22.4.1 Step 1: Provide Basic Information Page

To provide basic information about the generic technology connector that you want to create, use this page as follows

1. In the **Name** field, specify a name for the generic technology connector.

   The following are guidelines related to selecting a name for the generic technology connector:

   - The name must not be the same as that of any other connector (predefined connector or generic technology connector) on this Oracle Identity Manager installation.
   - The name must not be the same as that of any other connector object (such as resource objects, IT resources, and process forms) on this Oracle Identity Manager installation.

     Note: An error message is displayed if you specify a name that is the same as the name of an existing connector. However, an error message is *not* displayed if you specify a name that is the same as the name of an existing connector object. Therefore, you must ensure that the name you want to specify is not the same as the name of any existing connector object.

     See Chapter 28 for more information about connector objects that are automatically created as part of the generic technology connector creation process.

   - The name must not contain non-ASCII characters, because Oracle Identity Manager does not support non-ASCII characters in connector names. However, you can include the underscore character (_) in the name.

See Also: The "Names of Generic Technology Connectors and Connector Objects" section on page 26-1 of the "Known Issues" chapter for information about limitations related to the names of generic technology connectors.

2. If you want to use the generic technology connector for reconciliation, select **Reconciliation** and then perform the following steps:
   - From the **Transport Provider** list, select the Reconciliation Transport Provider that you want to use for this connector. This list displays the predefined Reconciliation Transport Providers and the Reconciliation Transport Providers that you create.
   - From the **Format Provider** list, select the Reconciliation Format Provider that you want to use for this connector. This list displays the predefined Reconciliation Format Providers and the Reconciliation Format Providers that you create.

     Note: If you select the Shared Drive Reconciliation Transport Provider, then you must also select the CSV Reconciliation Format Provider because all the parameters of this provider are bundled with the parameters of the Shared Drive Reconciliation Transport Provider.

   - If you want to use the connector to perform trusted source reconciliation with the target system, then select **Trusted Source Reconciliation**.

     Note: If you select the Trusted Source Reconciliation check box, then the Provisioning region of the page is disabled. This is because you cannot provision to a target system that you designate as a trusted source. You can only reconcile data from a trusted source.

3. If you want to use the generic technology connector for provisioning, select **Provisioning** and then perform the following steps:

   Note: You can select only Reconciliation, only Provisioning, or both Reconciliation and Provisioning.

   - From the **Transport Provider** list, select the Provisioning Transport Provider that you want to use for this connector. This list displays the predefined Provisioning Transport Providers and the Provisioning Transport Providers that you create.

     If you select the Web Services Provisioning Transport Provider and if Secure Sockets Layer (SSL) is enabled for the target Web service, then you must perform the procedure described in the "Configuring SSL Communication Between Oracle Identity Manager and the Target System Web Service" section on page 20-13.
   - From the **Format Provider** list, select the Provisioning Format Provider that you want to use for this connector. This list displays the predefined Provisioning Format Providers and the Provisioning Format Providers that you create.

If you select the SPML Provisioning Format Provider, then you must also select the Web Services Provisioning Transport Provider because the parameters of this provider are related to the parameters of the Web Services Provisioning Transport Provider.

4. Click **Continue**.

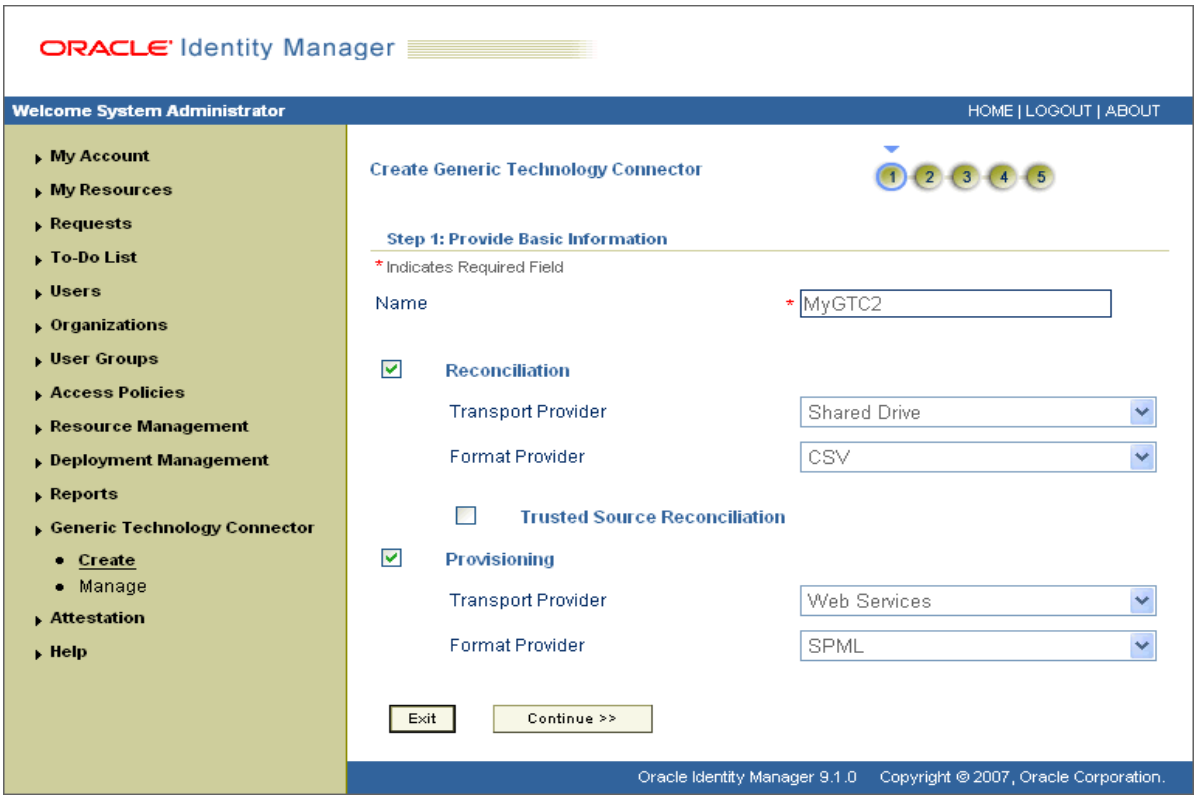
Table 22–1 lists sample entries for the GUI elements on the Step 1: Provide Basic Information page.

Table 22–1 Sample Entries for the Step 1: Provide Basic Information Page

Label on the Step 1: Provide Basic Information Page	Sample Value or Action	Reference Information
Name field	MyGTC2	NA
Reconciliation check box	Check box selected	NA
Transport Provider list	Shared Drive	Shared Drive Reconciliation Transport Provider on page 20-1
Format Provider list	CSV	CSV Reconciliation Format Provider on page 20-7
Provisioning check box	Check box selected	NA
Transport Provider list	Web Services	Web Services Provisioning Transport Provider on page 20-12
Format Provider list	SPML	SPML Provisioning Format Provider on page 20-7

Figure 22–1 shows the Step 1: Provide Basic Information page on which the entries described in Table 22–1 have been made.

Figure 22–1 Step 1: Provide Basic Information Page



22.4.2 Step 2: Specify Parameter Values Page

Use this page to specify values for the parameters of the providers that you select on the Step 1: Provide Basic Information page.

On this page, the provider parameters are divided into two categories:

- Run-time parameters

  See Also: Chapter 20, "Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager" for detailed information about the run-time parameters of predefined providers that you select on the Step 1: Provide Basic Information page

  Run-time parameters are input variables of the providers that you select on the previous page. A run-time parameter represents a value that is not constrained by the design of the provider. For example, the location of the directories containing the data files that you want to reconcile is a run-time parameter.

- Design parameters

  The parameters listed in this section are either design parameters of providers or reconciliation-specific parameters that are common to all generic technology connectors. A design parameter represents a value or set of values that is defined as part of the provider design.

  See Also: Chapter 20, "Predefined Generic Technology Connector Providers Shipped with Oracle Identity Manager" for detailed information about the design parameters of predefined providers that you select on the Step 1: Provide Basic Information page

For example:

The format of data files that can be parsed by a Format Provider is a design parameter for that provider. While designing the provider, you define the set of formats the provider can parse. On the Step 2: Specify Parameter Values page, you specify the particular format (from the set of supported formats) that an instance of the Format Provider must parse.

The following are reconciliation-specific design parameters:

Note: If you do not select the Reconciliation option on the previous page, then these reconciliation-specific design parameters are not displayed on this page.

– **Batch Size**

Use this parameter to specify a batch size for the reconciliation run. By using this parameter, you can break into batches the total number of records that the reconciliation engine fetches from the target system during each reconciliation run.

The default value of this parameter is `All`.

– **Stop Reconciliation Threshold**

During reconciliation, data from the Reconciliation Format Provider is accepted as input by the Validation Provider. Some of the reconciliation data records may not clear the validation checks. You can use the Stop Reconciliation Threshold parameter to automatically stop reconciliation if the percentage of records that fail the validation checks to the total number of reconciliation records processed exceeds the specified value.

The following example illustrates how this parameter works:

Suppose you specify 20 as the value of the Stop Reconciliation Threshold parameter. This means that you want reconciliation to stop if the percentage of failed records to the total number of records processed becomes equal to or greater than 20. Suppose the second and eighth records fail the validation checks. At this stage, the number of failed records is 2 and the total number of records processed is 8. The percentage of failed records is 25, which is greater than the specified threshold of 20. Therefore, reconciliation is stopped after the eighth record is processed.

Note:

- The Stop Reconciliation Threshold parameter is used during reconciliation only if you select Validation Providers on the Step 3: Modify Connector Configuration page.
- If reconciliation is stopped because the actual percentage of failed records exceeds the specified percentage, then the records that have already been reconciled into Oracle Identity Manager are not removed.

The default value of this parameter is `None`. This default value specifies that during a reconciliation run, you want all the target system records to be processed, regardless of the number of records that fail the checks.

– **Stop Threshold Minimum Records**

If you use the Stop Reconciliation Threshold parameter, then there may be a problem if invalid records are encountered right at the beginning of the reconciliation run. For example, suppose you specify 40 as the value of the Stop Reconciliation Threshold parameter. When reconciliation starts, suppose the first record fails the validation checks. At this stage, the percentage of failed records to total records processed is 100. Therefore, reconciliation would stop immediately after the first record is processed.

To avoid such situations, you can use the Stop Threshold Minimum Records parameter in conjunction with the Stop Reconciliation Threshold parameter. The Stop Threshold Minimum Records parameter specifies the number of records that must be processed by the Validation Provider before the Stop Reconciliation Threshold validation is enabled.

The following example illustrates how this parameter works:

Suppose you specify the following values:

Stop Reconciliation Threshold: 20

Stop Threshold Minimum Records: 80

With these values, from the eighty-first record onward, the Stop Reconciliation Threshold validation is enabled. In other words, after the eightieth record is processed, if any record fails the validation check, then the reconciliation engine calculates the percentage of failed records to total records processed.

The default value of this parameter is `None`.

Note:

- The Stop Threshold Minimum Records parameter is used during reconciliation only if you select Validation Providers on the Step 3: Modify Connector Configuration page.
- You must specify a value for the Stop Threshold Minimum Records parameter if you specify a value for the Stop Reconciliation Threshold parameter.

– **Reconciliation Type**

Use this parameter to specify whether you want the reconciliation engine to perform incremental or full reconciliation.

Note: The outcome of both full and incremental reconciliation is the same: target system records that are created or updated after the last reconciliation run are reconciled into Oracle Identity Manager.

In incremental reconciliation, only target system records that are newly added or modified after the last reconciliation run are brought to Oracle Identity Manager. Reconciliation events are created for each of these records.

In full reconciliation, all target system records are brought to Oracle Identity Manager. The optimized reconciliation feature identifies and ignores records that have already been reconciled. Reconciliation events are created for the remaining records.

You must select incremental reconciliation if either one of the following conditions is true:

* The target system time stamps or uniquely marks (in some way) files or individual data records that it generates, and the Reconciliation Transport Provider can recognize records that have been time stamped or marked by the target system.

  For example:

  Suppose the target system can time stamp the creation of or modifications to user data records. If you can create a custom Reconciliation Transport Provider that can read this time-stamp information, then only new or modified data records will be transported to Oracle Identity Manager during reconciliation.

* The target system provides only data records that are newly added or modified after the last reconciliation run.

If *neither* of these conditions is true, then you must select full reconciliation.

– **Reconcile Deletion of Multivalued Attribute Data**

Use this parameter to specify whether or not you want to reconcile into Oracle Identity Manager the deletion of multivalued attribute data (child data) on the target system.

The following example explains how this design parameter works:

There is an account for user `John Doe` on the target system. This user is a member of two user groups, `CREATE USERS` and `REVIEW PERMISSIONS`, on the target system. This user account (along with the group membership information) also exists on Oracle Identity Manager.

On the target system, suppose this user is removed from the `REVIEW PERMISSIONS` group. During the next reconciliation run, the action that will be taken in Oracle Identity Manager depends on whether or not you select the **Reconcile Deletion of Multivalued Attribute Data** check box:

* If you select the check box, then information about this user being a member of the `REVIEW PERMISSIONS` group on the target system is removed from the Oracle Identity Manager database. All other changes made to this user account on the target system are also reconciled.

* If you do not select the check box, then information about this user being a member of the `REVIEW PERMISSIONS` group on the target system is *not* removed from the Oracle Identity Manager database. However, all other changes made to this user account on the target system are reconciled.

– **Source Date Format**

Use this parameter to specify the format in which date values are stored in the target system.

The format that you specify is used to validate date values fetched during reconciliation and to convert the date values to the format used internally by Oracle Identity Manager.

The Validate Date Format Provider is one of the predefined Validation Providers. During a reconciliation run, the Validate Date Format Provider uses the source date format to validate date values fetched from the target system. Only date values that match the source date format are converted to the date format used by Oracle Identity Manager and then reconciled. This format

validation and conversion applies to all date fields (for example, Date of Birth and Hire Date) of the target system.

See Also: The "Validation Providers" section on page 20-22

For information about the date formats that you can specify, see the following page on the Sun Java Web site:

`http://java.sun.com/docs/books/tutorial/i18n/format/simpleDateFormat.html`

Note: If you want the source date format to be used in date validation, while performing the procedure described in the "Adding or Editing Fields in Data Sets" section on page 22-21, you must:

- Map date fields of the Source data sets to date fields of the Reconciliation Staging data sets.
- Edit each date field of the Reconciliation Staging data sets and set its data type to the Date data type.

The default value of the Source Date Format parameter is the date format specified as the value of the `XL.DefaultDateFormat` system property. If you do not specify a value for the Source Date Format parameter, then the default date format is used for date validation during reconciliation.

See Also: The "Rule Elements, Variables, Data Types, and System Properties" section in *Oracle Identity Manager Reference* for information about the system properties of Oracle Identity Manager

The following example illustrates how the Source Date Format parameter is used:

Suppose the following are date values in the target system:

- Date 1: `05/04/2007 06:25:44 PM`
- Date 2: `05/06/2007 07:31:44 PM`
- Date 3: `Thu, Apr 9, '98`
- Date 4: `07/03/2008 02:15:55 PM`

Scenario 1:

While creating the connector, you had entered the following as the value of the Source Date Format parameter:

`MM/dd/yyyy hh:mm:ss a`

During a reconciliation run, the record containing the Date 3 value is not reconciled because it does not conform to the specified source date format.

Scenario 2:

While creating the connector, you had not entered a value for the Source Date Format parameter. Therefore, during a reconciliation run, all four records are validated against the date format specified as the value of the `XL.DefaultDateFormat` system property.

The following is a provisioning-specific design parameter:

Note: If you do not select the Provisioning option on the previous page, then this provisioning-specific design parameter is not displayed.

- **Target Date Format**

  Use this parameter to specify the format in which you want to send date values to the target system during provisioning operations.

  During a provisioning operation, date values are converted to the format that you specify as the value of the Target Date Format parameter. This format conversion applies to all date fields (for example, Date of Birth and Hire Date) that are used in the provisioning operation.

  For information about the date formats that you can specify, see the following page on the Sun Java Web site:

  http://java.sun.com/docs/books/tutorial/i18n/format/simpleDateFormat.html

  If you do not specify a date format, then the following date format is used as the default value of this parameter:

  ```
  yyyy/MM/dd hh:mm:ss z
  ```

  The following example illustrates how the Target Date Format parameter is used:

  During a provisioning operation, any date value that you enter will be in the `yyyy/MM/dd hh:mm:ss z` format.

  Scenario 1:

  While creating the connector, you had entered the following as the value of the Target Date Format parameter:

  ```
  yyyy.MM.dd G 'at' hh:mm:ss z
  ```

  During a provisioning operation, an Oracle Identity Manager date value (for example, 2007/05/04 06:25:44 IST) will be converted into the target date format (for example, 2007.05.04 AD at 06:25:44 IST) and then sent to the target system.

  Scenario 2:

  While creating the connector, you had not entered a value for the Target Date Format parameter. During a provisioning operation, date values are sent to the target system in the (default) `yyyy/MM/dd hh:mm:ss z` format.

After you specify values for the run-time and design parameters, click **Continue**.

Note: If any value that you provide on this page is not correct, then an error message is displayed at the top of the page after you click **Continue**. If this happens, then fix the parameter value and click **Continue** again.

Table 22–2 lists sample entries for the Step 2: Specify Parameter Values page. The GUI elements displayed on this page are based on the entries made on the Step 1: Provide Basic Information page.

Table 22–2 Sample Entries for the Step 2: Specify Parameter Values Page

Label on the Step 2: Specify Parameter Values Page	Sample Value or Action	Reference Information
Run-Time Parameters of the Shared Drive Reconciliation Transport Provider		Shared Drive Reconciliation Transport Provider on page 20-1
Staging Directory (Parent Identity Data) field	D:\gctestdata\commaDelimited\parent	NA
Staging Directory (Multivalued Identity Data) field	D:\gctestdata\commaDelimited\child	NA
Archiving Directory field	D:\gctestdata\commaDelimited\archive	NA
File Prefix field	file	NA
Specified Delimiter field	,	NA
Tab Delimiter check box	Check box not selected	NA
Fixed Column Width field		NA
Unique Attribute (Parent Data) field	UserIDTD	NA
Run-Time Parameter of the Web Services Provisioning Transport Provider		Web Services Provisioning Transport Provider on page 20-12
Web Service URL field	http://acme123:8080/spmlws/services/HttpSoap11	NA
Run-Time Parameters of the SPML Provisioning Format Provider		SPML Provisioning Format Provider on page 20-7
Target ID field	target	NA
User Name (authentication) field	xelsysadm	NA
User Password (authentication) field		NA
Design Parameters of the Shared Drive Reconciliation Transport Provider		Shared Drive Reconciliation Transport Provider on page 20-1
File Encoding field	Cp1251	NA
Design Parameters of the Web Services Provisioning Transport Provider		Web Services Provisioning Transport Provider on page 20-12
Web Service SOAP Action field	http://xmlns.oracle.com/OIM/provisioning//processRequest	NA
Design Parameters of the SPML Provisioning Format Provider		SPML Provisioning Format Provider on page 20-7
WSSE Configured for SPML Web Service? check box	Check box not selected	NA
Custom Authentication Credentials Namespace field	http://xmlns.oracle.com/OIM/provisioning	NA
Custom Authentication Header Element field	OIMUser	NA
Custom Element to Store User Name field	OIMUserId	NA
Custom Element to Store Password field	OIMUserPassword	NA
SPML Web Service Binding Style (DOCUMENT or RPC) field	RPC	NA

Table 22–2 (Cont.) Sample Entries for the Step 2: Specify Parameter Values Page

Label on the Step 2: Specify Parameter Values Page	Sample Value or Action	Reference Information
SPML Web Service Complex Data Type field		NA
SPML Web Service Operation Name field	processRequest	NA
SPML Web Service Target Namespace field	http://xmlns.oracle.com/OIM/provisioning	NA
SPML Web Service Soap Message Body Prefix field		NA
ID Attribute for Child Dataset Holding Group Membership Information field		NA
Generic Design Parameters		This section
Target Date Format field	yyyy-MM-dd hh:mm:ss.fffffffff	NA
Batch Size field	All	NA
Stop Reconciliation Threshold field	None	NA
Stop Threshold Minimum Records field	None	NA
Source Date Format field	yyyy/MM/dd hh:mm:ss z	NA
Reconcile Deletion of Multivalued Attribute Data check box	Check box selected	NA
Reconciliation Type list	Incremental	NA

Figure 22–2 shows the first section of the Step 2: Specify Parameter Values page on which the entries listed in Table 2 have been made.

Figure 22–2 First Section of the Step 2: Specify Parameter Values Page

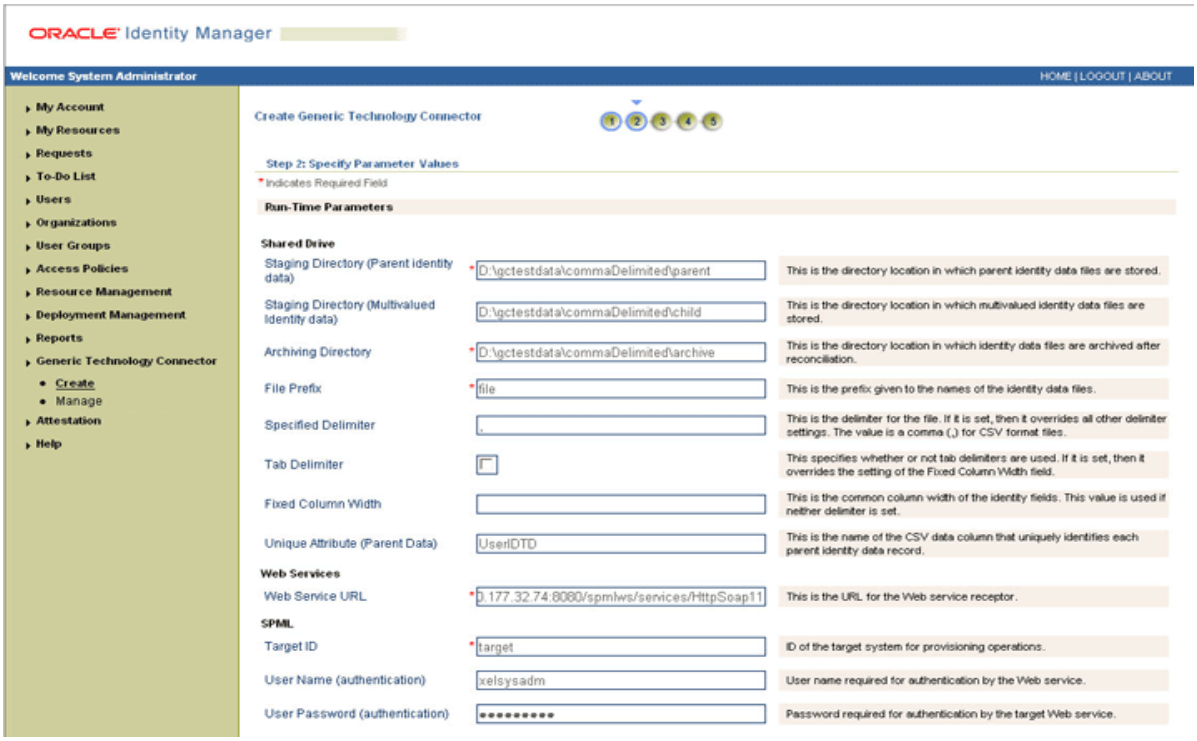


Figure 22–3 shows the second section of the Step 2: Specify Parameter Values page on which the entries listed in Table 2 have been made.

Figure 22–3 Second Section of the Step 2: Specify Parameter Values Page

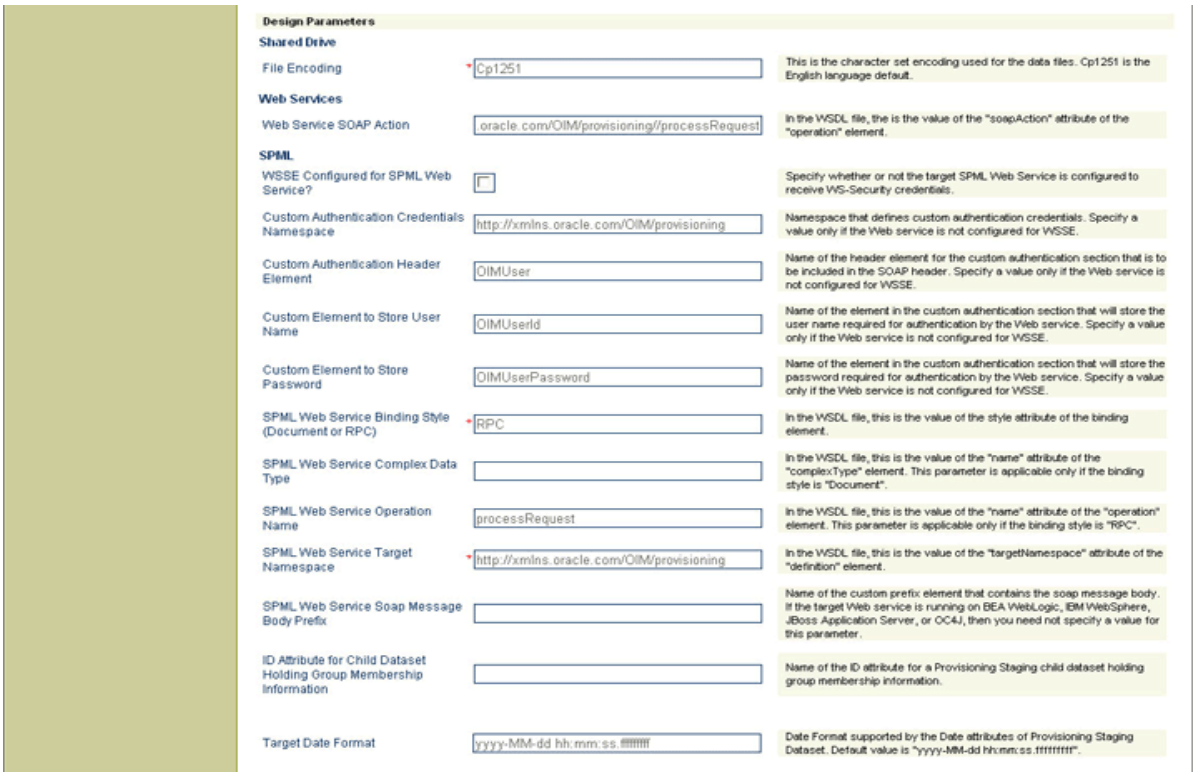
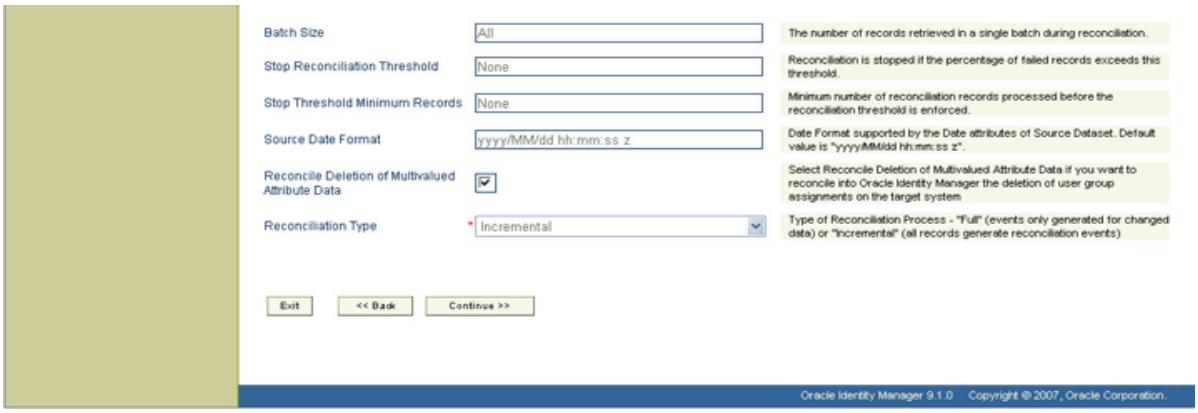


Figure 22–4 shows the third section of the Step 2: Specify Parameter Values page on which the entries listed in Table 2 have been made.

Figure 22–4 Third Section of the Step 2: Specify Parameter Values Page



22.4.3 Step 3: Modify Connector Configuration Page

Use this page to define data sets and mappings between the fields of the data sets. In other words, you use this page to specify the user data fields that you want to:

- Propagate from the target system to Oracle Identity Manager during reconciliation
- Propagate from Oracle Identity Manager to the target system during provisioning

In the generic technology connector context, the term **metadata** refers to the set of identity fields that constitute the user account information on the target system.

First Name, Last Name, Hire Date, and Department ID are examples of user data fields that constitute metadata. The values assigned to these fields constitute the user data on the target system. For example, the identity information of user John Doe on the target system can be composed of the following fields:

- First Name: John
- Last Name: Doe
- Hire Date: 04-December-2007
- Department ID: Sales
- . . .

After you click the **Continue** button on the Step 2: Specify Parameter Values page, the metadata displayed on the Step 3: Modify Connector Configuration page depends on the following factors:

- Input provided on the Step 1: Provide Basic Information and Step 2: Specify Parameter Values pages
- Availability of sample target system data

> **Note:** In the generic technology connector context, the term **metadata detection** refers to the process in which sample user data is read from the target system and the corresponding metadata (identity field names) is displayed on the Step 3: Modify Connector Configuration page.

Oracle Identity Manager performs the following steps while attempting to detect metadata:

1. The Reconciliation Transport Provider and Reconciliation Format Provider try to fetch and parse metadata from the target system.

   Together, the Shared Drive Reconciliation Transport Provider and CSV Reconciliation Format Provider can detect metadata from the target system. If you want custom providers to perform the same function, then you must ensure that:

   - The Java code for the Reconciliation Transport Provider contains an implementation of the `getMetadata()` method of the `ReconTransportProvider` interface.
   - The Java code for the Reconciliation Format Provider contains an implementation of the `parseMetadata()` method of the `ReconFormatProvider` interface.

     See Also: Chapter 21, "Creating Custom Providers for Generic Technology Connectors"

   If these providers successfully fetch and parse metadata from the target system, then Oracle Identity Manager uses information returned by them to display metadata and the following step is not performed.

2. If the Reconciliation Transport Provider and Reconciliation Format Provider cannot fetch and parse metadata from the target system, then the Provisioning Transport Provider and Provisioning Format Provider try to perform this function.

   The Web Services Provisioning Transport Provider and SPML Provisioning Format Provider cannot detect metadata from the target system. If you want custom providers to be able to detect metadata, then you must ensure that:

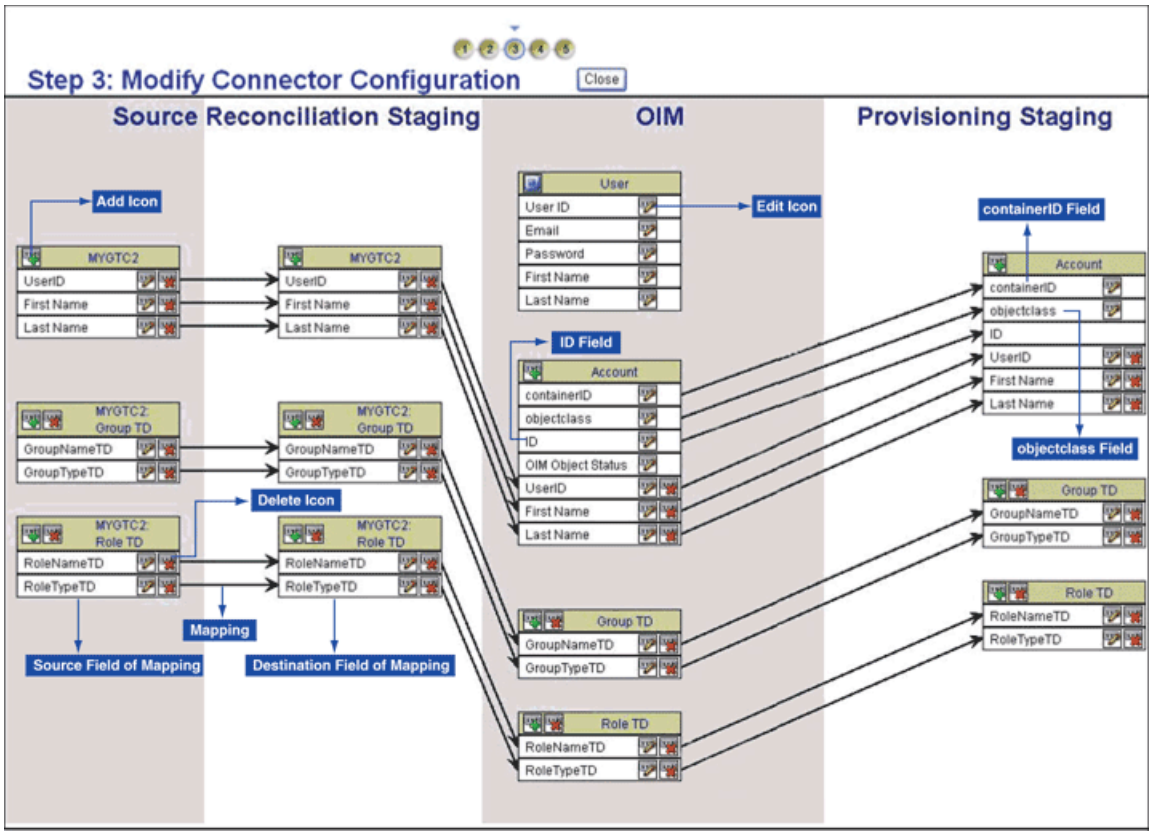
   - The Java code for the Provisioning Transport Provider contains an implementation of the `defineMetadata()` method of the `ProvisioningTransportProvider` interface.
   - The Java code for the Provisioning Format Provider contains an implementation of the `parseMetadata()` method of the `ProvisioningFormatProvider` interface.

     See Also: Chapter 21, "Creating Custom Providers for Generic Technology Connectors"

   If the Provisioning Transport Provider and Provisioning Format Provider successfully fetch and parse metadata from the target system, then Oracle Identity Manager uses information returned by these providers to display metadata. If these providers are not successful, then only the default fields defined for any of the provisioning-specific providers that you select are displayed. For example, the `ID` field of the OIM - Account data set and the `objectClass` and `containerID` fields of the Provisioning Staging data set are displayed by default. These data sets and fields are discussed later in this guide.

Figure 22–5 shows the Step 3: Modify Connector Configuration page for the sample entries listed at the end of the "Step 1: Provide Basic Information Page" and "Step 2: Specify Parameter Values Page" sections.

Figure 22–5 Step 3: Modify Connector Configuration Page



- Data Sets
- Mappings

Data Sets

The data sets displayed on the Step 3: Modify Connector Configuration page are categorized as follows:

> **See Also:** The "Functional Architecture of Generic Technology Connectors" section on page 19-2

- Source

  The Source data sets are displayed only if you select the Reconciliation option on the first page, regardless of whether or not you select the Provisioning option.

- Reconciliation Staging

  The Reconciliation Staging data sets are displayed only if you select the Reconciliation option on the Step 1: Provide Basic Information page, regardless of whether or not you select the Provisioning option.

- OIM

  The OIM data sets are always displayed, regardless of the options you select on the Step 1: Provide Basic Information page. However, the OIM - Account data set and its child data sets are not displayed if you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page.

The fields displayed in the OIM - User data set are predefined for the OIM User. You can show or minimize the full list of OIM - User data set fields by clicking the arrow icon at the top of the data set. The following fields are displayed in the minimized state of the data set:

– User ID

– Email

– Password

– First Name

– Last Name

Note: If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information Page, then all the fields of the OIM - User data set are displayed and you cannot use the arrow icon to minimize the display.

These fields constitute the minimum set of OIM User fields for which values must be defined. You can designate some or all of the remaining OIM - User data set fields as mandatory OIM User fields for your Oracle Identity Manager installation. You do this by ensuring that these fields always hold values when the OIM User is created.

Note: Data set and field names that take up more than a certain amount of space are truncated and dots are displayed after the truncated part of the names. For example, the Deprovisioning Date field of the OIM - User data set is displayed as follows:

```
Deprovisioning Da..
```

To view the full name of a field, you can click the edit icon for that field or the field to which that field is mapped. In the pop-up window, the field name that you want to view is on either the first page or the second page, depending on the data set to which the field belongs.

You can add user-defined fields (UDFs) to the list of predefined OIM User fields by using the Design Console. These UDFs are displayed in the OIM - User data set on the Step 3: Modify Connector Configuration page.

Depending on the options that you select on the Step 1: Provide Basic Information page, some fields are displayed by default on the Step 3: Modify Connector Configuration page:

– `ID` field

  The `ID` field is displayed by default in the OIM - Account data set, regardless of whether or not you select the Reconciliation option or Provisioning option on the Step 1: Provide Basic Information page. When an account is created, this field is used to store the value that uniquely identifies the account in Oracle Identity Manager and in the target system. For a particular user, this unique field is used to direct other operations, such as modify, delete, enable, disable, and child data operations.

  Every target system would have a unique field for tracking the creation of and updates made to a user account. While creating a custom Provisioning

Transport Provider, you must ensure that the provider retrieves this unique field value from the target system at the end of a Create User operation. This value must then be used to populate the `ID` field of the OIM - Account data set.

During reconciliation, the value of the `ID` field must come from the corresponding unique field of the Reconciliation Staging data set. To set this up, you must create a mapping between the two fields. The procedure to create a mapping is discussed later in this section.

Caution: If you select both the Provisioning and Reconciliation options while creating a generic technology connector and if you do not create a mapping between the ID field and the unique field of the target system, then records that are linked through reconciliation cannot be used for provisioning operations (such as modify, delete, enable, disable, and child data operations). This is because the ID field is not populated in the linked records.

- `objectClass` field

  The `objectClass` field is displayed by default in the OIM - Account data set and Provisioning Staging data set only if you select the SPML Provisioning Format Provider on the Step 1: Provide Basic Information page.

- `containerID` field

  The `containerID` field is displayed by default in the OIM - Account data set and Provisioning Staging data set only if you select the SPML Provisioning Format Provider on the Step 1: Provide Basic Information page.

- Provisioning Staging

  The Provisioning Staging data sets are displayed only if you select the Provisioning option on the first page, regardless of whether or not you select the Reconciliation option.

The display of data sets on the Step 3: Modify Connector Configuration page depends on the input that you provide on the Step 1: Provide Basic Information page and Step 2: Specify Parameter Values page. The display of fields within the data sets depends on whether or not metadata detection has taken place.

Note: Metadata detection does not take place if any of the following conditions are true:

- Sample target system data (including metadata) is not available.
- The Transport and Format Providers that you select are not capable of detecting metadata from sample target system data.

This is illustrated by the following example:

Suppose you select only the Reconciliation option on the Step 1: Provide Basic Information page. In addition, metadata detection has not taken place. Under these conditions, the display of data sets and fields on the Step 3: Modify Connector Configuration page can be summarized as follows:

The following data sets are displayed:

- Source

- Reconciliation Staging
- OIM

The fields that constitute the data sets are *not* displayed.

In addition, if you had selected the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then the OIM - Account data set and its child data sets are not displayed.

In Table 22–3, Scenario 1 shows the outcome of this set of input conditions. The rest of the scenarios in this table describe the display of data sets and fields under the combination of input conditions listed in the first row and first column of the table.

Table 22–3 Display of Data Sets and Fields Under Various Input Conditions

	Only Reconciliation Option Selected	**Both Reconciliation and Provisioning Options Selected**	**Only Provisioning Option Selected**
Metadata detection has *not* taken place	**Scenario 1** The following data sets are displayed: ■ Source ■ Reconciliation Staging ■ OIM The fields that constitute the data sets are *not* displayed. If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then the OIM - Account data set and its child data sets are not displayed.	**Scenario 2** The following data sets are displayed: ■ Source ■ Reconciliation Staging ■ OIM ■ Provisioning Staging The fields that constitute the data sets are *not* displayed.	**Scenario 3** The following data sets are displayed: ■ OIM ■ Provisioning Staging The fields that constitute the data sets are *not* displayed.
Metadata detection has taken place	**Scenario 4** The following data sets are displayed: ■ Source ■ Reconciliation Staging ■ OIM The fields that constitute the data sets are displayed. If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then the OIM - Account data set and its child data sets are not displayed.	**Scenario 5** The following data sets are displayed: ■ Source ■ Reconciliation Staging ■ OIM ■ Provisioning Staging The fields that constitute the data sets are displayed.	**Scenario 6** The following data sets are displayed: ■ OIM ■ Provisioning Staging The fields that constitute the data sets are displayed.

See Also: The "Multilanguage Support" section on page 26-5 of the "Known Issues" chapter for information about limitations related to the display of non-ASCII characters on this page

Mappings

Each flow line displayed on the Step 3: Modify Connector Configuration page represents a mapping (link) between two fields of different data sets. A mapping serves one of the following purposes:

- Establishes a data flow path between fields of two data sets, for either provisioning or reconciliation

  A mapping of this type forms the basis for validations or transformations to be performed on data.

- Creates a basis for comparing (matching) field values of two data sets

  The following are examples of matching-only mappings:

  – Mappings created between fields of the Reconciliation Staging data set and the OIM - User data set form the basis of a reconciliation rule.

  – A mapping between the unique field of the Reconciliation Staging data set and the `ID` field of the OIM - Account data set helps identify the key field for reconciliation matching. Along with the ID field, other fields of the OIM - Account data set can be (matching-only) mapped to corresponding fields of the Reconciliation Staging data set to create a composite key field for reconciliation matching.

You can perform the following actions on the Step 3: Modify Connector Configuration page:

- Adding or Editing Fields in Data Sets
- Removing Fields from Data Sets
- Removing Mappings Between Fields
- Removing Child Data Sets

22.4.3.1 Adding or Editing Fields in Data Sets

Identity fields detected through metadata detection are displayed on the Step 3: Modify Connector Configuration page. You can modify these fields and the mappings between them. If required, you can also add new fields on this page and create mappings between them.

The following is a summary of the actions that you can perform while adding or editing fields on the Step 3: Modify Connector Configuration page:

> **Note:** These actions are described in detail in the procedure that follows this list. The procedure also describes the conditions that must be fulfilled before you can perform some of these actions.

- Default attributes (such as the data type and length) are assigned to the fields displayed through metadata detection. You must edit these fields to set the required attributes for them.

Note: Oracle Identity Manager can recognize date values fetched during reconciliation only if you set the Date data type for fields of the Reconciliation Staging data sets. In addition, if you have specified a value for the Source Date Format parameter on the Step 2: Specify Parameter Values page, then you must map date fields of the Source data sets to the corresponding date fields of the Reconciliation Staging data sets.

The Source Date Format parameter is described in the "Step 2: Specify Parameter Values Page" section on page 22-6.

- You can create transformation mappings between fields by using a Transformation Provider. While performing this action, you can use the predefined Concatenation Transformation Provider or Translation Transformation Provider, or a custom Transformation Provider that you have created.
- You can create matching-only mappings between fields of the Reconciliation Staging data set and OIM data sets. Matching-only mappings that you create between the Reconciliation Staging data set and the OIM - User data set forms the reconciliation rule. Matching-only mappings that you create between the Reconciliation Staging data set and the OIM - Account data set identifies the key field for reconciliation matching.
- You can add a child data set to an existing data set.
- You can encrypt the value of a field, both in the process form and in the database.
- You can designate a field as a lookup field and select an input source for the field. The input source can be a lookup definition or a combination of columns from Oracle Identity Manager database tables.
- You can configure user account status reconciliation.

  If you want to configure user account status reconciliation, then refer to the "Configuring Account Status Reconciliation" section on page 20-19.

To add or edit a field in a data set:

Note: The display of the GUI elements and pages described in the following steps depends on the data set in which you are adding or editing a field. For example, the Required and Encrypted check boxes are not displayed if you are adding or editing a field in a Source data set.

1. Depending on whether you want to add or edit a field, click the Add icon for the data set or the edit icon for the field.
2. On the Step 1: Field Information page, specify values for the following GUI elements:

   See Also: The "Step 3: Modify Connector Configuration Page" section on page 24-3 for information about validations applied to the names of fields

   - **Field Name**: If you are adding a field, then specify a name for the field. The field name that you specify must contain only ASCII characters, because non-ASCII characters are not allowed.

- **Mapping Action**: Select the type of mapping that you want to create with this field as the destination field of the mapping. You can select one of the following mapping actions:
  - Select **Create Mapping Without Transformation** if you only want to create a one-to-one mapping between a source (input) field and the field that you are adding or editing, and you do not want to use a Transformation Provider.
  - Select the **Remove Mapping** option if you are editing the field and you want to remove the mapping for which this field is the destination field. The procedure to remove a mapping is covered in detail in the "Removing Mappings Between Fields" section on page 22-29.
  - The transformation mapping options displayed in the Mapping Action list are based on the predefined Transformation Providers and the custom Transformation Providers that you create. The following menu options correspond to the predefined Transformation Providers:

    *** Create Mapping With Concatenation**

    *** Create Mapping With Translation**

    See Also: The "Transformation Providers" section on page 20-16 for information about these predefined Transformation Providers

    Apply the following guidelines while selecting a transformation mapping:

    * You can create transformation mappings only between fields of the following data sets:

      - Source and Reconciliation Staging

      - OIM and Provisioning Staging

      This means that, for example, you cannot create transformation mappings between a field in a Reconciliation Staging data set and a field in an OIM data set.

      You cannot create a 1-to-2 mapping with the following source and destination fields:

      Source field: Unique field of the Reconciliation Staging data

      Destination fields: `User ID` field of the OIM - User data set and `ID` field of the OIM - Account data set

      This mapping is not supported. Instead, you must create a one-to-one mapping between the unique field of the Reconciliation Staging data and either the `User ID` field (of the OIM - User data set) or the `ID` field (of the OIM - Account data set).

    * Ensure that all the fields of Provisioning Staging data sets are mapped to corresponding fields of OIM - User and OIM - Account data sets.

    * When you create a mapping that has any field of the OIM - User data set as the source or destination field, the display of the OIM - User data set fields list is frozen in the position it was in (expanded or minimized) when the mapping was created. To unfreeze the display of the OIM - User data set so that you are able to use the arrow icon, you must remove all mappings that have any OIM - User data set field as the source or destination field.

* A literal field can be used as one of the input fields of a transformation field. If you select the Literal option, then you must enter a value in the field. You must not leave the field blank after selecting it.

See "Step 3: Modify Connector Configuration Page" on page 26-2 for information about limitations related to creating transformation mappings.

- **Matching Only**: Select this check box if the field is to be used as the destination field of a matching-only mapping. As mentioned earlier in this document, you can create the following types of matching-only mappings:

Note: You must create matching-only mappings for both parent and child data sets.

  - To create the reconciliation rule, you create matching-only mappings between fields of the Reconciliation Staging data set and the OIM - User data set. Each mapping represents a reconciliation rule element. If there are child data sets, then you must ensure that the names of fields of the Reconciliation Staging data set that are input fields for the matching-only mappings are not used in any of the Reconciliation Staging child data sets.
  - To specify the key field for reconciliation matching, you create a matching-only mapping between the unique field of the Reconciliation Staging data set and the ID field of the OIM - Account data set. Along with the ID field, other fields of the OIM - Account data set can be (matching-only) mapped to corresponding fields of the Reconciliation Staging data set to create a composite key field for reconciliation matching.

Caution: If the name of a Reconciliation Staging field used in a matching-only mapping were to be reused as the name of a field in a Reconciliation Staging child data set, then matching would not take place during a reconciliation run.

This known issue is explained in the "Step 3: Modify Connector Configuration Page" section on page 26-2.

- **Create End-to-End Mapping**: If you are adding a field, then select this check box if you want the same field to be added in all the data sets that are displayed to the right of the data set in which you are adding the field.
- **Multi-Valued Field**: Select this check box if you want to add a child data set. If you select this check box, then the name that you specify in the Field Name field is used as the name of the child data set.

Note: If you select the Trusted Source Reconciliation check box on the Step 1: Provide Basic Information page, then this check box (in selected or deselected state) is ignored. This is because the reconciliation of multivalued (child) data is not supported in trusted source reconciliation.

- **Data Type**: Select the data type of the field.

After metadata detection, the String data type is applied by default to all the fields of the Reconciliation Staging and OIM - Account data sets. Where required, you must use the Data Type list to specify the actual data type of each field.

- **Length**: Specify the character length of the field.
- **Required**: Select this check box if you want to ensure that the field always contains a value.
- **Encrypted**: Select this check box if the value of the field must be stored in encrypted form in the Oracle Identity Manager database.
- **Password Field**: Select this check box if the value of the field must be encrypted on the process form. Values of fields for which this check box is selected are displayed as asterisks (*) on the process forms.

Note: If you select the Encrypted and Password Field check boxes, then see "Password-Like Fields" on page 24-4 for information about guidelines that you must follow.

- **Lookup Field**: Select this check box if you want to make the field a lookup field.

3. Click **Continue**.
4. If you select the **Lookup Field** check box on the Step 1: Field Information page, then the Step 2: Lookup Properties page is displayed. On this page, you can select and specify values for any combination of the lookup properties described in Table 22–4.

Table 22–4 Lookup Properties

Lookup Property	Value
Column Names	In the **Property Value** field, enter the name of the database column containing the values that must be displayed in the lookup window. If required, you can enter multiple database column names separated by commas. **Note:** If you select the Lookup Column Name property, then you must also select the Column Names property, which is described later in this table. After you enter a value in the **Property Value** field, click **Submit**. The following SQL query can be used to illustrate how the Column Names and Lookup Column Name properties are used: `SELECT USR_FIRST_NAME, USR_LOGIN, USR_LAST_NAME FROM USR` Suppose you set the following as the values of the two properties: - Column Names: `USR_FIRST_NAME, USR_LAST_NAME` - Lookup Column Name: `USR_LOGIN` When the user selects a particular `USR_FIRST_NAME, USR_LAST_NAME` combination from the lookup window, the corresponding `USR_LOGIN` value is stored in the database.
Column Captions	In the **Property Value** field, enter the name of the column heading that must be displayed in the lookup window. If multiple columns are going to be displayed in the lookup window, then enter multiple column captions separated by commas, for example, **Organization Name**, **Organization Status**. After you enter a value in the **Property Value** field, click **Submit**.

Table 22–4 (Cont.) Lookup Properties

Lookup Property	Value
Column Widths	In the **Property Value** field, enter the character width of the column that must be displayed in the lookup window. This must be the same as the maximum length of the underlying field or column from which data values are drawn to populate the lookup field. If the lookup window is going to display multiple columns, then enter multiple column widths separated by commas. After you enter a value in the **Property Value** field, click **Submit**.

Table 22–4 (Cont.) Lookup Properties

Lookup Property	Value
Lookup Query	To specify a value for the Lookup Query property: 1. In the **Property Value** field, enter the SQL query (without the `WHERE` clause) that must be run when a user double-clicks the lookup field to populate the data columns displayed in the lookup window. 2. Click **Submit**. 3. On the Step 2: Add Validation page, select values from the following lists to create a `WHERE` clause for the `SELECT` statement that you specify in Step 1: - Filter Column - Source - Field Name From the values that you select, the `WHERE` clause is created as follows: `WHERE Filter_Column=Source.Field_Name` 4. Click **Save**. To correctly display the data returned from a query, you must add a `lookupfield.header` property to the `xlWebAdmin_`*`locale`*`.properties` file. **See Also:** *Oracle Identity Manager Globalization Guide* for information about the `xlWebAdmin_`*`locale`*`.properties` file For example, consider the following SQL query: `SELECT usr_status FROM usr` To view the data returned from the query, you must add the following entry to the `xlWebAdmin_`*`locale`*`.properties` files: `lookupfield.header.users.status=User Status` If the `xlWebAdmin_locale.properties` file does not contain a `lookupfield.header` property for your specified query, then the Administrative and User Console displays a lookup window after you click the corresponding lookup icon. The syntax for a `lookupfield.header` property is as follows: `lookupfield.header.`*`column_code`*`=display value` The *`column_code`* portion of the entry must be lowercase and any spaces must be replaced by underscore characters (_). By default, the following entries for lookup field column headers are already available in the `xlWebAdmin_locale.properties` file: `lookupfield.header.lookup_definition.lookup_code_information .code_key=Value` `lookupfield.header.lookup_definition.lookup_code_information .decode=Description` `lookupfield.header.users.manager_login=User ID` `lookupfield.header.organizations.organization_name=Name` `lookupfield.header.it_resources.key=Key` `lookupfield.header.it_resources.name=Instance Name` `lookupfield.header.users.user_id=User ID` `lookupfield.header.users.last_name=Last Name` `lookupfield.header.users.first_name=First Name` `lookupfield.header.groups.group_name=Group Name` `lookupfield.header.objects.name=Resource Name` `lookupfield.header.access_policies.name=Access Policy Name`

Table 22–4 (Cont.) Lookup Properties

Lookup Property	Value
Lookup Code	In the **Property Value** field, enter the lookup definition code name. This code must generate all information pertaining to the lookup field, including lookup values and the text that is displayed with the lookup field when a lookup value is selected. The classification type of the lookup definition code must be of Lookup Type (that is, the Lookup Type option on the Lookup Definition form must be selected). To enter a lookup code, open the Lookup Definition form, query for the required code, and then copy the code into the Property Value field. After you enter a value in the **Property Value** field, click **Submit**. **Note:** The Lookup Code property can be used to replace the combination of the **Column Captions**, **Column Names**, **Column Widths**, **Lookup Column Name**, and **Lookup Query** properties. In addition, the information contained in the Lookup Code property supersedes any values set in these five lookup properties. If you want to implement lookup fields reconciliation, then create a scheduled task that populates the lookup code.
Lookup Column Name	In the **Property Value** field, enter the name of the database column containing the value that must be stored corresponding to the Column Names value selected by the user in the lookup window. If required, you can enter multiple database column names separated by commas. **Note:** If you select the Column Names property, then you must also select the Lookup Column Name property. See the "Lookup Column Name" row in this table for more information about how these two properties are used. After you enter a value in the **Property Value** field, click **Submit**.
Auto Complete	If you enter `True` in the **Property Value** field, then users can filter the values displayed in the lookup window by entering the first few characters of the value they want to select and then double-clicking the lookup field. The outcome of this action is that only lookup values that begin with the characters entered by the users are displayed in the lookup window. For example, for the State lookup field, a user can enter `New` in the field. When the user double-clicks the State lookup field, only states that begin with `New` (for example, New Hampshire, New Jersey, New Mexico, and New York) are displayed in the lookup window. If you do not want to let users filter the display of values in the lookup field, then enter `False` in the **Property Value** field. The default value of the **Auto Complete** property is `False`. After you enter a value in the **Property Value** field, click **Submit**.

If you want to edit the value of a property that is displayed in the table on the Step 2: Lookup Properties page, select the edit option for that property and then click **Edit**. If you want to remove a property that is displayed in the table, select the delete option for that property and then click **Delete**.

After you specify properties for the lookup field, click **Continue**.

5. If you select a transformation option from the Mapping Action list on the Step 1: Field Information page, then the Step 3: Mapping page is displayed. Use this page to define the transformation function that you want to perform on the input data to the field that you are adding. The steps to be performed depend on the Transformation Provider option (Concatenation, Translation, or custom Transformation Provider) that you select on the previous page:

   If you select a predefined Transformation Provider (Concatenation or Translation), then see "Transformation Providers" on page 20-16 for detailed information about the procedure to specify parameter values for the predefined Transformation

Provider. That section also provides detailed information about configuring user account status reconciliation.

You must use the Translation Transformation Provider if you want to configure the reconciliation of user account status information. This procedure is described in the "Translation Transformation Provider" section on page 20-17.

After you specify values for the transformation provider, click **Continue**.

6. If required, select a validation check for the field and then click **Add**. In other words, select the Validation Provider that you want to use.

   The validation options displayed in this list are based on the predefined Validation Providers and any custom Validation Providers that you create.

7. Click **Continue**, and then click **Close**.

8. If you do not want to perform any other action on the Step 3: Modify Connector Configuration page, then click the **Close** button that is displayed at the top of the page. You must perform the previous step before you click this Close button.

22.4.3.2 Removing Fields from Data Sets

To remove a field from a data set:

1. Click the Delete icon for that field.

2. If you do not want to perform any other action on the Step 3: Modify Connector Configuration page, then click the **Close** button that is displayed at the top of the page.

22.4.3.3 Removing Mappings Between Fields

To remove a mapping:

1. Click the edit icon for the destination field of the mapping that you want to remove.

   Note: If the destination field itself is the source field for another mapping, then that mapping is not removed.

2. On the Step 1: Field Information page, select **Remove Mapping** from the **Transformation** list.

3. Click **Continue**.

4. On the last page, click **Close**.

5. If you do not want to perform any other action on the Step 3: Modify Connector Configuration page, then click the **Close** button that is displayed at the top of the page.

22.4.3.4 Removing Child Data Sets

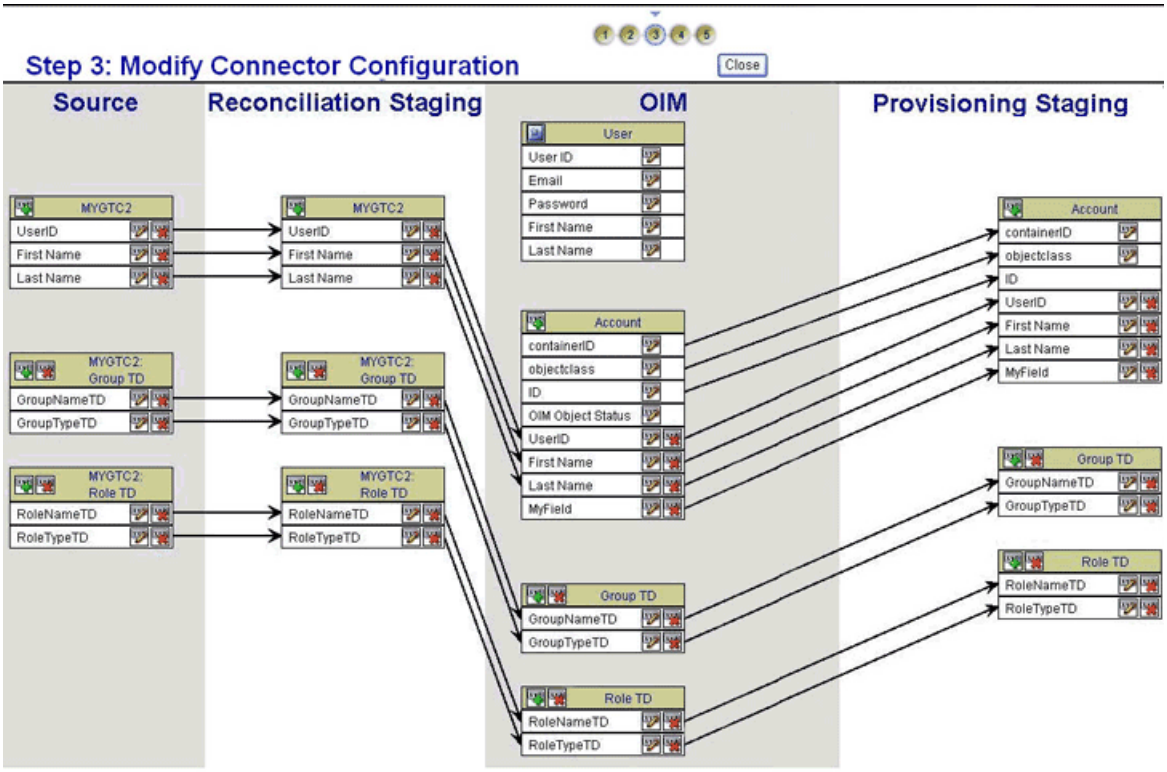
To remove a child data set:

1. Click the Delete icon for the data set.

2. If you do not want to perform any other action on the Step 3: Modify Connector Configuration page, then click the **Close** button that is displayed at the top of the page.

Figure 22–6 shows the Step 3: Specify Connector Configuration page after the `MyField` field was added to the OIM - Account and Provisioning Staging data sets.

Figure 22–6 Step 3: Modify Connector Configuration Page After Addition of a Field



22.4.4 Step 4: Verify Connector Form Names Page

Use this page to specify form names for the process forms corresponding to the OIM - Account data set and its child data sets.

> **Note:** If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then the OIM - Account data set and its child data sets are not created. Therefore, this page is not displayed if you select the Trusted Source Reconciliation option.

The generic technology connector framework automatically creates certain objects after you submit all the information required to create a generic technology connector. Parent and child process forms corresponding to the OIM - Account data sets are examples of objects that are automatically created. Each process form on a particular Oracle Identity Manager installation must have a unique name.

> **See Also:** Chapter 28, "Connector Objects Created by the Generic Technology Connector Framework"

On the Step 4: Verify Connector Form Names page, the generic technology connector framework displays default names for these process forms based on the names of the corresponding data sets. You must verify and, if required, change the names of these forms to ensure that they are unique for this installation of Oracle Identity Manager. While changing the name of a form, you must use only ASCII characters. An error

message is displayed if you specify non-unique form names or if any name contains non-ASCII characters.

> **Note:** You cannot revisit this page, so ensure that the form names that you specify meet all the requirements before you click Continue.

After you specify the form names, click **Continue**.

Instead of clicking Continue, you can click **Back** to return to the Step 2: Specify Parameter Values page. However, metadata detection does not take place if you make changes on this page and then click the Continue button. This is to ensure that any customization in the data set structure and mappings made during the first pass through this page does not get overwritten. You can manually add or edit fields and mappings on the Step 3: Modify Connector Configuration page.

Figure 22–7 shows the Step 4: Verify Connector Form Names page.

Figure 22–7 Step 4: Verify Connector Form Names Page

22.4.5 Step 5: Verify Connector Information Page

Use this page to review information that you have provided up to this point for creating generic technology connectors. The following is a page-wise explanation of the changes that are permitted on the earlier pages:

- Step 1: Provide Basic Information page

  You can use either the View link or Back button to reopen and view the information provided on the Step 1: Provide Basic Information page. You cannot

change the information displayed on this page, because any change in this information would amount to creating a new generic technology connector.

- Step 2: Specify Parameter Values page

  You can use either the Change link or Back button to reopen this page. You can change parameter values on this page. However, metadata detection does not take place when you submit the changed values. This is to ensure that any customization in the data set structure and mappings made during the first pass through this page does not get overwritten. You can manually add or edit fields and mappings on the Step 3: Modify Connector Configuration page.

- Step 3: Modify Connector Configuration page

  You can use the Change link to reopen this page and then add or edit fields and mappings.

- Step 4: Verify Connector Form Names page

  You cannot revisit this page.

After you verify all the information displayed on the Step 5: Verify Connector Information page, click **Create**.

At this stage, the generic technology connector framework creates all the standard connector objects on the basis of the information that you provide. The list of these objects includes the connector XML file, which is created and imported automatically into Oracle Identity Manager. Except for the form names, the names of the connector objects are in the *GTCname*_GTC format.

For example, if you specify DB_conn as the name of a generic technology connector that you create, then all (except the forms) the connector objects are named DB_CONN_GTC.

> **See Also:** Chapter 28, "Connector Objects Created by the Generic Technology Connector Framework"

At the end of the process, a message stating that the connector has been successfully created is displayed on the page.

Note: If the creation process fails, then objects that are created are not automatically deleted. This point is also mentioned in the "Connector Objects" section on page 26-8 of the "Known Issues" chapter.

See "Errors Encountered at the End of the Connector Creation Process" on page 25-1 for a listing of error messages related to the creation process.

Figure 22–8 shows the first section of the Step 5: Verify Connector Information page on which the entries listed at the end of the "Step 1: Provide Basic Information Page" and "Step 2: Specify Parameter Values Page" sections and the changes described at the end of the "Step 3: Modify Connector Configuration Page" section have been made.

Figure 22–8 First Section of the Step 5: Verify Connector Information Page

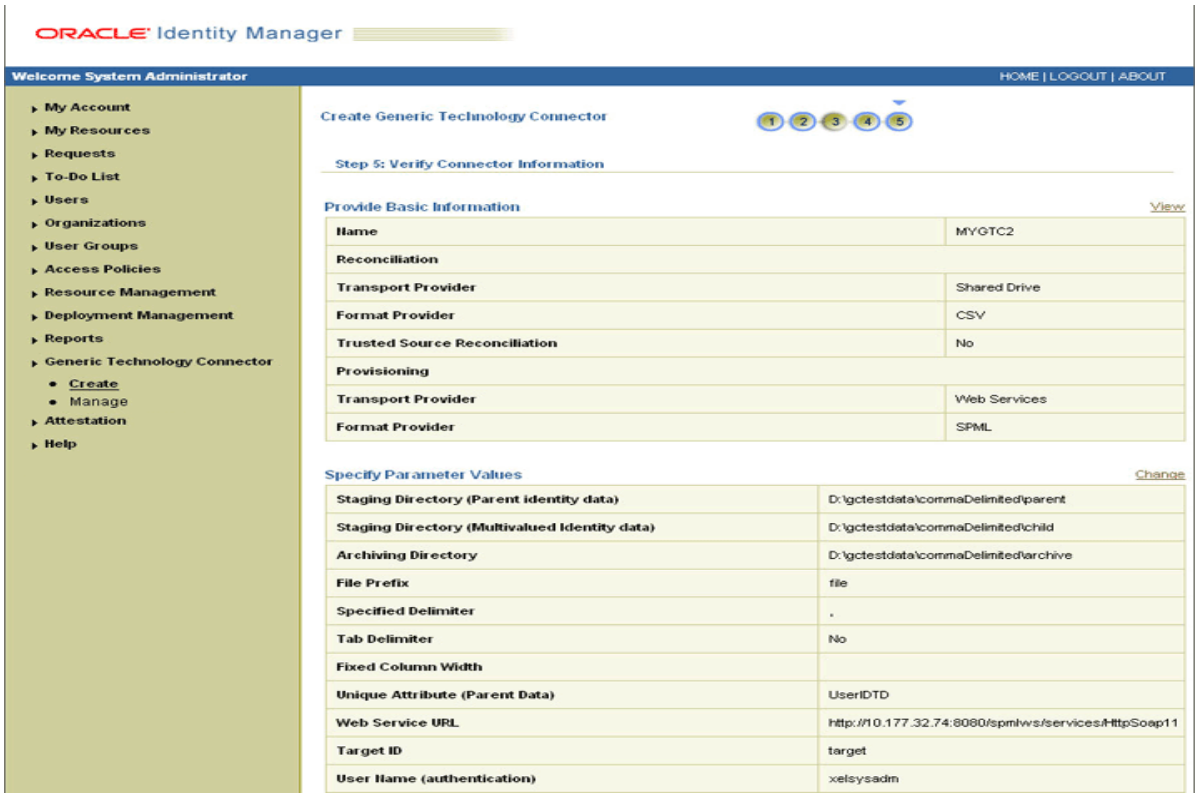
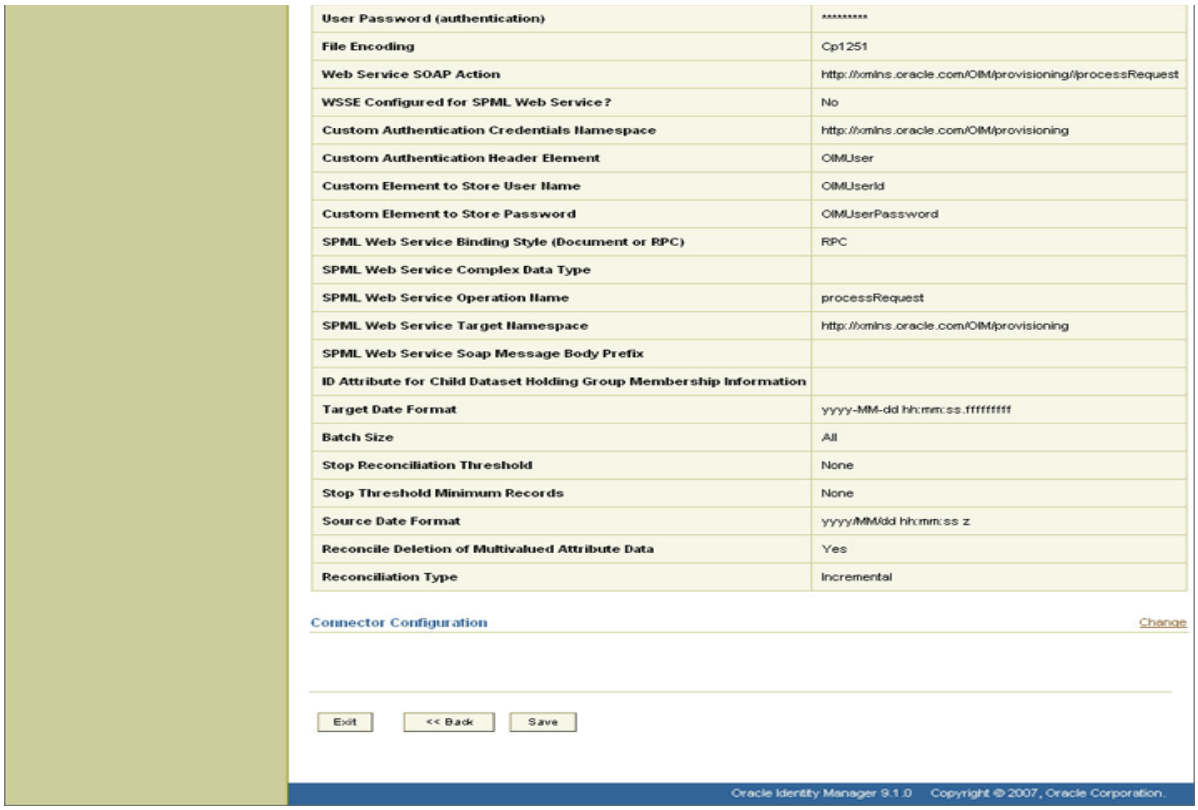


Figure 22–9 shows the second section of the Step 5: Verify Connector Information page on which the entries listed at the end of the "Step 1: Provide Basic Information Page" and "Step 2: Specify Parameter Values Page" sections and the changes described at the end of the "Step 3: Modify Connector Configuration Page" section have been made.

Figure 22–9 Second Section of the Step 5: Verify Connector Information Page



22.5 Configuring Reconciliation

Note: If you select only the Provisioning option on the Step 1: Provide Basic Information page, then you can skip this section because you need not configure reconciliation.

A reconciliation scheduled task is created automatically when you create the generic technology connector. To configure and run this scheduled task, follow the instructions in the "Modifying Scheduled Tasks" section on page 12-53.

Note: The name of the scheduled task is in the following format:

*GTC_Name*_GTC

For example, if the name of the generic technology connector is `WebConn`, then the name of the scheduled task is `WebConn_GTC`.

22.6 Configuring Provisioning

Note: If you select only the Reconciliation option on the Step 1: Provide Basic Information page, then you can skip this section because you need not configure provisioning.

A process definition is one of the objects that are automatically created when you create a generic technology connector. The name of the process definition is in the following format:

*GTC_name*_GTC

For example, if the name of the generic technology connector is WebConn, then the name of the process definition is WebConn_GTC.

The process tasks that constitute this process definition can be divided into two types:

- System-defined process tasks

  System-defined process tasks are included by default in all newly created process definitions.

- Provisioning-specific process tasks

  Provisioning-specific process tasks are included in the process definition of a generic technology connector only if you select the Provisioning option on the Step 1: Provide Basic Information page, regardless of whether or not you select the Reconciliation option.

The following are provisioning-specific process tasks:

- Create User
- Delete User
- Enable User
- Disable User
- Updated *Field_Name* (this task is created for each field of the OIM - Account data set, except the ID field)
- For mappings created between fields of the OIM - User data set and the Provisioning Staging data set, the following process tasks are created:
  - Change *User_data_set_field_name*
  - Edit *Provisioning_Staging_field_name*

  For example, suppose you create a mapping between the Last Name field of the OIM - User data set and the LName field of the Provisioning Staging data set. The following process tasks are automatically created along with the rest of the provisioning-specific process tasks:
  - Change Last Name
  - Edit LName

In addition, the following provisioning-specific process tasks are created for each child data set of the OIM - Account data set:

- Child Table *Child_Form_Name* row Inserted
- Child Table *Child_Form_Name* row Updated
- Child Table *Child_Form_Name* row Deleted

All provisioning-specific process tasks have the following default assignments:

- Target Type: Group User With Highest Priority
- Group: SYSTEM ADMINISTRATORS
- User: XELSYSADM

If required, you can modify these default assignments by following the instructions given in the "Modifying Process Tasks" section in *Oracle Identity Manager Design Console Guide*.

22.7 Enabling Logging for the Generic Technology Connector

Note: This is an optional step. Perform the procedure discussed in this section only if you want to enable logging for the generic technology connector.

Depending on the application server that you use, see the "Setting Log Levels" section in one of the following guides for information about the procedure that you must follow to enable logging:

- *Oracle Identity Manager Installation and Configuration Guide for Oracle WebLogic Server*
- *Oracle Identity Manager Installation and Configuration Guide for IBM WebSphere Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for JBoss Application Server*
- *Oracle Identity Manager Installation and Configuration Guide for Oracle Application Server*

23

Managing Generic Technology Connectors

The generic technology connector framework offers features that enable you to modify a generic technology connector. In addition, you can export or import a generic technology connector by using the Deployment Manager.

These features of the generic technology connector framework are discussed in the following sections:

23.1 Modifying Generic Technology Connectors

Caution: The Design Console can be used to modify connector objects that are automatically created at the end of the generic technology connector creation process. If you use the Manage Generic Technology Connector feature to modify a generic technology connector whose connector objects have been customized by using the Design Console, then all the customization work done using the Design Console would get overwritten. Therefore, Oracle recommends that you to follow one of the following guidelines:

- Do not use the Design Console to modify generic technology connector objects.

  The exception to this guideline is the IT resource. You can modify the parameters of the IT resource by using the Design Console. However, for the changes to take effect, you must purge the cache either before or after you modify IT resource parameters. See *Oracle Identity Manager Best Practices Guide* for information about running the `PurgeCache` utility.

- If you use the Design Console to modify generic technology connector objects, then do not use the Manage Generic Technology Connector feature to modify the generic technology connector.

See Chapter 28 for information about connector objects that are created automatically by the generic technology connector framework.

In addition, you can modify only one connector at a time. If you try to use the Modify pages for two different connectors at the same time on the same computer, then the Modify features would not work correctly.

Chapter 26, "Known Issues of Generic Technology Connectors" discusses both these points.

To modify a generic technology connector:

1. Open the Administrative and User Console.
2. Expand **Generic Technology Connector**.
3. Click **Manage**.
4. Search for the connector that you want to modify. To simplify your search, you can use a combination of the search criteria provided on this page. Alternatively, to view all the generic technology connectors that have been created on this Oracle Identity Manager installation, click **Search connectors** without specifying any search criteria.
5. In the results that are displayed, click the generic technology connector that you want to modify.
6. Click **Edit Parameters**. The Step 2: Specify Parameter Values page of the connector creation process is displayed. From this point onward, follow the procedure described in the "Step 2: Specify Parameter Values Page" section on page 22-6.

Note: The only difference between this procedure and the procedure that you follow to create the generic technology connector procedure is that automatic metadata detection does not take place when you modify an existing generic technology connector.

Caution: If you modify attributes of fields of the OIM - Account data set or its child data sets, then corresponding changes are not made in the Oracle Identity Manager database entries for these data sets. At the same time, no error message is displayed.

Therefore, for this release of Oracle Identity Manager, Oracle recommends that you do not modify the fields or child data sets of the OIM - Account data set.

This point has also been discussed in the "Step 3: Modify Connector Configuration Page" section on page 26-2 of the "Known Issues" chapter.

23.2 Exporting Generic Technology Connectors

You can export the XML file of a generic technology connector. This XML file contains definitions for all the objects that are part of the connector. If you want to use the same generic technology connector on a new Oracle Identity Manager installation, you must first export the XML file and then import it into the new Oracle Identity Manager installation.

To export the connector XML file:

See Also: The "Exporting Deployments" section on page 13-1

1. Open the Administrative and User Console.
2. Expand **Deployment Management**.
3. Click **Export**.
4. On the first page of the Deployment Manager Wizard, select **Generic Connector** from the list and then click **Search**.
5. In the search results, select the generic technology connector whose XML file you want to export.
6. Click **Select Children**.
7. For the selected generic technology connector, select the child entities that you want to export and then click **Select Dependencies**.
8. Select the dependencies that you want to export, and then click **Confirmation**.
9. After you verify that the elements displayed on the page cover your export requirements, click **Add for Export**.
10. Click **Exit wizard and show full selection**, and then click **OK**.

23.3 Importing Generic Technology Connectors

To copy a generic technology connector to a different Oracle Identity Manager installation:

1. If the connector uses custom providers, then you must copy the files created during provider creation to the appropriate directories on the destination Oracle Identity Manager installation.

   See Also: Chapter 21, "Creating Custom Providers for Generic Technology Connectors" for more information about these provider files and the directories into which you must copy them

2. Export the connector XML file on the source Oracle Identity Manager installation.
3. Import the connector XML file on the destination Oracle Identity Manager installation.

   Caution: You must ensure that the names you select for a generic technology connector and its constituent objects on a staging server do not cause naming conflicts with existing connectors and objects on the production server.

   The following scenario explains why you must follow this guideline:

   Suppose you create a generic technology connector on a staging server, and then want to import the connector to a production server. While creating the generic technology connector on the staging server, you would have ensured that the names of the generic technology connector and the connector objects are unique on that server. At the same time, you must also ensure that the names are not the same as the names of connectors and connector objects on the production server.

   If any of the names happen to be the same, then the old objects would be overwritten by the new objects when you import the connector XML file from the staging server to the production server. No message is displayed during the overwrite process, and the process would lead to eventual failure of the affected connectors.

   This is also mentioned in the "Names of Generic Technology Connectors and Connector Objects" section on page 26-1 of the "Known Issues" chapter.

   To ensure that you are able to revert to a working state in the event that an object is overwritten, you must create a backup of the destination Oracle Identity Manager database before you import a connector XML file.

To import the connector XML file:

1. Open the Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the connector XML file from the directory into which you copy it.
5. Click **Add File**.
6. Click **Next**, **Next**, and then **Skip**.
7. Click **View Selections**.

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

8. Click **Import**. The connector file is imported into Oracle Identity Manager.

After you import the connector XML file, you must update the run-time parameters of the generic technology connector.

Note: These values are not copied in the connector XML file when you export it.

To update the values of the run-time parameters, follow the procedure described in the "Modifying Generic Technology Connectors" section on page 23-2.

23.4 Upgrading Generic Technology Connectors to Oracle Identity Manager Release 9.1.0.1

If you upgrade from Oracle Identity Manager release 9.0.3.*x* to release 9.1.0.1, you must also upgrade the generic technology connectors that you created by using Oracle Identity Manager release 9.0.3.*x*. The procedure to upgrade generic technology connectors depends on the conditions under which you want to perform the upgrade operation:

- Scenario 1: You created a generic technology connector on Oracle Identity Manager 9.0.3.*x*. Later, you upgrade to Oracle Identity Manager 9.1.0.1.
- Scenario 2: You created a generic technology connector on Oracle Identity Manager release 9.0.3.*x*. You want to port the generic technology connector to an Oracle Identity Manager release 9.1.0.1 installation. To achieve this, you first export the generic technology connector XML file on the release 9.0.3.*x* installation and then import this XML file on the release 9.1.0.1 installation.

In both scenarios, the next step is to perform the procedure described in the "Modifying Generic Technology Connectors" section on page 23-2. While performing that procedure, you can change the values such as provider parameter values, field definitions, and field mappings according to your requirements. At the same time, you must specify or change values as prompted by the validations on the Manage Generic Technology Connector pages.

In Scenario 2, when you import a release 9.0.3.*x* generic technology connector into a release 9.1.0.1 Oracle Identity Manager installation, a non-fatal exception is recorded in the application server log file. This occurs only if the connector supports provisioning, regardless of whether or not it supports reconciliation. You can ignore this exception. No error message is displayed on the Administrative and User Console. This is also documented in the "General Known Issues" section on page 26-9.

24

Best Practices for Creating and Using Generic Technology Connectors

This chapter discusses the best practices, or guidelines, for creating and using generic technology connectors.

> **Note:** Some of the best practices have been repeated at appropriate places in the rest of the guide. Detailed descriptions are provided for best practices that are discussed only in this chapter.

Depending on the context in which you must apply them, the best practices are divided into the following sections:

- Step 1: Provide Basic Information Page
- Step 2: Specify Parameter Values Page
- Step 3: Modify Connector Configuration Page
- Shared Drive Reconciliation Transport Provider
- Custom Providers
- Connector Objects
- Modifying Generic Technology Connectors

24.1 Step 1: Provide Basic Information Page

Apply the following guidelines while specifying a name for a generic technology connector:

- **Summary:**

  Ensure that the name contains only ASCII characters. You can include the underscore (_) character, but do not include any other non-ASCII character in the name.

  Description:

  For most of the connector objects that are automatically created at the end of the connector creation process, the name of the generic technology connector is part of the name of the object itself. For example, if the name of the generic technology connector is `WebConn`, then the name of its scheduled task is `WebConn_GTC`.

  In the Oracle Identity Manager database, there is no provision for storing objects with names in non-ASCII characters. Therefore, an error message is displayed if

you enter non-ASCII characters while specifying the name of a generic technology connector.

- Ensure that the name is not the same as the name of any connector or connector object on the Oracle Identity Manager installation.
- If you plan to create the generic technology connector on a staging server and then move it to a production server, then ensure that the name of the generic technology connector does not cause naming conflicts with existing connectors or connector objects on the production server.
- Before you import a generic technology connector created on a staging server to a production server, create a backup of the destination Oracle Identity Manager database to ensure that you are able to revert to a working state in the event that a connector object is overwritten.
- If you select the Shared Drive Transport Provider, then you must select the CSV Format Provider.
- If you select the SPML Provisioning Format Provider, then you must select the Web Services Provisioning Transport Provider.
- If you select the Shared Drive Reconciliation Transport Provider, then ensure that there is data in the prescribed format on at least the first two lines of the parent and child data files provided by the target system for reconciliation. The prescribed form of data is discussed in the "Shared Drive Reconciliation Transport Provider" section on page 20-1.
- If you select the Shared Drive Reconciliation Transport Provider, then ensure that the required permissions are set on the staging and archiving directories before reconciliation begins. The required permissions are discussed in the "Permissions to Be Set on the Staging and Archiving Directories" section on page 20-6.
- Do not try to create more than one generic technology connector at a time, even from different sessions of the Administrative and User Console for the same Oracle Identity Manager installation.

24.2 Step 2: Specify Parameter Values Page

This section describes the following known issues related to the input that you specify on the Step 2: Specify Parameter Values page:

- **Summary:**

  If you use the Shared Drive Reconciliation Transport Provider, then:

  – Do not specify the same path for the staging and archiving directories. Existing files in the archiving directory are deleted if you specify the same path for both directories.

  – Ensure that the names of files in the staging directory are different from the names of files in the archiving directory. If the file names happen to be the same, then existing files in the archiving directory are overwritten at the end of a reconciliation run.

  Description:

  When you use the Shared Drive Reconciliation Transport Provider, after each reconciliation run, data files are moved from the staging directory to the archiving directory. The files moved to the archiving directory are not time-stamped or marked in any way. Therefore, when you use the Shared Drive Transport Provider, bear in mind the following guidelines:

- The archiving directory path and name that you specify must not be the same as the staging directory path and name. If you specify the same path and name, then the existing files in the archiving directory are deleted at the end of the reconciliation run.
- During the current reconciliation run, if data files with the same names as the files used in the last reconciliation run are placed in the staging directory, then the existing files in the archiving directory are overwritten by the new files from the staging directory. This can be illustrated by the following example:

  Suppose that at the end of the last reconciliation run, the following files were moved automatically from the staging directory to the archiving directory:

  ```
  usrdataParentData.csv
  usrdataRoleData.csv
  usrdataGroupMembershipData.txt
  ```

  For the current reconciliation run, you place the following files in the staging directory:

  ```
  usrdataParentData.csv
  usrdataRoleData_04Feb07.csv
  usrdataGroupMembershipData_04Feb07.txt
  ```

  At the end of the current reconciliation run, these files are moved to the archiving directory. When this happens, the old `usrdataParentData.csv` file is overwritten by the new one.

  Therefore, if you want to ensure that files in the archiving directory are not overwritten at the end of a reconciliation run, then you must ensure that the names of files in the staging directory are not the same as the names of files in the archiving directory.

- **Summary:**

  Metadata detection does not take place a second time if you go back to the Step 2: Specify Parameter Values page. Therefore, if required, you must manually make changes in the fields and field mappings displayed on the Step 3: Modify Connector Configuration page.

  Description:

  Suppose you want to change a value that you provide on the Step 2: Specify Parameter Values page. You can return to this page from the Step 4: Verify Connector Form Names or Step 5: Verify Connector Information page. However, metadata detection would not take place a second time when you click the Continue button after changing the provider parameter value. This functionality is aimed at preserving changes that you may have manually made on the Step 3: Modify Connector Configuration page.

  As an extension of this functionality, metadata detection does not take place even when you modify an existing generic technology connector.

24.3 Step 3: Modify Connector Configuration Page

This section discusses best practices related to the following areas:

- Names of Fields
- Password Fields
- Password-Like Fields

- Mappings
- OIM Data Sets

24.3.1 Names of Fields

Note that the following validations are applied when you specify a field name while adding or editing fields:

- Two fields that belong to the same data set (parent or child) cannot have the same name.
- Two child data sets of the same parent data set cannot have the same name.
- The name of a field in a parent data set cannot be the same as the name of one of its child data sets.
- Two different child data sets can have fields that have the same name, regardless of whether or not the child data sets belong to the same parent data set. For example, the `GroupMembership` data set and `Role` data set can each have a field with the name `UsrID`.
- Two different parent data sets can have fields that have the same name. Similarly, these data sets can also have child data sets that have the same name.
- The name of a child data set can be the same as that of one of its fields.

24.3.2 Password Fields

To ensure the security of passwords, password information must not be reconciled through a generic technology connector. In other words, you must ensure that the Source and Reconciliation Staging data sets do not contain the Password field. In addition, you must not map any field of the Reconciliation Staging data sets to the Password field of the OIM - User data set.

24.3.3 Password-Like Fields

A password-like field is a field to which you set the Encrypted and Password Field attributes (by selecting the Encrypted and Password Field check boxes). You can create a password-like field by setting these two attributes to a field that you add to the OIM - Account data set.

To secure the contents of password-like fields, bear in mind the following guidelines while adding or editing these fields:

- You can use the Password Field and Encrypted check boxes to secure the display and storage of password information in Oracle Identity Manager. However, when you map password-like fields to fields of the Provisioning Staging data set, you must take all necessary precautions to secure the data propagated in these fields. For example, you must ensure that this data is not stored in a plain-text file on the target system at the end of a provisioning operation.

  Oracle recommends creating only one-to-one mappings between the password field of the OIM - Account data set and the Provisioning Staging data set. In other words, this password field must not be used as an input field for a transformation mapping with a Provisioning Staging field. The same precaution must be taken for the Password field of the OIM - User data set.

- As mentioned earlier, the Password field is one of the predefined fields of the OIM - User data set. The Password Field and Encrypted attributes are set for this field. By using the Design Console, you can set the Password Field and Encrypted

attributes for a UDF that you create. This would give the newly created UDF the same properties as the existing Password field. However, the generic technology connector framework treats this field the same as any other text field (with the String data type) and the contents are not encrypted in the Administrative and User Console or database.

This has also been mentioned in the "General Known Issues" section on page 26-9.

24.3.4 Mappings

Apply the following best practices while working with fields of the OIM data sets:

- **Summary:**

  If you select the Translation Transformation Provider to create a mapping, then specify the name of a lookup definition in the Lookup Code Name region. If you specify a data set name and field in the Lookup Code Name region, then translation would fail during actual reconciliation or provisioning operations.

  Description:

  If you select the Translation Transformation Provider while creating a mapping, then the Step 2: Mapping page displays options for selecting a field from a data set and specifying a literal. Because you are using the Translation Transformation Provider, you must select the Literal option and enter the name of the lookup definition that contains the Code Key and Decode values for the translation. You must not select a data set name and field in the Lookup Code Name region. Although there is no validation to stop you from selecting a data set name and field, the translation operation would fail during actual reconciliation or provisioning operations.

- Create a mapping between the ID field of the OIM - Account data set and the field that uniquely identifies records of the Reconciliation Staging data set.
- Along with the ID field, other fields of the OIM - Account data set can be (matching-only) mapped to corresponding fields of the Reconciliation Staging data set to create a composite key field for reconciliation matching.
- Create mappings between all fields in Provisioning Staging data sets and corresponding fields in OIM data sets.
- To create a reconciliation rule, you create matching-only mappings between fields of the Reconciliation Staging data set and the OIM - User data set. If there are child data sets, then ensure that the names of fields of the Reconciliation Staging data set that are input fields for the matching-only mappings are not used in any of the Reconciliation Staging child data sets. If you do not follow this guideline, then reconciliation would fail.

  This has also been mentioned in the "Step 3: Modify Connector Configuration Page" section on page 26-2.

- A literal field can be used as one of the input fields of a transformation mapping. If you select the Literal option, then you must enter a value in the field. You must not leave the field blank after selecting it.

24.3.5 OIM Data Sets

Apply the following best practices while working with fields of the OIM data sets:

- For trusted source reconciliation, the following fields of the OIM – User data set must always hold values:

- User ID
- First Name
- Last Name
- Organization Name
- Xellerate Type
- Role

In addition, you can select other OIM – User fields that must be populated when a user account is created through reconciliation. For each of these fields, you must create mappings with the corresponding fields of the Reconciliation Staging data sets. During a reconciliation run, you must ensure that the fields of the target system that serve as the source for these fields always hold values.

For provisioning, you can select fields of the OIM – User and OIM – Account data sets whose values must be propagated to the target system. After you identify these fields, create mappings between them and their corresponding fields in the Provisioning Staging data sets. During a provisioning operation, you must enter values for each of these fields.

- If required, add user-defined fields (UDFs) to the list of predefined OIM - User data set fields by using the Design Console.

  However, do not use the Design Console to set the Password Field and Encrypted attributes for the UDF. The contents of a UDF are not encrypted if the Password Field and Encrypted attributes have been set for the field by using the Design Console.

  This has also been mentioned in the "General Known Issues" section on page 26-9.

- Do not modify or delete attributes of OIM - Account data set fields in an existing generic technology connector.

24.4 Shared Drive Reconciliation Transport Provider

Summary

If parent records and child data records are created and linked in both the target system and Oracle Identity Manager, then you must ensure that the staging directory contains both parent data and child data files at the start of each reconciliation run.

Description

Suppose there are parent data records with associated child data records in the target system. To reconcile these records into Oracle Identity Manager, you place the parent and child data files containing these records in the staging directory. During the reconciliation run, the child data records are linked to their corresponding parent data records. Before the start of any subsequent reconciliation run, if you remove the child data files from the staging directory, then reconciliation events are not created for this form of child data record deletion. If you want to remove child data records for specific parent data records, then you must remove the child data records from the child data file. You must ensure that the child data file is placed in the staging directory for each reconciliation run, even if there are no child data records (from the third line onward) in the files.

24.5 Custom Providers

Apply the following guideline while working with custom providers:

When you develop code for a custom Provisioning Transport Provider, ensure that the provider returns the unique field value at the end of a Create User operation. This functionality is implemented by the `sendData` method of the Provisioning Transport Provider. See "Role of Providers During Provisioning" on page 21-5 for more information.

24.6 Connector Objects

Apply the following guidelines while working with connector objects created automatically during generic technology connector creation:

- **Summary:**

  Do not attempt to use for provisioning the resource object created automatically for a reconciliation-only generic technology connector.

  Description:

  Suppose you select only the Reconciliation option while creating a generic technology connector. At the end of the creation process, a resource object is one of the objects created automatically for this generic technology connector. However, you cannot provision this resource object to any user because a generic adapter is not created for a reconciliation-only generic technology connector.

- **Summary:**

  Do not attempt to provision generic technology connector resource objects to organizations defined in Oracle Identity Manager.

  Description:

  A resource object is one of the connector objects that get created automatically during generic technology connector creation. This resource object can be provisioned only to OIM Users. You must not attempt to provision it to organizations defined in Oracle Identity Manager.

  This has also been mentioned in the "Connector Objects" section on page 26-8.

- You can use the Design Console to customize connector objects that are automatically created during generic technology connector creation. After you customize connector objects, if you perform a Manage Generic Technology Connector operation, then all the customization done on the connector objects would be overwritten. Therefore, Oracle recommends that you to apply one of the following guidelines:

  – Do not use the Design Console to modify generic technology connector objects.

    The exception to this guideline is the IT resource. You can modify the parameters of the IT resource by using the Design Console. However, if you have enabled the cache for the `GenericConnector` and `GenericConnectorProviders` categories, then you must purge the cache either before or after you modify IT resource parameters. See the "Purging the Cache" section in *Oracle Identity Manager Best Practices Guide* for more information.

  – If you use the Design Console to modify generic technology connector objects, then do not use the Manage Generic Technology Connector feature to modify the generic technology connector.

  This has also been mentioned in the "Connector Objects" section on page 26-8.

- Prepopulate adapters are not part of the set of connector objects that are created automatically when you create a generic technology connector. However, while creating a generic technology connector, you can map provisioning input to literals and user data fields. Although this feature cannot be used to prepopulate the User Defined Form, it can be used to prepopulate the provisioning data packet.

24.7 Modifying Generic Technology Connectors

Apply the following best practices while modifying generic technology connectors:

Do not try to modify more than one generic technology connector at a time, even from different sessions of the Administrative and User Console for the same Oracle Identity Manager installation.

25

Troubleshooting Generic Technology Connector Errors

This chapter provides solutions to some commonly encountered problems associated with using generic technology connectors. The information in this chapter is divided into the following sections:

- Errors Encountered at the End of the Connector Creation Process
- Common Errors Encountered During Reconciliation
- Common Errors Encountered During Provisioning

25.1 Errors Encountered at the End of the Connector Creation Process

The following are error messages that may be displayed at the end of the generic technology connector creation process. Each message explains the event that causes or during which the error message is displayed.

- An error was encountered while generating the import XML file for generic technology connector *connector_name*.
- An error was encountered while updating the IT resource parameters with the values provided for the run-time provider parameters of generic technology connector *connector_name*.
- An error was encountered while either generating the XML file for generic technology connector *connector_name* or saving it in the Oracle Identity Manager database.
- An error was encountered while importing the XML file for generic technology connector *connector_name*. The required lock on the import operation could not be acquired.
- An error was encountered while saving the information for generic technology connector *connector_name*. Check the application logs for more details.
- An error was encountered while creating a resource object for the generic technology connector *connector_name*. An existing resource object has the same name as the one being assigned to this resource object.

25.2 Common Errors Encountered During Reconciliation

Table 25–1 provides solutions to some commonly encountered problems associated with the reconciliation process.

Note: These errors are logged only if you are using the Shared Drive Reconciliation Transport Provider and the CSV Reconciliation Format Provider.

If any of these errors occurs, then the error message is written to the application server log file.

Table 25–1 Common Errors Encountered During Reconciliation

Problem Description (Error Message)	Solution
No run time provider parameters available	Use the Manage Generic Technology Connector feature to check the values specified for the run-time parameters. Then, retry reconciliation.
No design time provider parameters available	Use the Manage Generic Technology Connector feature to check the values specified for the design parameters. Then, retry reconciliation.
Staging directory location is not defined	Use the Manage Generic Technology Connector feature to check the value specified for the Staging Directory (Parent Identity Data) parameter. Then, retry reconciliation.
File encoding is not defined	Use the Manage Generic Technology Connector feature to check the value specified for the File Encoding (Parent Data) parameter. Then, retry reconciliation.
Archive directory location is not defined	Use the Manage Generic Technology Connector feature to check the value specified for the Archiving Directory parameter. Then, retry reconciliation.
Cannot process files as not even fixed-width delimiter has been defined	Use the Manage Generic Technology Connector feature to check if a value has been specified for one of the following parameters: ■ Specified Delimiter ■ Tab Delimiter ■ Fixed Column Width Then, retry reconciliation.
No Parent files in staging directory No files available for reading	Ensure that data files are present in the directory specified as the value of the Staging Directory (Parent Identity Data) parameter. Then, retry reconciliation.
No child data present in staging directory No files available for reading	Ensure that data files are present in the directory specified as the value of the Staging Directory (Multivalued Identity Data) parameter. Then, retry reconciliation.
The Staging directory cannot be accessed. Either the directory path does not exist or necessary access permissions are missing	Ensure that the directories specified as parameter values have the required permissions. See "Shared Drive Reconciliation Transport Provider" on page 20-1 for information about the required permissions. Then, retry reconciliation.
Data files could not be read as its File encoding is not supported.	Use the Manage Generic Technology Connector feature to check the value specified for the File Encoding parameter. Then, retry reconciliation.
Not able to parse metadata	Check the metadata (contents of the second row) present in the parent and child data files. There may be a problem with the delimiter used in the files. Fix the problem, and then retry reconciliation.
Not able to parse header	Check the header (contents of the first row) of the data files. There may be a problem in the format of the header. See "Shared Drive Reconciliation Transport Provider" on page 20-1 for information about the header format. Fix the problem, and then retry reconciliation.
Current Record is erratic and cannot be parsed	Check the entry that is written to the application server log file. It may contain errors that cannot be parsed. Fix the problem, and then retry reconciliation.

25.3 Common Errors Encountered During Provisioning

The following table provides solutions to some commonly encountered problems associated with the provisioning process.

Note: Most of these errors are logged only if you are using the Web Services Provisioning Transport Provider and the SPML Provisioning Format Provider.

If any of these errors occurs, then the error message is displayed on the UI and written to the application log file.

Table 25–2 Common Errors Encountered During Provisioning

Problem Description	Solution
Response code: SPML Velocity Properties Not Read **Response Description:** The SPML template properties could not be read.	There is a problem with the Oracle Identity Manager installation. Contact Oracle Support, and send them information about this problem and the response code and description displayed. In addition, send the relevant logs generated after running Oracle Identity Manager with logging set to the DEBUG level.
Response code: SPML Template Not Read **Response Description:** The SPML template file was not found.	There is a problem with the Oracle Identity Manager installation. Contact Oracle Support, and send them information about this problem and the response code and description displayed. In addition, send the relevant logs generated after running Oracle Identity Manager with logging set to the DEBUG level.
Response code: SPML Unknown Operation **Response Description:** This provisioning operation is not one of the permitted operations: Create, Delete, Enable, Disable, Modify, and Child Table Operations.	There is a problem with the Oracle Identity Manager installation. Contact Oracle Support, and send them information about this problem and the response code and description displayed. In addition, send the relevant logs generated after running Oracle Identity Manager with logging set to the DEBUG level.
Response code: SPML Provisioning Input Null **Response Description:** SPML provisioning input data is null.	Check if the provider parameters have been correctly specified. Check if provisioning was initiated by direct provisioning or request provisioning. Retry the procedure by using the direct provisioning option.
Response Code: SPML Template Context Processing Error **Response Description:** An error was encountered while processing the template context for generation of SPML request.	There is a problem with the Oracle Identity Manager installation. Contact Oracle Support, and send them information about this problem and the response code and description displayed. In addition, send the relevant logs generated after running Oracle Identity Manager with logging set to the DEBUG level.
Response code: SPML Provisioning Operation Name Missing **Response Description:** The operation name for provisioning is missing.	The generic technology connector may not have been created correctly. Try creating another connector by using the same set of configurations (providers) but with fewer attributes. Try direct provisioning.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response code: SPML Provisioning Child Name Missing **Response Description:** The child name is missing.	You may have been trying to perform provisioning for one particular type (for example, role or membership) of multivalued attribute when this error occurred. The connector may not have been created correctly. Try creating another connector by using the same set of configurations (providers) but only one multivalued attribute, which is the one that failed the first time. Try direct provisioning.
Response code: SPML Provisioning Child Meta-Data Null **Response Description:** The child metadata list is null.	You may have been trying to perform provisioning for one particular type (for example, role or membership) of multivalued attribute when this error occurred. The connector may not have been created correctly. Try creating another connector by using the same set of configurations (providers) but only one multivalued attribute, which is the one that failed the first time. Try direct provisioning.
Response code: SPML Provisioning Child Metadata Problem **Response Description:** An error was encountered while sorting the child metadata list.	You may have been trying to perform provisioning for one particular type (for example, role or membership) of multivalued attribute when this error occurred. The connector may not have been created correctly. There is a problem in the order that has been set for the provisioning fields. Try creating another connector with fewer attributes for the relevant multivalued field. Try direct provisioning. After each successful round of provisioning, try adding fields one by one by performing the Manage Generic Technology Connector procedure. The point at which you start facing this issue again identifies the field that is not in the correct order.
Response code: SPML Provisioning ID Missing **Response Description:** The unique ID is missing.	You are trying to run an operation on a created user. However, the Create User operation itself may not have run successfully and the unique ID (psoID) that was expected as the response was not received. Therefore, the provisioned instance data was not updated in Oracle Identity Manager. Check why this operation failed.
Response code: SPML Provisioning Target ID Missing **Response Description:** The unique Target ID is missing.	Check the provider parameters that have been entered. TargetID may be missing.
Response code: OIM API Error **Response Description:** An error was encountered in the Oracle Identity Manager API layer.	Check if Oracle Identity Manager is operating correctly for other operations. Check the connectivity between the Oracle Identity Manager front end and the database. **Note:** This error is not related to the providers that you use.
Response code: OIM Process Form Not Found **Response Description:** The process form was not found in Oracle Identity Manager.	The generic technology connector may not have been created correctly. Try creating another connector by using the same set of configurations. Try direct provisioning. **Note:** This error is not related to the providers that you use.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response code: OIM Process Form Instance Not Found **Response Description:** The process form instance was not found for the specified form during update.	The provisioned instance information in the Oracle Identity Manager database may have become corrupted. Try direct provisioning. If the problem persists, then there may be an issue with the generic technology connector. Create another generic technology connector by using the same set of configurations. **Note:** This error is not related to the providers that you use.
Response code: OIM Atomic Process Instance Not Found **Response Description:** The process instance found is not an atomic process.	The provisioned instance information in the Oracle Identity Manager database may have become corrupted. Try direct provisioning. If the problem persists, then there may be an issue with the generic technology connector. Create another generic technology connector by using the same set of configurations. **Note:** This error is not related to the providers that you use.
Response code: Column Not Found **Response Description:** An expected column was not found in the result set.	The generic technology connector may not have been created correctly. Try creating another connector by using the same set of configurations. Try direct provisioning. **Note:** This error is not related to the providers that you use.
Response code: Invalid Provider **Response Description:** The provider name specified is invalid.	The Provisioning Format, Transformation, or Provisioning Transport Provider in use may not have been registered correctly. Check if you have correctly followed the steps to register the providers. If this error is displayed when a predefined provider is used, then check the directory on the Oracle Identity Manager server for the XML files of these providers. These XML files are in the following directory: *OIM_HOME*/xellerate/GenericConnector/ProviderDefinitions
Response code: IT Resource Instance Not Found **Response Description:** The IT resource instance was not found in Oracle Identity Manager.	The generic technology connector may not have been created correctly. Try creating another generic technology connector by using the same set of configurations. Try direct provisioning. **Note:** This error is not related to the providers that you use.
Response code: Version Not Found **Response Description:** The required process form version was not found in Oracle Identity Manager.	The generic technology connector may not have been created correctly. Try creating another connector by using the same set of configurations. If you have edited an existing connector by adding a new field to an existing data set, then that operation may have failed. Try making the same change again in the connector. **Note:** This error is not related to the providers that you use.
Response code: Version Not Defined **Response Description:** The required process form version was not defined in Oracle Identity Manager.	The generic technology connector may not have been created correctly. Try creating another connector by using the same set of configurations. If you have edited an existing connector by adding a new field to an existing data set, then that operation may have failed. Try making the same change again in the connector. **Note:** This error is not related to the providers that you use.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response code: Web Service Not Found **Response Description:** The Web service was not found on the target server. Check the service name and IP address.	Check the service name and IP address provided in the Web service URL. If these are correct, then check if the Web service is running.
Response code: Web Service Connection Refused **Response Description:** The Web service connection could not be established. Check that the server is running and the specified port is correct.	Check if the Web service is running.
Response code: Web Service No Such Method **Response Description:** The Web service method could not be started. Check the operation name and parameters.	Check the operation name and parameters.
Response code: Web Service Null Parameter Value **Response Description:** The parameter value passed to the Web service is null.	Check if the provisioning process ran correctly. The Provisioning Format Provider may not have run correctly and, therefore, may have generated NULL output.
Response code: Web Service HTTP Library Missing **Response Description:** The Web service HTTP library is not included in the classpath.	There is a problem with the Oracle Identity Manager installation. Contact Oracle Support and send them information about this problem and the response code and description displayed. In addition, send the relevant logs generated after running Oracle Identity Manager with logging set to the DEBUG level.
Response code: Web Service Null Result Value **Response Description:** The Web service result value is null.	Check if the Web service is running correctly. At present, it is generating NULL output as the response to the Oracle Identity Manager provisioning request.
Response code: Web Service Invocation Issue **Response Description:** An error was encountered while invoking the Web service.	Check the credentials of the Web service.
Response code: Web Service Target URL Missing **Response Description:** The Web service target URL required to invoke the Web service is missing.	Check the values of the provider parameters. The Web service URL may be missing. Modify the generic technology connector and provide this value again.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response code: Web Service Target Method Name Missing **Response Description:** The Web service target method name required to invoke the Web service is missing.	Check the values of the provider parameters. The Web service operation name may be missing. Modify the generic technology connector and provide this value again.
Response code: Web Service Response XML Parsing Error **Response Description:** An error was encountered during XML parsing of the Web service response.	Check if the Web service is running correctly. It is generating an SPML response that does not conform to the format specified for the Web service provider.
Response code: Web Service Response ID Error **Response Description:** Either a unique ID is not getting generated from the Web service, or its value could not be parsed because of an incorrect attribute name in the response XML file.	Check if the Web service is running correctly. For the Create User operation, it is generating an SPML response that does not conform to the specified format. In addition, it is not returning the `psoID` created in the target system. The provider specification for the Web Service provider expects the return of the psoID field.
Response code: Web Service Protocol Connection Error **Response Description:** An error was encountered in the Oracle-SOAP HTTP connection.	Check the service name and IP address provided in the Web service URL. If these are correct, then check if the Web service is running. Check the operation name and parameters.
Response code: Web Service Protocol Processing Error **Response Description:** An error was encountered while calling the Oracle-SOAP API.	Check the service name and IP address provided in the Web service URL. If these are correct, then check if the Web service is running. Check the operation name and parameters.
Response Code: Unable to parse the date **Response Description:** Error encountered while parsing the date.	The value specified for the Target Date Format parameter is not correct. For information about the date formats that you can specify, see the following Web page: `http://java.sun.com/docs/books/tutorial/i18n/format/simpleDateFormat.html#datepattern`
Response Code: Data Access Error **Response Description:** A data access error occurred while executing the query or loading the result set.	Check if Oracle Identity Manager is operating correctly for other operations. Check the connectivity between the Oracle Identity Manager front end and the database. **Note:** This error is not related to the providers that you use.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response Code: SSL Handshake Did Not Happen **Response Description:** An SSL handshake did not happen during the secure communication with the target Web service.	Check if the SEcure Sockets Layer (SSL) configuration between Oracle Identity Manager and the target system has been correctly completed. If required, perform the procedure again.
Response Code: Error in Initialization of SSL-Related Properties **Response Description:** An error was encountered during the initialization of SSL-related properties. The relevant values are read from the "RMSecurity" element in the *OIM_SERVER*/xellerate/config/xlconfig.xml file.	Check the configuration entries corresponding to the `RMSecurity` element of the `xlconfig.xml` file.
Response Code: Invalid Web Service Keystore or password **Response Description:** An invalid keystore name or password was encountered in the *OIM_HOME*/xellerate/config/xlconfig.xml file. Check the configuration entries corresponding to the "RMSecurity" element.	Check the configuration entries corresponding to the `RMSecurity` element of the `xlconfig.xml` file.
Response Code: Error Encountered During Web Service Keystore Initialization **Response Description:** Keystore initialization failed. Credentials of the keystore are mentioned in the *OIM_HOME*/xellerate/config/xlconfig.xml file under the "RMSecurity" element.	Check the configuration entries corresponding to the `RMSecurity` element of the `xlconfig.xml` file.
Response Code: Invalid ID **Response Description:** An invalid ID is present in the input SPML request.	Check the value specified for the `Target ID` parameter.
Response Code: Object already exists **Response Description:** This object already exists in the target system.	Check if the object that you are trying to create already exists on the target system.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response Code: Operation Not Supported **Response Description:** The requested provisioning operation is not supported.	Check if the target system supports the requested provisioning operation. For information about the types of SPML provisioning operations that can be performed by using the SPML Provisioning Format Provider, see the "SPML Provisioning Format Provider" section on page 20-7.
Response Code: Invalid ID Type in Input SPML Request **Response Description:** An invalid ID type is present in the input SPML request.	Check the sample SPML request corresponding to the type of request that was sent, and determine if the target system supports all the ID values that were included in the request. You can access the sample SPML requests in the following directory: *OIM_HOME*/xellerate/GTC/Samples/spml
Response Code: ID in Input SPML Request Does Not Exist in the Target System **Response Description:** The ID in the input SPML request does not exist in the target system.	Ensure that the `psoID` value that was sent in the request exists in the target system.
Response Code: Requested Execution Mode Not Supported **Response Description:** The requested execution mode is not supported.	Ensure that the target system supports the execution of requests in synchronous mode.
Response Code: Invalid Container **Response Description:** The object cannot be added to the specified container. Refer to the log file for more information. Check the value of the "errorMessage" element in the SPML response.	Check if a container corresponding to the container ID specified in the request exists on the target system.
Response Code: Nonstandard SPML Error **Response Description:** A target-specific error was encountered. Refer to the log file for more information. Check the value of the "errorMessage" element in the SPML response.	Check the value of the `errorMessage` element in the SPML response. This element contains the target system error message that was generated when the error was encountered.
Response Code: SPML Response Is for Asynchronous Mode **Response Description:** The SPML response is for asynchronous mode, which is not supported for this release.	Ensure that the target system sends responses corresponding to the synchronous mode of request execution.

Table 25–2 (Cont.) Common Errors Encountered During Provisioning

Problem Description	Solution
Response Code: Error Encountered While Parsing Constituent Elements of Web Service URL **Response Description:** An error was encountered while parsing the constituent elements of the Web service URL. Check if the specified URL contains the protocol, host name, port and the endpoint. Oracle recommends copying the URL from the relevant WSDL file while specifying provider parameter values during connector creation.	Check if the specified URL contains the protocol, host name, port, and endpoint. Oracle recommends copying the URL from the relevant WSDL file while specifying provider parameter values during connector creation.
Response Code: SPML Response failed V2 schema validation **Response Description:** SPML Response received is not compliant with the SPML V2 standard specifications.	Ensure that the SPML response returned by the target system conforms to the SPML V2 standard specification.

26

Known Issues of Generic Technology Connectors

Known issues related to generic technology connectors are divided into the following categories:

26.1 Names of Generic Technology Connectors and Connector Objects

This section describes the following known issues related to the names that you specify for generic technology connectors and connector objects:

Summary:

- No warning is displayed if the name that you specify for a generic technology connector is the same as the name of an existing connector object.
- No warning is displayed if an existing connector object is overwritten by a new connector object when you import a connector XML file.

Description:

During the creation or modification of a generic technology connector, various objects are automatically created or modified by the generic technology connector framework. You are prompted to specify names for the generic technology connector and process forms. The framework automatically generates names for the remaining objects. These autogenerated names are based on the name that you specify for the generic technology connector.

When you specify a name for the generic technology connector, you must ensure that the name is unique across all object categories (such as resource objects and IT resources) for that Oracle Identity Manager installation. Similarly, you must also ensure that the process form names are unique. This guideline must be followed even while importing a generic technology connector XML file to a different Oracle Identity Manager installation. You must ensure that the names of objects defined in the XML file are not the same as the names of objects belonging to the same category on the destination Oracle Identity Manager installation. For example, the name of the scheduled task defined in the XML file must not be the same as the name of any other scheduled task on the destination Oracle Identity Manager installation.

The scope of this guideline covers all connector objects, regardless of whether the object is used by a predefined connector or a generic technology connector on the destination Oracle Identity Manager installation.

If you do not follow this guideline, then existing objects that have the same name as imported objects are overwritten during the XML file import operation. No message is displayed during the overwrite process, and the process leads to eventual failure of the affected connectors.

This point has also been discussed in the "Connector Objects" section on page 26-8.

26.2 Step 3: Modify Connector Configuration Page

This section describes the following known issues related to the input that you specify on the Step 3: Modify Connector Configuration page:

- **Summary:**

  While modifying an existing generic technology connector, if you modify the fields or child data sets of the OIM - Account data set, then corresponding changes are not made in the Oracle Identity Manager database entries for the forms that are based on these data sets. At the same time, no error message is displayed.

  Description:

  The Step 3: Modify Connector Configuration page provides features to add, modify, and delete fields and field mappings. You can use these features to modify the length or data type of fields in the OIM - Account data set or its child data sets. However, this action would not translate into corresponding changes in the Oracle Identity Manager database entries for these data sets. At the same time, no error message is displayed.

  This issue will be fixed in a future release of Oracle Identity Manager. Until then, you must not make changes in the fields or child data sets of the OIM - Account data set.

- **Summary:**

  Suppose you create a generic technology connector, use it for provisioning or reconciliation, and then delete fields or child data sets of the OIM - Account data set. An error occurs the next time you perform provisioning or reconciliation by using the same generic technology connector.

  Description:

  Suppose you create a generic technology connector and then use it for provisioning or reconciliation. You then delete some fields or child data sets of the OIM - Account data set of this generic technology connector. The next time you perform provisioning or reconciliation by using the same generic technology connector, an exception is thrown.

  After you use the generic technology connector for provisioning or reconciliation even once, deleting the fields or child data sets of the OIM - Account data set is an invalid operation. This is because data linked to the fields or child data sets that you delete has already been stored in the Oracle Identity Manager database.

  Therefore, you must not delete fields or child data sets of the OIM - Account data set if the generic technology connector has already been used to perform provisioning or reconciliation.

  In a future release, an appropriate error message will be displayed instead of the exception that is thrown at present.

- **Summary:**

  If the name of a Reconciliation Staging field used in a matching-only mapping were to be reused as the name of a field in a Reconciliation Staging child data set, then reconciliation would fail.

  Description:

  You create a reconciliation rule by creating matching-only mappings between fields of the Reconciliation Staging data set and OIM - User data set. If there are child data sets, then you must ensure that the names of fields of the Reconciliation Staging data set that are input fields for the matching-only mappings are not used in any of the Reconciliation Staging child data sets. If the name of a Reconciliation Staging field used in a matching-only mapping were to be reused as the name of a field in a Reconciliation Staging child data set, then reconciliation would fail.

  The following example illustrates this scenario:

  The `AD_User` data set is the Reconciliation Staging parent data set. The following are the fields of this data set:

  – User ID

  – Name

  – Designation

  – Location

  The `Admin_Groups` data set is a child data set of the `AD_User` data set. If you use the `User ID` field of the `AD_User` data set to create a matching-only mapping with the OIM - User data set, then you cannot have a field with the name `User ID` in the `Admin_Groups` data set. If this child data set were to contain a field with the name `User ID`, then reconciliation would fail.

- **Summary:**

  The Password field is displayed in the OIM – User data set, even though this field is not reconciled by the reconciliation engine.

  Description:

  If you select the Trusted Source Reconciliation option on the Step 1: Provide Basic Information page, then the Password field is displayed in the OIM – User data set on the Step 3: Modify Connector Configuration page, even though this field is not reconciled by the reconciliation engine. If you create a mapping between this field and the corresponding target system field in the Reconciliation Staging data set, then the reconciliation field mapping that is automatically generated would try to map the field to the Password field. This, in turn, would cause the reconciliation event to fail.

- There are limitations related to creating transformation mappings across the following data sets:

  – Source and Reconciliation Staging

  – OIM and Provisioning Staging

  These limitations are as follows:

  – You cannot create a transformation mapping between a child data set of the Source or OIM data set and a different (that is, not corresponding) child data set of the Reconciliation Staging or Provisioning Staging data sets. This also means that you cannot create a many-to-one mapping from multiple child

data sets of one parent data set to a single child data set of another parent data set.

The following example illustrates this limitation:

Suppose the Source parent data set has the following child data sets:

MyGTC:Group data set

* Field 1: Group Name
* Field 2: Group Type

MyGTC:Role data set

* Field 1: Role Name
* Field 2: Role Type

Suppose the Reconciliation Staging parent data set has the following child data sets:

MyGTC:Group data set

* Field 1: Group Name
* Field 2: Group Type

MyGTC:Role data set

* Field 1: Role Definition

According to this limitation, you cannot create a transformation mapping between, for example, the Group Name field of the Source data set and the Role Definition field of the Reconciliation Staging data set.

However, you can create a many-to-one transformation mapping between, for example, the Role Name and Role Type fields of the Source data set and the Role Definition field of the Reconciliation Staging data set.

– You cannot create a transformation mapping between a Source or OIM parent data set and a Reconciliation Staging or Provisioning Staging child data set.

The following example illustrates this limitation:

Suppose the following are OIM data sets and their fields:

OIM - Account data set

* Field 1: Name
* Field 2: Address
* Field 3: User ID
* .. .

Suppose the following are Provisioning Staging child data sets and their fields:

Group data set

* Field 1: Group Name
* Field 2: Group Type

According to this limitation, you cannot create a transformation mapping between, for example, the Name field of the OIM - Account data set and the Group Name field of the Group data set.

- To create a reconciliation rule, you create matching-only mappings between fields of the Reconciliation Staging data set and the OIM - User data set. If there are child data sets, then ensure that the names of fields of the Reconciliation Staging data set that are input fields for the matching-only mappings are not used in any of the Reconciliation Staging child data sets.

  If this guideline is not followed, then reconciliation would fail.

- Suppose you set the Date data type for a field on a child form. A Delete Child Record provisioning operation would fail if there is a date value in this field during the operation.

26.3 Multilanguage Support

This section describes the following known issues related to the Multilanguage Support feature:

- **Summary:**

  No warning is displayed if there are non-ASCII characters in the first or second line of the data files in the staging directory.

  Description:

  There is no support for non-ASCII data in the metadata of target system user data. If you use the CSV Reconciliation Format Provider, then this limitation means that you cannot include non-ASCII characters in the metadata line (second line) of the parent and child data files that you store in the staging directory.

  The reason for this limitation is as follows:

  The generic technology connector framework creates User Defined process forms in Oracle Identity Manager and names the forms and their fields on the basis of the input metadata. In addition, database tables and columns are created for these forms and their fields, respectively. Because non-ASCII characters cannot be used in database object names, these characters are not supported in the target system metadata.

  The generic technology connector framework may be able to parse and correctly display non-ASCII characters in the first and second lines of the data files. However, to ensure that the connector objects are created correctly, you must ensure that non-ASCII characters are not used in the first and second lines of the data files.

  Note: From the third line onward in the data files, the field data values can contain non-ASCII characters. These data values are reconciled and stored in the Oracle Identity Manager database.

- **Summary:**

  For any language that Oracle Identity Manager supports, if the browser language setting does not match the operating system language setting of the Oracle Identity Manager server, then data is not displayed correctly on the Step 3: Modify Connector Configuration page.

  Description:

  The Step 3: Modify Connector Configuration page displays an image that is dynamically created by the generic technology connector framework. The following are limitations related to the display of localized text items on this page:

The language in which you want field labels to be displayed must match the following language settings:

– Oracle Identity Manager language

– Operating system language

– Browser language

If the browser language setting is the same as the operating system language setting of the Oracle Identity Manager server, then all the text items (field names and GUI element labels) are displayed in the required language.

Note:

- Localized GUI element labels are displayed only if you create and use resource bundles that contain localized labels for these GUI elements.
- If you are using the Traditional Chinese or Simplified Chinese language, then the browser locale (language and country/region) must be the same as the operating system locale (language and country/region) for all the text items to be displayed in the required language.

If the browser language is not the same as the operating system language, then the following static labels would be displayed in English (regardless of the browser language):

– Labels of the OIM - User and OIM - Account data sets: "User" and "Account"

– Labels of the fields that constitute the OIM - User data set:

  * "User ID"

  * "Email"

  * "First Name"

  * "Last Name"

For non-ASCII languages, labels for the remaining items on the Step 3: Modify Connector Configuration page would not be displayed correctly.

- **Summary:**

  Certain text items displayed on the Step 3: Modify Connector Configuration page are always displayed in English.

  Description:

  For this release, some of the static text displayed on the Step 3: Modify Connector Configuration page has not been localized. For example, suppose you create a generic technology connector named `MyGTC`. When you provision the resource object of this connector to a user, the following text is displayed on the page:

  ```
  Provisioning form for MyGTC

  Child Form of MyGTC representing child-dataset:
  child_data_set_name
  ```

  In this release of Oracle Identity Manager, the static part of this text is always displayed in English.

If required, you can localize the static text as follows:

See Also: *Oracle Identity Manager Globalization Guide*

1. For the language to which you want to localize the text, open the corresponding `customResources.properties` file. The files for all the languages that Oracle Identity Manager supports are in the *`OIM_HOME`*`/xellerate/customResources` directory.

   The following example illustrates this step of the procedure.

   Suppose you specify the following values while creating a generic technology connector:

   – Connector Name: `MyGTC`

   – Parent Form name: `ADUser`

   – Child data set name: `ADUserRole`

   – Child form name: `ADURole1`

   If you want the static text to be displayed in the Spanish language, then open the `customResources_es.properties` file. This file is in the *`OIM_HOME`*`/xellerate/customResources` directory.

2. In the `customResources.properties` file for the required language, add the following lines:

   ```
   global.UD_PARENT_FORM_NAME.description=Localized_text_for_"Provisioning
   form for" GTC_name

   global.UD_CHILD_FORM_NAME.description=Localized_text_for_"Child Form of"
   GTC_name Localized_text_for_"representing the child data set":
   child_data_set_name
   ```

   In these two lines, replace:

   * *`PARENT_FORM_NAME`* with the name of the parent form

     The parent form name is always converted to uppercase letters in Oracle Identity Manager. Therefore, the name that you enter must be in uppercase letters.

   * *`Localized_text_for_"Provisioning form for"`* with localized text for the words "Provisioning form for"

   * *`GTC_name`* with the name of the generic technology connector

   * *`CHILD_FORM_NAME`* with the name of the child form

     The child form name is always converted to uppercase letters in Oracle Identity Manager. Therefore, the name that you enter must be in uppercase letters.

   * *`Localized_text_for_"Child Form of"`* with localized text for the words "Child form for"

   * *`child_data_set_name`* with the name of the child data set

   For example:

   For the Spanish language, add the following lines in the `customResources_es.properties` file:

   ```
   global.UD_ADUSER.description=Spanish_text_for_"Provisioning form for" MyGTC
   ```

```
global.UD_ADUROLE1.description=Spanish_text_for_"Child Form of" MyGTC
Spanish_text_for_"representing the child data set": ADUserRole
```

26.4 Connector Objects

This section describes the following known issues related to the connector objects that are automatically created by the generic technology connector framework:

- **Summary:**
  - No warning is displayed if the name that you specify for a generic technology connector is the same as the name of an existing connector object.
  - No warning is displayed if an existing connector object is overwritten by a new connector object when you import a connector XML file.

  Description:

  This point has also been discussed in the "Names of Generic Technology Connectors and Connector Objects" section on page 26-1.

- **Summary:**

  After an error occurs during generic technology connector creation, form names are not displayed on the Step 4: Verify Connector Form Names page when you revisit that page by clicking Back on the Step 5: Verify Connector Information page.

  This is intentional and not the result of an issue or limitation of the software.

  Description:

  As mentioned earlier in this guide, some connector objects are automatically created even if the overall generic technology connector creation process fails. This set of connector objects includes process forms whose names you specify on the Step 4: Verify Connector Form Names page. In the event that the connector creation process fails, you are prompted to enter new form names through the display of blank fields on the Step 4: Verify Connector Form Names page. This is to ensure that the uniqueness checks on the process form names are reapplied when you submit the new form names.

  As an alternative to revisiting the previous pages and providing input for creating the generic technology connector, you can start all over again from the Step 1: Provide Basic Information page and re-create the generic technology connector.

- **Summary:**

  You cannot provision generic technology connector resource objects to organizations defined in Oracle Identity Manager.

  Description:

  A resource object is one of the connector objects that get created automatically during generic technology connector creation. This resource object can be provisioned only to OIM Users. You must not attempt to provision it to organizations defined in Oracle Identity Manager.

- **Summary:**

  Customization work done on objects of a generic technology connector would be overwritten if you perform a Manage Generic Technology Connector operation.

  Description:

You can use the Design Console to customize connector objects that are automatically created during generic technology connector creation. However, after you customize connector objects, if you perform a Manage Generic Technology Connector operation, then all the customization done on the connector objects would be overwritten. Therefore, Oracle recommends that you to apply one of the following guidelines:

- Do not use the Design Console to modify generic technology connector objects.

  The exception to this guideline is the IT resource. You can modify the parameters of the IT resource by using the Design Console. However, if you have enabled the cache for the `GenericConnector` and `GenericConnectorProviders` categories, then you must purge the cache either before or after you modify IT resource parameters. See *Oracle Identity Manager Best Practices Guide* for information about running the `PurgeCache` utility.

- If you use the Design Console to modify generic technology connector objects, then do not use the Manage Generic Technology Connector feature to modify the generic technology connector.

- Connector objects that are automatically created are not deleted even if the generic technology connector creation process fails.

26.5 General Known Issues

This section describes the following known issues that do not fall under any of the preceding categories:

- **Summary:**

  Unsafe-Filename exceptions may be thrown during the generic technology connector creation process.

  Description:

  On Oracle WebLogic Server and Oracle Application Server, the Unsafe-Filename exception may be thrown during the generic technology connector creation process. This exception can be ignored. The generic technology connector creation process is not affected by the occurrence of these exceptions. This issue is not seen on IBM WebSphere Application Server and JBoss Application Server.

- Generic technology connectors do not support the reconciliation of parent data deletion.

  You cannot use a generic technology connector to reconcile the deletion of parent data. For example, if the account of user `John Doe` is deleted from the target system, then you cannot use a generic technology connector to reconcile this user deletion in Oracle Identity Manager.

- **Summary:**

  The contents of a UDF are not encrypted if the Password Field and Encrypted attributes have been set for the field by using the Design Console.

  Description:

  As mentioned earlier, the Password field is one of the predefined fields of the OIM - User data set. The Password Field and Encrypted attributes are set for this field. By using the Design Console, you can set the Password Field and Encrypted attributes for a UDF that you create. This would give the newly created UDF the

same properties as the existing Password field. However, the generic technology connector framework treats this field the same as any other text field (with the String data type) and the contents are not encrypted in the Administrative and User Console or database.

- In this release of Oracle Identity Manager, the generic technology connector framework does not provide some of the functionality that the Design Console offers for creating reconciliation rules. Only reconciliation rules of the following pattern can be created:

  ```
  A equals B

  "and"

  C equals D

  "and"

  E equals F
  ```

  For more information about working with reconciliation rules, refer to *Oracle Identity Manager Design Console Guide*.

- While creating a generic technology connector, you cannot specify that the target system requires a remote manager to communicate with the target system. Therefore, a generic technology connector cannot use a remote manager.

- You use the Target Date Format parameter to specify the format in which date values must be sent to the target system during provisioning. Date validation for this parameter does not take place if you enter a date in numeric format. For information about the date formats that you can specify, see the following Web page:

  http://java.sun.com/docs/books/tutorial/i18n/format/simpleDateFormat.html#datepattern

- Scheduled tasks that are not currently running have the `INACTIVE` status. These tasks run at the next specified date and time. Under certain conditions, a scheduled task is automatically assigned the `NONE` status. However, this status change does not affect the functionality of the task, which continues to run at the specified date and time.

- When you import a release 9.0.3 generic technology connector into a release 9.1.0.1 Oracle Identity Manager installation, a non-fatal exception is recorded in the application server log file.

  This occurs only if the connector supports provisioning, regardless of whether or not it supports reconciliation. You can ignore this exception message. No error message is displayed on the Administrative and User Console.

- During a Manage Generic Technology Connector operation, if you change the data type of a field in the OIM - Account data set, then an error is thrown when you click Create on the Step 5: Verify Connector Information page.

27

Using Oracle Identity Manager As a Target System for Provisioning Operations

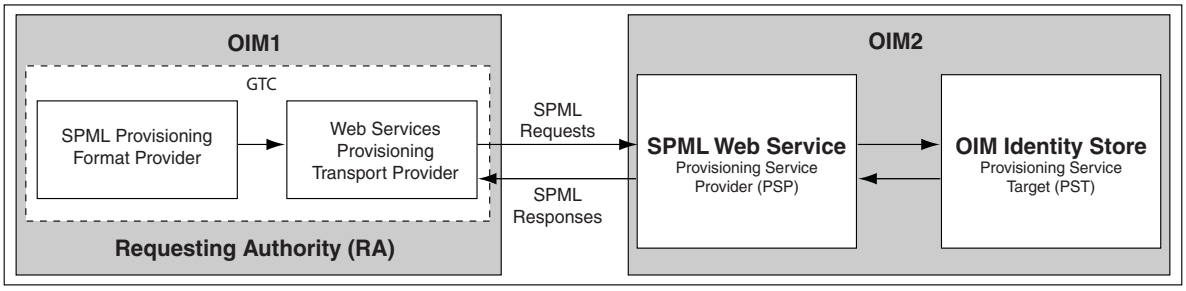
You can create a generic technology connector to perform provisioning operations on a target Oracle Identity Manager installation. In other words, an Oracle Identity Manager installation can be used as a provisioning-only target system for another Oracle Identity Manager installation.

See Also:

- SPML Provisioning Format Provider on page 20-7
- The "SPML Web Service" chapter of *Oracle Identity Manager Tools Reference*

Figure 0–1 illustrates the setup for sending SPML requests to an Oracle Identity Manager installation configured as a target system.

Figure 0–1 Setup for Using Oracle Identity Manager As a Provisioning Target



The following sample scenario illustrates the working of this setup:

OIM1 and OIM2 are two different Oracle Identity Manager installations. On OIM1, you have created a generic technology connector (GTC1) that contains the SPML Provisioning Format Provider and Web Services Provisioning Transport Provider. OIM2 is a target system of OIM1. The SPML Web Service is running on OIM2.

See Also: The "SPML Provisioning Format Provider" section on page 20-7 for information about supported SPML operations

For OIM Users on OIM1, target resource accounts can be created, modified, or deleted on OIM2. When you create, modify, or delete an OIM2 (target resource) account of a user through OIM1, the following sequence of events takes place:

1. The SPML Provisioning Format Provider of GTC1 converts the provisioning operation data into an SPML request and bundles it into a SOAP packet.
2. The Web Services Provisioning Transport Provider of GTC1 sends the SOAP packet to the SPML Web Service of OIM2.
3. The SPML Web Service parses the SPML request and performs the provisioning operation.
4. Because the provisioning operation was successfully performed on OIM2, the SPML Web Service sends an SPML response (indicating success of the operation) back to the Web Services Provisioning Transport Provider.
5. The `psoID` value is extracted from the SPML response by the Web Services Transport provider and passed on to the generic technology connector framework as the ID field value.

To create a generic technology connector for use as the provisioning link to a target Oracle Identity Manager installation, perform the instructions described in the "Using the Administrative and User Console to Create the Generic Technology Connector" section on page 22-3. Steps that are specific to creating this generic technology connector are as follows:

1. On the Step 1: Provide Basic Information page:

   Select the Provisioning option and then select the following providers:

   - Web Services Provisioning Transport Provider
   - SPML Provisioning Format Provider

2. On the Step 2: Specify Parameter Values page:

   Specify values for the run-time and design parameters. While performing this procedure, you need not specify a value for the Target Date Format parameter. This is because the default value of the date format is used.

3. On the Step 3: Modify Connector Configuration page:

   The Web Services Provisioning Transport Provider and SPML Provisioning Format Provider do not have the capability to detect metadata. Therefore, you must manually add fields and create mappings on the Step 3: Modify Connector Configuration page as follows:

   a. Create the following fields in the Provisioning Staging - Account data set. These are mandatory fields.

      – Users.User ID
      – Users.First Name
      – Users.Last Name
      – Organizations.Organization Name
      – Users.Xellerate Type
      – Users.Role
      – Users.Password

      Because you are using the SPML Provisioning Format Provider, the following fields are automatically created in the Provisioning Staging - Account data set as part of metadata detection:

      – containerID

– objectclass

– ID

Note: In the provisioning operation, the value of the `containerID` field takes precedence over the value of the `Organizations.Organization Name` field. If an SPML request sent by the generic technology connector contains values for both the `containerID` and `Organizations.Organization Name` fields, then the value of the `containerID` field is used in the provisioning operation.

If required, you can also create the following fields in the Provisioning Staging data set. These are nonmandatory fields.

– Users.Middle Name

– Users.Status

– Users.Provisioned Date

– Users.Creation Date

– Users.Manager Login

– Users.End Date

– Users.Start Date

b. Create the mappings shown in the following table. The word "recommended" in the heading of the first column is used to indicate that it is not mandatory to use the source fields listed in that column for creating mappings with the fields listed in the second column.

Recommended Source Field in the OIM - User Data Set	Destination Field in the Provisioning Staging - Account Data Set
User ID	Users.User ID
First Name	Users.First Name
Last Name	Users.Last Name
Organization	Organizations.Organization Name
User Type	Users.Xellerate Type
Employee Type	Users.Role
Password	Users.Password

Because you are using the SPML Provisioning Format Provider, the following mappings are created as part of metadata detection.

Source Field in the OIM - Account Data Set	Destination Field in the Provisioning Staging - Account Data Set
containerID This is the recommended source field. You can use any field.	containerID

Source Field in the OIM - Account Data Set	Destination Field in the Provisioning Staging - Account Data Set
objectclass This is the recommended source field. You can use any field.	objectclass
ID	ID

If you add fields from the list of nonmandatory fields given in Step 3.a, then you must create mappings between those fields and the corresponding fields in the OIM data sets.

c. If required, create child data sets for the OIM - Account and Provisioning Staging - Account data sets and then create mappings between corresponding fields of the child data sets.

On the Step 2: Specify Parameter Values page, you specify a value for the ID Attribute for Child Dataset Holding Group Membership Information parameter. You must ensure that a field with the same name as the value you specify is included in the child data set.

See Also: The "SPML Provisioning Format Provider" section on page 20-7 for more information about the ID Attribute for Child Dataset Holding Group Membership Information parameter

After you perform these steps, click **Close** on the Step 3: Modify Connector Configuration page.

4. On the Step 4: Verify Connector Form Names page:

Accept or modify the values displayed on this page.

5. On the Step 5: Verify Connector Information page:

Review the information displayed on this page, and then click **Create**.

28

Connector Objects Created by the Generic Technology Connector Framework

The list of connector objects created by the generic technology connector framework depends on the combination of the Reconciliation and Provisioning options that you select on the Step 1: Basic Information page:

- Both Reconciliation and Provisioning Are Selected
- Only Reconciliation Is Selected
- Only Provisioning Is Selected

Note: Except for the form names, the names of the generic technology connector objects are in the *GTC_NAME*_GTC format, where *GTC_NAME* is the name that you assign to the connector.

For example, if you specify DBTables_conn as the name of a generic technology connector that you create, then all the connector objects (except the forms) are named DBTables_conn_GTC.

0.1 Both Reconciliation and Provisioning Are Selected

The following objects are created when you select both the Provisioning and Reconciliation options on the Step 1: Basic Information page:

- IT resource type

  The parameters of the IT resource type are the run-time parameters of the Format and Transport Providers (for both reconciliation and provisioning) that you select on the first page.

- IT resource

  The IT resource is an instance of the IT resource type. It contains the run-time parameter values of the providers.

- Resource object

  The resource object holds the values of the fields that constitute the Reconciliation Staging parent data set. For each Reconciliation Staging child data set, multivalued reconciliation fields (with corresponding child fields as their attributes) are automatically created.

Note: When you select the trusted source reconciliation option, a trusted resource object is one of the objects automatically created at the end of the connector creation process.

- Parent and child forms

  Parent and child forms are based on the OIM - Account data set and its child data sets, respectively. By default, the names of the forms are the same as the names of their corresponding data sets. On the Step 3: Verify Form Names page, you can change the form names as required.

- Process definition

  The process definition contains the reconciliation field mappings and the system-defined and provisioning-specific process tasks. See "Configuring Provisioning" on page 22-34 for information about the process tasks that are included in the process definition.

- Generic adapter

  The generic adapter contains the code for all the provisioning functions that a generic technology connector performs.

- Scheduled task

  During a reconciliation run, the scheduled task triggers the reconciliation processes in the predefined sequence. The "Configuring Reconciliation" section on page 22-34 provides information about setting up the scheduled task.

- Reconciliation rule

  The reconciliation rule consists of rule elements. A single rule element represents a mapping created between a field of the Reconciliation Staging data set and a field of the OIM - User data set.

- Action rules

  The following are the default action rules created for target resource reconciliation:

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

The following are the default action rules created for trusted source reconciliation:

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

The user group to which the creator of the generic technology connector belongs is made the administrator of the following connector objects that are automatically created during the generic technology connector creation process:

- IT resource
- Resource object (Administrator and Object Authorizer)

- All forms
- Process definition
- Reconciliation fields
- Reconciliation field mappings

0.2 Only Reconciliation Is Selected

See "Both Reconciliation and Provisioning Are Selected" on page 28-1 for the list of objects that are created when you select both the Reconciliation and Provisioning options. From that list, the following objects are ***not*** created when you select only the Reconciliation option on the Step 1: Basic Information page:

- Generic adapter
- Provisioning-specific process tasks

  However, the process definition itself and its constituent system-defined process tasks are created.

0.3 Only Provisioning Is Selected

See "Both Reconciliation and Provisioning Are Selected" on page 28-1 for the list of objects that are created when you select both the Reconciliation and Provisioning options. From that list, the following objects are ***not*** created when you select only the Provisioning option on the Step 1: Basic Information page:

- Scheduled task
- Reconciliation rule
- Reconciliation fields
- Reconciliation field mappings

Part III

Appendixes

Part III contains the following appendix:

- Appendix A, "System Configuration Considerations for Administrators"

A

System Configuration Considerations for Administrators

In the previous release, this appendix described the settings in the Administrative and User Console for configuring functions such as user registration and account creation. From the current release onward, you will find this information in the "Settings for Configuring Administrative and User Console Functions" section of *Oracle Identity Manager Reference*.

Index

A

B

C

D

E

F

G

H

I

L

M

O

P

R

S

T

U

V

W

X