Oracle® Identity Manager

Administrative and User Console Guide

Release 9.0

B32136-01

October 2006

ORACLE®

Oracle Identity Manager Administrative and User Console Guide, Release 9.0

B32136-01

Primary Author: Don Gosselin

Contents

5 My Resources

6 Requests

7 To-Do List

8 Users

9 Organizations

10 User Groups

11 Access Policies

12 Resource Management

A Understanding Attestation

List of Figures

Preface

This preface introduces you to the *Oracle Identity Manager Administrative and User Console Guide* discussing the intended audience and conventions of this document. It also includes a list of related Oracle documents.

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

The *Oracle Identity Manager Administrative and User Console Guide* is intended for Database Administrators, System Administrators, and developers.

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

This guide assumes that you have read and understood the following documents:

For more information, see the following documents in the Oracle Identity Manager documentation set:

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0 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.

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 (group memberships, e-mail address, and so on).
- 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 question and answer (Q&A).
- Set up your user proxy.
- View and manage your pending requests, if you are the authorized approver.

In addition, depending on your privileges 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 provisioned.
- Create requests for resources for any users you manage.
- Complete draft requests for resources for any users you may manage.
- Approve the provisioning of resources for other users.
- Respond to request for more information.

The rest of this manual describes the actions you can perform in Oracle Identity Manager. The following topics are discussed:

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

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

See Also:

- *Oracle Identity Manager Administrative and User Console Customization Guide* for information on how to customize Oracle Identity Manager Administrative and User Console
- *Oracle Identity Manager Globalization Guide* for information on how to globalize Oracle Identity Manager Administrative and User Console

Understanding User Roles and Capabilities

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

Table 1–1 User Roles and Capabilities

Role	What they can do
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.

Overview of the Resource Model

Oracle Identity Manager allows resources to be requested and 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 that you are given on that resource are governed by a provisioning processes that an Oracle Identity Manager Administrator defines. Access to a resource may be provisioned uniformly for all users. Or, Access may be provisioned in a unique fashion, based on variables such as the following:

- Your role, for example, administrator, accountant
- Your location
- Your employment status, for example, full time, 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 Microsoft Exchange application and that resource was successfully provisioned to you, you can log in to that application using the user ID and password, if one was required, established for you by Oracle Identity Manager

Oracle Identity Manager controls the provisioning of resources using processes and the 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.

Approval Processes

An approval process determines if a resource is to be approved or not for provisioning to one or more users or organizations for whom it was 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, he or she can view all tasks in the request. If you are an approver for a request, the request ID appears when you click the **Pending Approvals** link under **To-Do List.**

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

Provisioning Processes

A provisioning process is the process used to actually provision the resource to one or more users or organizations for whom it was 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

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

This chapter discussed the following topics:

Creating an Oracle Identity Manager Account

If you do not already have account in Oracle Identity Manager, you need to create one. A user ID cannot include the following characters:

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

Depending on how your system is configured, you may need to contact your manager to have them create an account for you.

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, write down the Request ID after submitting your request. You need the request ID to track the status of your request.

To create an account for yourself:

1. Access your corporate portal link to Oracle Identity Manager.

   The Oracle Identity Manager landing page appears.

2. From the landing page for Oracle Identity Manager, find the **Self-Register** label in the left navigation pane and click **Create Request**.

   The User Self-Registration page appears.

3. Enter your data.

   Required information is marked with an asterisk (*). Be sure to select and specify answers to password challenge questions if your system requires them. Depending on how your system administrator configured Oracle Identity Manager, you may be required to specify answers to a number of challenge questions to reset your password when you forget it.

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. Write down the Request ID after submitting your request. You need the request ID to track the status of your request.

   A link to the request appears.

5. If your request requires an approval, on the Oracle Identity Manager landing page, click the **Track Request** option under **Self-Register** in the left navigation pane.

   The Track Self-Registration request page appears. You can check the status of your request on this page by entering the numeric ID of the request.

Changing Your Password

If you have forgotten your Oracle Identity Manager password, you can contact your system administrator to have your account unlocked, or you can reset it from a page where you are prompted to answer several validation questions. If you supply the correct answers to these questions, Oracle Identity Manager enables you to change your password.

You can reset your password even if you exceed the maximum number of login retry attempts, and your Oracle Identity Manager account is locked to prevent further attempts at login. However, if you exceed the maximum number of attempts to correctly answer your challenge questions, your account is locked and can only be unlocked by an Oracle Identity Manager system administrator.

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

To reset a lost password:

1. Access your corporate portal link to Oracle Identity Manager.

   The Oracle Identity Manager landing page appears.

2. From the landing page for Oracle Identity Manager, find the **Help** label in the left navigation pane and click Forgot Password?

   The Verify User ID page appears.

3. On the Verify UserID page, enter your ID in the **User ID** field and click **OK**.

   The **Change Password** page appears.

4. Answer the questions on this page.

   The questions that appear on this page and the answers are specified in your account options. You select these questions and answers the first time you log in to the Oracle Identity Manager Administrative and User Console.

5. Supply the correct answers to the password challenge questions, enter your new password in both fields, and click **Submit**.

Tracking a Self-Registration Request

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 Oracle Identity Manager.

   The Oracle Identity Manager landing page appears.

2. In the left navigation pane, click **Track Request** under **Self-Registe**r.

   The Track Self-Registration page appears.

3. On the Track Self-Registration page, enter the ID of the request associated with your self-registration in the **Request ID** field.

4. Click **Track Request**.

   Oracle Identity Manager displays the details regarding the self-registration request status.

Logging In to the Administrative and User Console

Before logging in to the Oracle Identity Manager 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 an Oracle Identity Manager Account" 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 link to Oracle Identity Manager.
2. Enter your User ID and Password in the **Oracle Identity Manager login** page.
3. Click **Login**.

Logging Out of the Administrative and User Console

You may be logged out of Oracle Identity Manager due automatically to inactivity after a specific period of time. You can also log out if you are working in a non-single sign-on environment.

To log out of the Administrative and User Console in a non-single sign-on environment:

1. Click **Logout**.

   A confirmation message appears.

2. Click **Logout** or **Cancel**.

3

Using Oracle Identity Manager

This section describes how to use the main features of the Oracle Identity Manager Administrative and User Console. It discusses the following topics:

- Searching in Oracle Identity Manager
- Understanding Special User interface Behavior

Searching in Oracle Identity Manager

Many fields in Oracle Identity Manager pages have lookup capabilities. You use these capabilities when you need 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 pre-defined menu choices. Others provide full search capabilities, also referred to as a query function.

This rest of this section discusses the following topics:

- Constructing a Search (or Query)
- Using Wildcards
- Understanding Search Behavior

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 only remember a user's first name, enter that and leave the other fields blank. Oracle Identity Manager displays all user records that have the same first name as the one you entered.

If you leave all fields blank prior to conducting a search, Oracle Identity Manager displays all records of that type. To restart a search, click **Clear**. Some screens also provide a **Cancel** button that you can click to cancel a search.

Note: Searches in Oracle Identity Manager are case insensitive. For example, you can enter "RAJA" or "raja" to search for a user named Raja.

Using Wildcards

In addition to entering data in fields to limit the records retrieved by your search, you can enter a wildcard characters in addition to the values that you enter in a particular search field. The wildcard causes Oracle Identity Manager to further filter your 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 b* in the **User ID** field and execute a search, Oracle Identity Manager displays all users whose User ID begins with the letter B, for example, bsmith, bobj, barbarak, and so on. If the asterisk is placed in the middle of a search value, as in j*n, Oracle Identity Manager displays all records that begin with j and end with n, for example, john, joan, johann, and so on. If you place the asterisk at the beginning of the search value, as in *A, you retrieve all records that end in A, for example, laura, maria, and so on.

Understanding Search Behavior

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 search while creating or tracking a request, Oracle Identity Manager only shows users 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, Oracle Identity Manager displays all users with a first name of John, who work in the NY office and who are managed by you.

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

Understanding Special User interface Behavior

The following sections describe how you can configure the Administrative and User Console to meet your data display requirements:

- Trancating Text Entries
- Displaying Process Forms with Child Tables

Trancating Text Entries

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

To customize a field to show the entire entry name:

1. Find the XellerateFull.ear file.
2. In this file, find the xlWebApp.war file.
3. Find the xlWebAdmin.properties file in the following directory:

   XL_HOME/xellerate/webapp/precompiled/jsp-temp/WEB-INF/classes
4. Modify the value of the `global.property.tableColumnSize` property in the xlWebAdmin.properties file.

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.

Displaying Process Forms with Child Tables

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

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

- When you navigate to **User Detail**, in the Resource Profile and click the **Edit** or **View** links for the **Resource and Process Form**.
- When you use the **User Direct Provisioning Wizard, Step 3** through **Step 6**.
- When you navigate to **Organization Detail,** in the Resource Profile and click the Edit or View links for the **Resource and Process Form**.
- When you use the **Organization Direct Provisioning Wizard, Step 3** through **Step 6**.
- When you navigate to **Resource Detail**, in the Organizations Associated with this Resource, and click the Edit or View links for the Resource and Process Form.

To display a child table with more than 10 columns:

1. Find the xlWebAdmin.properties file in the following directory:

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

2. Modify the value of `global.property.NumberOfChildTableColumns` in the `xlWebAdmin.properties` file.

   The default is 10 columns. You can change it to the desired number.

4

My Account

This section describes how to access and manage your Oracle Identity Manager account.

This chapter discusses the following topics:

Viewing and Modifying Your Account Profile

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

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

To view and edit your account:

1. Log in to Oracle Identity Manager.

   The **Welcome to Oracle Identity Manager** page appears.

2. In the left navigation pane, click **My Account**., then click **Account Profile**.

3. In the Account Profile page, click the **Modify Account Profile** button.

   Oracle Identity Manager displays the account information.

4. Make the desired changes and click **Save Profile**.

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

   Oracle Identity Manager stores the request for auditing purposes.

Changing Your Password

You can change your Oracle Identity Manager password. 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**.

   The My Account menu expands.

2. Click **Change Password**.

   The **Change Password** page appears.

3. Enter your current password in the **Old Password** field, then enter your new password and confirm that password.

4. Click **Save**.

   If your password satisfies system-defined criteria, your password is changed.

Specifying Questions and Answers for Password Change and Retrieval

Oracle Identity Manager enables you to select verification questions and the answers to these questions. You configure challenge questions and answers the first time you log in to your Oracle Identity Manager account. These questions are used to verify your identity if you have forgotten your password and need to reset it, or if you want to change your password.

Your Oracle Identity Manager system administrator determines number of questions you must answer and the list of potential questions from which you may select.

You can change your challenge questions and the answers.

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 Question page appears.

4. Select your challenge questions, ensuring that you select at least the minimum number of questions, then click **Select**.

   The **Provide Challenge Answers** page appears.

5. Enter an answer for each question listed.

   Be sure to supply answers that you can easily remember.

6. Click **Save**.

7. Click **OK** to confirm your answers.

   If you forget your password or when you want to reset it, you are presented with the questions, and you must provide the answers, that you selected in the preceding steps.

Delegating Your Responsibilities to a Proxy

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

When the proxy user logs into Oracle Identity Manager, the **Home** page displays the user for whom the logged in user is a proxy. Tasks that would be normally be assigned to the user are displayed in the proxy user's **Pending Request** list. See the section on Pending Requests for more information.

To designate a proxy users:

1. In the left navigation pane, click **My Account**, then click **My Proxy.**

   The **Proxy Details** page appears.

2. If no proxy is defined at this time, click **Assign** to delegate a user.

   The **Assign Proxy** page appears.

3. In the Proxy Name field, select **Your Manager** or **Other User**.

   By default the Manager 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 appears. It displays all the user names that are available for defining a proxy user.

4. Select the **User ID** radio button to define your proxy user, then click **Select**.

   The **Assign Proxy** page appears with the selected user ID.

5. In the **Start Date** field, click the calendar icon and highlight the date that you want to activate the proxy user.

6. In the **End Date** field click the calendar icon and highlight the date that you want the proxy user to be deactivated.

7. Click **Assign**.

   If the end date is not specified, the proxy assignment is active until you remove it. A **Confirmation** page appears with the selected **User ID** as defined for the proxy user.

8. If information in the Confirmation page is correct, click **Assign**.

   The **Proxy Details** page appears 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

My 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 Your 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 appears.

   This page displays a table that contains information about provisioned resources associated with this user. It shows:

Field	Description
Resource Name	This is the name of the resource being provisioned.
Date Provisioned	This is the date when the resource was provisioned.
Status	This is the status (state) of the resource.

2. To request a new resource for yourself, on this page click **Request New Resources**.

   The Create a Request to Provision Resource(s) - Step 1: Provision Resources page appears.

3. To select the resources you want to request, check the **Resource Name** check box, then click **Add** to add them to the **Selected** list.

   Click **Remove** to delete the resource from the Selected list.

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

   If a resource you are requesting has a resource form associated with it, then the Create a Request to Provision Resource(s) - Step 2: Provide Resource Data page appears. Otherwise, the Create a Request to Provision Resource(s) - Step 3: Verify Information page appears.

4. If the Create a Request to Provision Resource(s) - Step 2: Provide Resource Data page appears, enter the required data for the requested resource and click **Continue**.

   The Create a Request to Provision Resource(s) - Step 3: Verify Information page appears.

5. On the Create a Request to Provision Resource(s) - Step 3: Verify Information page, enter data as described in the following tables.

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

   The **Resources Selected** table displays the following information:

Field	Description
Resource Name	This is the name of the resource you are requesting/provisioning.
Details	This is any additional detailed information about the resource.

6. To add a comment, click the **add a comment** link.

   The **Add Request Comment** page appears.

7. After entering your comment in the Comment field, click **Add Comment** to insert your comment in your resource request.

   Click **Clear** to erase the text in the Comment field or **Close** to dismiss this page.

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

8. To modify this resource request, either click the **Change** link to change the resource or add another comment by clicking on the **Add** link.

   The appropriate page appears.

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

   The **Request Submitted** page appears. Otherwise, click **Schedule for Later** to activate at a later time.

   This page shows the following information:

Field	Description
Status	This is the status (state) of the request.
Requester	This is the name of the person who made the request.
Action	This is the action taken for this request.
Date	This is when the request was executed.

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

    If you click **Scheduled 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.

The **Schedule for Later** page appears.

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

Viewing Your 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 Request**.

   The **My Request** page appears.

   This page defaults to the **Raised by me** option. You can search for the request using the search syntax for a specific target. Use the drop-down menu to select one of the following search criteria:

   - Request ID (default)
   - Requester

   Enter a value to match this search criteria. To use the **Request Type** criterion, select the corresponding value from the **Request Type** box.

   The **Results** table displays the following information:

Field	Description
Request ID	The identification number of the request.
Request Type	The type of the request.
Requester	The name of the person who made the request. **Note:** The Requester information is not displayed when the **Raised by me** option is selected.
Request Preview	The summary of the user and the associated resource for this request.

2. To view the list of request made by another user (a proxy user) for you, select the **Raised for me** option.

   The **My Request** page appears.

   The table on this page is similar to the **Raised by me** page, but it displays resources that were raised on your behalf.

   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 add resources to users or organizations. A user who is entitled to be provisioned with the resource will see the request when they log in.

   When you select the **Raised by me** option, you are the requester. No **Requester** column is displayed for this option. You will see all your requests under this option.

Requesting New Resources

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

To make a new request for resources:

1. In the left navigation pane, click **My Resources**, then click **Request New Resources**.

   The Create a Request To Provision Resource(s) page appears.

2. To select the resources you want to request, check the **Resource Name** check box, then click the **Add** button to add them to the **Selected** list.

   Use the **Remove** button to delete the resource from the **Selected** list.

3. Click **Continue**.

   The Create a Request To Provision Resource(s) – Step 2: Provide Resource Data page appears. This page displays the resource object for the target user.

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

   Click **Continue** to provide additional information about the resource object you wish to provision. Otherwise, click **Back** or **Exit**.

   The Create a Request To Provision Resource(s) – Step 2: Provide Resource Data page appears. This page is for supplying additional information for this resource object.

5. Enter the additional information in the field, and click **Continue**, otherwise click **Back** or **Exit**.

   The Create a Request To Provision Resource(s) – Step 3: Verify Information page appears.

6. On this page, the **Users Selected** table on this 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.

   The **Resources Selected** table displays the following information:

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

7. To add a comment if desired, click the **add a comment** link.

   The **Add Request Comment** page appears.

8. After entering your comment in the Comment field, click **Add Comment** to insert your comment with your resource request. Otherwise, you can click **Clear** to erase the text in the Comment field or **Close** to dismiss this page.

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

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

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

    The **Request Submitted** page appears.

    This page shows the following information:

Field	Description
Status	The status (state) of the request.
Requester	The name of the person who made the request.
Action	The action taken for this request.
Date	This is when the request was executed.

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

    The **Schedule for Later** page appears.

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

6

Requests

Oracle Identity Manager enables you to create and track requests for resources that you have requested for users and organizations. If you are 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 the task. If you are both an approval and an administrator, you can to 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.

Creating and Managing Requests

Oracle Identity Manager enables you to create and manage requests for provisioning resources to yourself, other users, and organizations.

If you are an Oracle Identity Manager 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, Oracle Identity Manager does not require you to be an administrator to request it for yourself.
- If the resource is configured as allowed for all users, Oracle Identity Manager does not require you to be an administrator to request it for another user.

If a resource is not set as allowable for all users, 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 may be requested for you, contact your Oracle Identity Manager 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

The **Resource** option lets you choose the following options:

- **Grant Resources**: enables resources to be provisioned to a target.
- **Disable Resources**: temporarily disables resources.
- **Re-enable Resources**: after the resources are disabled, you can re-enable resources.
- **Revoke Resources**: deletes resources permanently. You cannot re-enable a resource back after you have revoked it.

This section discusses the following topics:

Granting Resources

The following procedure describes how to grant provisioning of a resource. You can provision the same resource multiple times if the resource is configured for this usage.

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

To grant a resource request:

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

   The Make a Request page appears. This page defaults to the **Grant Resource** option. Use this option to grant a resource to a specific user or organization.

2. Click **Continue**.

   The Create a Request To Provision Resource(s) – Step 1: Select Type page appears.

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

   Select the **Organization** option to provision a resource to one or many organization(s).

   Click **Continue**.

   If you selected the **Users** option, the Create a Request To Provision Resource(s) – Step 2: Select User(s) page appears.

   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 **Users** checkbox then click **Add** to place the user name or names in the **Selected** list.

   Use the **Remove** button to delete any user or users 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 using the User Defined Field Definition form for **Form Name=Requests**. For more information, see the *Oracle Identity Manager Design Console Guide*.

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

   The Create a Request To Provision Resource(s) – Step 3: Provide Resource page appears.

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

   Use the **Remove** button to delete any user(s) 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**.

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

   The Create a Request To Provision Resource(s) – Step 4: Provide Resource Data page appears. This page displays information about the resource and the user for this request.

6. If the information on this page is correct, 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 Create a Request To Provision Resource(s) – Step 5: Verify Information page appears.

8. To add a comment if desired, click the **Add a comment** link.

   The **Add Request Comment** page appears.

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

   Or, click **Clear** to erase the text in the Comment field or **Close** to dismiss 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 appears.

    This page shows the following information:

Field	Description
Status	The status (state) of the request
Requester	The name of the person who made the request

Field	Description
Action	The action taken for this request
Date	When the request was executed

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

    You can only specify a date that is later than today's date. The **Schedule for Later** page appears.

    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**.

Disabling Resources

The following procedure describes how to disable a request for the provisioning of a resource or resources.

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

To disable a request:

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

   The **Make a Request** page appears.

2. Select the **Disable Resource** radio button, and click **Continue**.

   The Create a Request To Disable Resourc(es) – Step 1: Select Type page appears.

   This page lets you select one of the following options:

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

     In this example, the Users option is selected.

3. Click **Continue**.

   The Create a Request To Disable Resources – Step 2: Select User(s) page appears.

4. Select the user name checkboxes, then click **Add** to place the user names in the **Selected** list.

   Use the **Remove** button to delete any user or users 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 done, click **Continue**

The Create a Request To Disable Resources – Step 3: Provide Resources page appears.

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

   Use the **Remove** button to delete any resources in the **Selected** list.

6. Click **Continue**.

   If multiple instances of a resource instance are provisioned for the user, the Create a Request To Disable Resources – Step 4: Resolution page appears. Otherwise, the Create a Request To Disable Resources – Step 5: Verify Information page appears.

7. If the Create a Request To Disable Resources – Step 4: Resolution page appears, select the resource instance you want to disable, then click **Continue**.

   The Create a Request To Disable Resources – Step 5: Verify Information page appears.

8. The Create a Request To Disable Resources – 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
Resource Name	The name of the resource you are requesting or provisioning
Details	Any additional detailed information about the resource

9. To add a comment, click the **add a comment** link.

   The **Add Request Comment** page appears.

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

    Click **Clear** to erase the text in the **Comment** field. Click **Close** to dismiss this page.

    The **Verify Information** page displays the added comment if you added one.

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

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

    The **Request Submitted** page appears.

    This page shows the following information:

Field	Description
Status	The status (state) of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	When the request was executed

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

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

Re-enabling Resources

You can re-enable a resource after you disable it. You cannot re-enable a revoked resource.

> **Note:** Since re-enabling resources for an organization is similar to re-enabling resources for a user, the following procedure only includes the steps for re-enabling resources for a user.

To create a request to re-enable a resource:

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

   The **Make a Request** page appears.

   This page defaults to the **Grant Resource** option.

2. Select the **Re-enable Resource** option to provide access to resources that were earlier disabled for this user, and click **Continue**.

   The Create a Request To Re-enable Resource(s) – Step 1: Select Type page appears.

3. Click **Users** to re-enable resources that were disabled for one or many users.

   Otherwise, select **Organization** to re-enable resources that were disabled for one or many organization(s). In this example, the **Users** option is selected.

4. Click **Continue**.

   The Create a Request To Re-enable Resource(s) – Step 2: Select User(s) page appears.

   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** checkbox and click **Add** to place the user name or names in the **Selected** list, or click the **Remove** button to delete users in the **Selected** list.

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

   The Create a Request To Re-enable Resource(s) – Step 3: Provide Resource page appears.

6. Select the resource name checkbox, then click **Add** to place the resource name in the Selected list, or use the **Remove** button to delete users from the **Selected** list, and click **Continue**.

   If multiple instances of a resource instance are provisioned for the user, the Create a Request To Re-enable Resources – Step 4: Resolution page appears. Otherwise,

the Create a Request To Re-enable Resources – Step 5: Verify Information page appears.

7. If the Create a Request To Re-enable Resources – Step 4: Resolution page appears, select the resource instance you want to disable, and then click **Continue**.

   The Create a Request To Re-enable Resources – Step 5: Verify Information page appears.

8. To add a comment, click the **add a comment** link.

   The **Add Request Comment** page appears.

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 erase the text in the **Comment** field or **Close** to dismiss this page.

10. Verify the information on the Create a Request To Re-enable Resources – Step 5: Verify Information page, then click **Submit Now** to make the request active.

    If you click **Submit Now**, the **Request Submitted** page appears.

    This page shows the following information:

Field	Description
Status	The status (state) of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	When the request was executed

    If you wish to view the details of this request, click the **Request ID** link. The Request Details page appears. For more information on this page, see the Track (Resources) section.

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

    The Schedule for Later page appears.

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

Revoking Resources

Revocation is a permanent operation.

To create a request to revoke access to a resource:

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

   The **Make a Request** page appears.

2. Select the **Revoke Resource** radio button, then click **Continue**.

   The Create a Request To Revoke Resources – Step 1: Select Type page appears.

   This page lets you select one of the following options:

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

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

3. Click **Continue**.

   The Create a Request To Revoke Resources – Step 2: Select User(s) page appears.

4. Select the user's name(s) checkbox then click **Add** to place the user names in the **Selected** list.

   Use the **Remove** button to delete any users in the **Selected** list. then click **Continue**.

   The Create a Request To Revoke Resources – Step 3: Provide Resources page appears.

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

   Use the **Remove** button to delete any resources in the **Selected** list, then click **Continue**.

   If multiple instances of a resource instance are provisioned for the user, the Create a Request To Revoke Resources – Step 4: Resolution page appears. Otherwise, the Create a Request To Revoke Resources – Step 5: Verify Information page appears.

6. If the Create a Request To Revoke Resources – Step 4: Resolution page appears, select the resource instance you want to disable, and then click **Continue**.

   The Create a Request To Revoke Resources – Step 5: Verify Information page appears.

7. The Create a Request To Revoke Resources – 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	Any additional detailed information about the resource

8. To add a comment, click the **add a comment** link.

   The **Add Request Comment** page appears.

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

   The **Verify Information** page displays the added comment.

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

To modify the information for this resource request, click the **Change** link to change the resource or click the **Add** link to add another comment. These links jump to the appropriate page.

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

    The **Request Submitted** page appears. This page shows the following information:

Field	Description
Status	The status (state) of the request
Requester	The name of the person who made the request
Action	The action taken for this request
Date	When the request was 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 appears. Use the calendar icon to define a date to activate your request, and then click **Submit**.

Tracking Requests

Depending on the privileges that have been assigned to you in Oracle Identity Manager, you may be able to view requests for resources. Additionally, you may be able to 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 tasks 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

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 appears. To locate the request you want to track, you can search for existing requests according to the options listed as radio buttons. You can only select 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, Oracle Identity Manager displays all requests.

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

Field	Description
User ID	Enables you to track requests that were created for yourself or another user. Select **Self** or **Other**. If you select **Other**, you must click **Find User ID** and specify the user associated with the requests you wish to track. You can use the 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	Enables you to 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 wildcard character (*) search for requests beginning or ending with specific characters or numbers.
Creation Date	Enables you to track requests by date that they were created. Select this option, then enter the start and end dates for the range on which you wish to query. Oracle Identity Manager then displays all requests created between those dates.
Resource Name	Enables you to track requests according to the resources to be provisioned (that is, the resources specified on the request). Select this option, and then enter the name of the resource. You can use a wildcard character (for example, *) to perform searches for requests containing a resource name that begins or ends with specific characters.
Status	Enables you to track requests according to the request's status, 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.

2. Click **Search**.

   Oracle Identity Manager displays all requests that match the criteria you entered and the number of requests that match the query. If your query has retrieved several pages of requests, use the **First**, **Previous**, and **Next** links to navigate 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 appears.

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

Viewing Approval Details

This page displays all approvals for this 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 Task(s)** page appears. 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	This request is assigned to the user or proxy user. It can also be assigned to a user group or proxy group.
Action	The **Action** column has a checkbox 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 appears that displays the tasks and **Confirm** and **Cancel** buttons. If you click Re-assign, the console displays a list of all the users that you (or the logged in user) have permission to see to whom you can reassign the task. This page has a radio button that, when selected, lists all the groups that you (or the logged in user) can see to whom the task can be re-assigned.

Viewing Provisioning Details

You can view provisioning tasks by User, Organization, or Resource depending on whether the request was created for a user or 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 **Provisioning Details** option from the **Additional Details** box.

   The **Provisioning Task**(s) page appears. The **Provisioning Details** field shows all tasks associated with the provisioning processes.
3. Select the desired radio button to display the information you want to view.

Viewing by User/Organization

When selecting the **User/Organization** button, the page will display all the tasks for 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.

The information table shows the following:

Field	Description
Resource Name	This is the name of the resource object to be provisioned.
Resource Status	Current Status of the resource request.
Process Instance Name	This name is either an Approval process or a Provisioning process.
Data	This text is a link to the Process Form for this user.
Descriptive Data	This is a number that uniquely identifies the process.

Viewing by Resource

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

The information table shows the following:

Field	Description
User/Organization	This is the name of the user or organization that has been provisioned with this resource object.
Resource Status	Current Status of the resource request.
Process Instance Name	This name of the provisioning process.
Data	This text is a link to the Process Form for this user.
Descriptive Data	This is a number that uniquely identifies the process.

Viewing Request Comments

A request is viewed by any user with view privileges. 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 **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 the **Add a comment** link. If there is a comment added to this request, the Request Details >> Request Comments page appears with the comment.

   This page displays a table with the following information:

Field	Description
Comment	This is the actual comment that was added.
Date	The date that the comment was added.
Add By	This user name that is logged into Oracle Identity Manager.

Viewing Request Status History

Request 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. Until the request is completed or rejected, there are many steps and actions that needs to be executed, such as a user manual action or a system action.

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 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 in the following table:

Field	Description
Status	Current status of the resource request.
Date	The date that the request was created.
Create by	The name that created this request

7

To-Do List

A To-Do list is a list of tasks within a process. The processes for approving requests and their associated resources and making them available for provisioning consist of tasks.

Before resources in a request can be provisioned to target users, other users who are assigned as approvers for tasks must provide approval. If you have set Oracle Identity Manager to require approvals for self-registration, the approval tasks associated with user self-registration requests also appear and require action by an assigned approver in order to complete the registration process.

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 tasks in a request, you can view all tasks in the request but only approve those assigned to you. You can also view pending requests for users who you manage.

You define a process using the Process Definition form of the Oracle Identity Manager Design Console. When defining the process, you specify a type of either **Provisioning** or **Approval**. 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 users.

This rest of this chapter discusses the following topics:

Reviewing Pending Approvals

You use the Pending Approvals page to view and complete the tasks that are assigned to you and view requests that are assigned to users that you manage.

To review pending approvals:

1. Click **Pending Approvals** under **To-Do List**.

   The Pending Approval page appears, with a list of all requests that contain one or more tasks for which you are an approver. By default, the page opens with pending request(s) 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** radio button.

   The page displays the appropriate pending requests.

You can also query for specific requests by using the **Search** criteria drop-down menu. It includes:

- Request ID
- Requester
- Assign To

The **Results** table has a description of the search criteria. Enter the appropriate value in the corresponding field. To use the **Request Type** criterion, select the corresponding value from the **Request Type** box. The **Results** table displays the following fields:

Field	Description
Request ID	This is the request's unique, system-generated identification number.
Request Type	The Request Type can be: ■ Add/Revoke/Enable/Disable Resources for Users or Organizations ■ Enable/Disable/Delete/Create/Modify Entity
Requester	This is the user who created the request.
Request Preview	This is a summary of the request. The information being displayed includes the User ID or Organization and the resource.
Assign To	This the user assigned to approve this request.
Approve/Deny	Use this field to select the desired request to either approve or deny it.
Reassign	Use this field to select the desired request to be Reassigned to another user or user group.

3. To approve a pending request, select the desired checkbox in the **Approve/Deny** column, then click **Approve**.

   The request ID is removed from the **Results** table.

   To deny a pending request, select the4 desired checkbox in the **Approve/Deny** column, then click **Deny**. The request ID is removed from the **Results** table.

4. To reassign a pending request, select the desired checkbox in the **Re-Assign** column, then click **Re-Assign**.

   The **Re-Assign Pending Approvals** page appears.

5. Select the checkbox for the user or group you want to re-assign this request to, then click **Re-Assign**.

   The Confirm page appears.

Managing Open Tasks

The **Open Tasks** option lists tasks that are defined for a provisioning process. The Open Tasks option displays all open provisioning tasks that are assigned to you or a person that you manage. Use the **Open Tasks** option to re-try a task if it has a status of rejection, re-assign a provisioning task to another user, or set a response for a provisioning task. This section describes the following tasks:

- Viewing Open Tasks

Viewing Open Tasks

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

To view the open tasks:

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

   The **Open Tasks page** appears.

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 the corresponding field. To use the **Open Task Type** and **Object Type** criteria, select the value from the corresponding box. Then click **Go**. The **Results** table displays the following information about the provisioning task:

Field	Description
Task Name	This is the name of the task that you have defined in the Process Definition form for this resource name(s).
Task Status	Current status of the resource task.
Resource Name	The name of the resource associated with this provisioning task.
Resource Type	The type of resource defined in the Resource Object form. There are three categories for resource type: Generic, System, and Application
Date Assigned	The date that the provisioning task was assigned.
Assigned To	The user name of the user who the provisioning task is assigned to.
Re-Try	If this checkbox is activated, it indicates that the status of the provisioning task is Rejected. Use this checkbox to Re-Try the provisioning task.
Re-Assign	Use this checkbox to assign this provisioning task to another user or user group.
Set Response	Use this checkbox to set a response for this provisioning task.
Complete Manually	Use this checkbox to manually complete the provisioning task.

Reassigning an Open Task

You can assign an open task to another user.

To reassign an open task:

1. Select the desired provisioning task name checkboxes, then click **Re-Assign**.

The Re-Assign Open Tasks page appears

2. Select a User ID or Group ID and then click **Re-Assign**.

   Only one user or group can be selected.

   A Confirmation page appears. This page displays the User ID (first name and last name) in the first sentence and the provisioning task as a bullet item.

3. Click **Confirm Re-assign Tasks**, or click **Cancel**.

   The **Open Tasks** page appears.The provisioning task that you have re-assigned is no longer in the **Results** table.

Setting a Response to an Open Task

To set a response to an open task:

1. Select one or more provisioning task name checkboxes, then click **Set Response.**

   The **Specify Task Responses** page appears.

2. Select a response for the provisioning task, 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 appears. The provisioning task that you have set response for no longer appears in the **Results** table.

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

Viewing Attestation Requests

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

To view attestation requests:

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

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

Column	Description
Process Names	The name of the process.
Process Code	The code for the process.
Data Type	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 was assigned by the attestation process.
Current Request	Specifies the date and time on which the attestation task was 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 needs to 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:

Column	Description
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	Stores the date and time when this entitlement was last attested
Comments	Comments that you entered for the entitlement
Actions	Contains **Certify**, **Reject**, **Decline**, and **Delegate** buttons that you select to specify the action for the entitlement

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

Saving Attestation Actions

The following procedure describes how to save an attestation action.

> **Note:** Saving does not submit the attestations. To submit attestations, you must follow the procedures in"Submitting Attestations" on page 7-6.

To save an attestation action:

1. Follow the procedures in "Viewing Attestation Requests" on page 7-4 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 Attestation Request >> Save Actions page appears and displays a table listing the entitlements in the current attestation request for which you have selected an action. Any entitlement for which you selected an action of **Delegate** also allows you to search for a reviewer in the **Delegated Reviewer** field.

3. On the Attestation Request >> 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**.

Updating Comments and Delegations

To update an attestation request:

1. Follow the procedures in "Viewing Attestation Requests" on page 7-4 to select the attestation process that you want to update.
2. Follow the procedures in "Saving Attestation Actions" on page 7-5 to enter comments or select delegated reviewers for any entitlements.
3. Click **Update Existing Comments & Delegation Information**.

   The Attestation Request >> Update Comments and Delegates page appears and displays a table listing the entitlements in the current attestation request for which you have selected an action.
4. In the Attestation Request >> Update Comments and Delegates page, select the check boxes next to the entitlements that you want to update, enter any new comments, and select a delegated reviewer.
5. Click **Save**.

Submitting Attestations

The following procedure describes how to submit an attestation.

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

To submit an attestation:

1. Follow the procedures in "Viewing Attestation Requests" on page 7-4 to select the attestation process that you want to submit.
2. Follow the procedures in "Saving Attestation Actions" on page 7-5 to enter comments or select delegated reviewers for any entitlements.
3. On the Attestation Request page, click **Submit Attestation**.

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

8

Users

Administrators can create and manage user records, for example, Oracle Identity Manager accounts, that your employee require.

Even if you allow users to self-register, you may still want to provide 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:

Creating Users

To create a user account:

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

   The Create User page appears.

2. Enter the data required for user registration.

   Required fields are marked with an asterisk.

3. In the Organization field, click the magnifying glass icon to display the Organization lookup dialog.

4. Select an organization from the list and click **Select.**

5. Click **Create User**.

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

   If you select any of the options in the additional details box, you will see limited information since you have just created the user. When viewing the details of each search criteria, you can add or assign the user with the desired resource.

In 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 they are locked out due to exceeing a login re-try limit
- **Delete:** Delete the user account
- **Change Password:** Change the current password

Editing the User Profile

To edit a user profile:

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

   The Manage User page appears.

2. In the Manage User page, select one or more attributes from the menus, and enter search criteria, including an asterisk (*) if you need a wild card, in the text box next to the menu.

   To use the **Employee Type** and **Status** search criteria, select values from the corresponding boxes.

3. Click **Search User**.

   A list of users appears.

4. Click the field for the user whose information you want to edit.

   The User Detail page appears.

5. Click Edit.

6. Edit the data for the user and click **Save**, or click **Cancel Edit**.

Disabling the User

Disabling a user prevents them from being provisioned. 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**, then click Manage.

   The Manage User page appears.

2. In the Manage User page, select one or more attributes from the menus, and enter search criteria, including an asterisk (*) if you need a wild card, in the text box next to the menu.

   To use the **Employee Type** and **Status** search criteria, select values from the corresponding boxes.

3. Click **Search User**.

   A list of users appears.

4. Click the checkbox for the user whose information you want to disable, then click Disable.

Changing the User's Password

You can reset user passwords.

To change a password:

1. Click **Change Password**.

   The **Change Password** page appears.

2. Enter a new password and confirm.

3. Click **Save Password**, or click **Cancel.**

Managing Users

You enable, disable, provision resources to, and unlock user accounts. A user account must be disabled to be eligible for enabling. Only locked accounts can be unlocked. An account becomes locked if a user has exceeded the maximum number of login retry attempts. After a configured number of retries, the user is locked out.

The following procedure describes how to manage a user account.

To edit a user's Oracle Identity Manager record:

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

   The Manage User page appears.

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

   Use one or more menus to dselect 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 list of user records retrieved will be. To use the **Employee Type** and **Status** search criteria, select values from the corresponding boxes.

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 checkbox 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 pull-down menu to view additional details about the user.

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

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

   - Click the **Group Membership** option in the menu 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 the **Proxy Details** option in the menu 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

Organizations

System Administrators can create and manage information pertaining to their organization. This chapter describes how to create and manage organizations in Oracle Identity Manager .

This chapter discusses the following topics:

Creating Organizations

To create an organization:

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

   The Create Organization page appears

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

   In the **Type** field, use the pull-down menu to 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** pop-up.

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

Managing Organizations

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

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 appears.

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 appears in the **Results** table, it will be in the **Organization Name** field, which is a sub-organization 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**: This is the current status of the organization (Active, Disabled, or Deleted).
4. Enter the appropriate value that corresponds with the search criteria, or use the asterisk (*) wildcard to query for all the organizations.

   The search Results page appears. This page lets you disable and delete an organization.

Enabling an Organization

To enable an organization:

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

   The Confirm Enable page appears.

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

Disabling an Organization

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 appears.

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

Deleting an Organization

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 appears.

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

Managing Organization Details

You can enable, disable, revoke, and provision resources to organizations and sub-organizations. 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 appears.

   The Organization Detail page appears.

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

   In 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 Organization Information >>Resource Profile page appears. 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 Organization Information >>Users page appears.

   In 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 sub-organization for this organization, the Organization Information >>Sub-Organization page appears.

   In the Sub-Organization page, you can move sub-organizations to a different organization.

6. If you view information based on administrators for this organization, the Organization Information >> Administrative Groups page appears.

   In the Administrative Groups page, you can

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

7. If you view information based on Permitted Resources for this organization, the Organization Information >> Permitted Resources page appears.

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

10

User Groups

You use user groups to create and manage records of collections of users to whom you may assign some common functionality, such as access rights, roles, or permissions.

User groups can be organization-independent, spanning across multiple organizations, or they can contain users from a single organization.

A group enables you to accomplish the following for multiple users:

- Designate the menu items that the users can access through the Oracle Identity Manager Administrative and User Console.
- Assign users or sub-groups to the user groups
- Designate the statuses to which the user can set process tasks.
- Make modifications and request permissions for data objects.
- Designate group administrators, for example, enable members of another user group to assign or remove members to or from the current user group and modify other characteristics of the group.
- Designate provisioning policies for a user group.

  These policies determine if a resource object is to be provisioned automatically 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 Oracle Identity Manager users can be assigned automatically to the user group.

Oracle Identity Manager provides three default user group definitions:

- System Administrators
- Operators
- All Users

You may modify the permissions associated with these user groups, and you can 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 generally 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 but not limited to the ability to access one's own user record. By default, each user automatically belongs to the All Users user group.

This chapter includes the following sections:

Note: A user cannot be removed from the All Users group.

Important: 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 privileges for performing self-registration in the Oracle Identity Manager Administrative and User Console.

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

Creating Groups

When you first create a new user group, the Group Detail page only shows a group name. You add information 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**, the click **Create**.
2. The **Create User Group** page appears.
3. Enter the name of the user group in the **Name** field.
4. Click **Create**.
5. The **Group Detail** page appears.
6. Click **Edit** to modify the Group Name, or click **Delete** to delete the user group.

Managing Groups

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

This section describes the following topics:

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 appears.

2. Select the Group Name attribute the menu, then enter a value in the text box next to the menu.

   You can use an asterisk (*) wildcard to query for all user groups.

3. Click **Search**.

   The search results page appears. This page enables you to view and delete user groups.

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 appears.

3. Click **Confirm Delete** to complete deleting this user group, or click **Cancel**.

Viewing and Administering a User Group

After selecting the user group you that you want to view, you can view the details of that particular user group, including the following:

- Member and Sub-Groups
- Menu Items
- Administrative Groups
- Access Policies
- Membership Rules
- Permissions
- Allowed Reports

Member and Sub-Groups

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

To work with members and sub-groups:

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 appears.

2. From the additional details box, select Members and Sub-Groups.

   The Group Detail >>Members and Sub-Groups page appears.

3. Click Assign Users.

   The Group Detail >> Members and Sub-Groups >> Search Member Users page appears.

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

   The **Results** table appears.

5. To increase or decrease the priority of a member, click the radio button 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, click the member's radio button in the **Remove** column of the **Results** table, and then click **Remove Member.**
7. Select the desired User ID(s) checkbox, then click **Assign**.

   The Confirmation page appears with the User ID names that you have just selected.
8. If these are the correct user names you want to assign to this user group, then click **Confirm Assigns**.

   Otherwise, click **Cancel**.

Menu Items

The **Menu Items** search criteria displays all menu items that are permitted for this user group. The **Menu Items** option enables you to assign a new menu item for the user group.

To work with menu items for this 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 appears.
2. From the additional details box, select **Menu Items**.

   The Group Detail >>Menu Items page appears
3. Click **Assign Menu Items**.

   The Group Detail >> Menu Items >> Assign Menu Items page appears.
4. Select the desired menu item name checkboxes, then click **Assign**.

   The Confirmation page appears.
5. If these are the correct menu item names you want to assign to this user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The **Result table** appears with the menu items permitted for this user group. This page also enables you to delete the menu items you wish not to permit.
6. To delete a menu item, select the menu item name checkbox, then click **Delete**.

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

Administrative Groups

You can view all administrative groups associated with a user group. You can also do the following:

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

Assigning an Administrative Group

This page also enables you to delete an administrative group from this user 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 appears.

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

   The Group Detail >> Administrative Groups page appears.

3. Click **Assign Administrative Groups**.

   The Group Detail >> Administrative Groups >> Assign Administrative Groups page appears.

   This page displays all administrative groups available to be associated with this user group.

4. Select the desired administrative group name checkbox and respective permission settings for write and delete accesses, then click **Assign**.

   The Confirmation page appears.

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

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

Creating a New 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 appears.

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

   The Group Detail >> Administrative Groups page appears.

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

   The Assign Administrators – Step 1: Assign Administrators page appears.

4. Select the user name checkbox 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 Assign Administrators – Step 2: Specify Alias page appears.

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

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

   The Assign Administrators – Step 3: Specify Permissions page appears. By default the **Read** permission checkbox is activated.

7. If desired, activate the Write or Delete permission, then click Continue.

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

   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, use the **Change** link.

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

The Group Detail >> Administrative Groups page appears.

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 appears.

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

   The Group Detail >> Administrative Groups page appears.

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

   The Group Detail >> Administrative Groups >> Update Permissions page appears

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

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

   Otherwise, click **Cancel**.

   The **Confirmation** page appears. 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 Group Details >> Administrative Groups page appears.

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

6. To delete an administrative group, select the desired group name checkboxes and click **Delete**.

Access Policies

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

To work with access policies:

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 appears.

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

   The **Group Detail >> Access Policies** page appears.

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

   The Group Detail >> Access Policies >> Assign Access Policies page appears.

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

4. Select the desired access policy(s) checkbox for this user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The **Confirmation** page appears.

5. If this is the correct access policy you want to assign for this user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The **Group Detail >> Access Policies** page appears.

6. To delete this access policy, select the desired policy name(s) checkbox and click **Delete**.

Membership Rules

You can displays 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 appears.

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

   The **Group Detail >> Membership** Rules page appears.

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

   The Group Detail >> Membership Rules >> Assign Membership Rules page appears. This page displays the name of the membership rule.

4. Select the desired membership rules checkbox for this user group, then click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The **Confirmation page** appears.

5. If this is the correct membership rule you want to assign for this user group, click **Confirm Assign**.

   Otherwise, click **Cancel**.

   The Group Detail >> Membership Rules page appears.

6. To delete this membership rule, select the desired membership rule checkboxes and click **Delete**.

Permissions

You can view all available permissions for a user group, assign, and update new permissions for a user group.

To work with user 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 appears.

2. From the additional details box, select **Permissions**.

The Group Detail >> Permissions page appears.

3. To assign a new permission, click **Assign**.

   The Group Detail >> Permissions >> Assign Permissions page appears. This page displays the name of the permission and activated permission settings, **Insert**, **Write,** and **Delete Access**.

4. Select the desired permission name checkbox and respective permission settings, then click **Assign**.

   Otherwise, click **Cancel**.

   The Confirmation page appears.

5. lf this is the permission you want to assign to this user group, click **Confirm Assign**, otherwise, click **Cancel**.

   The Group Detail >> Permissions page appears.

6. To delete a permission name, select the desired permission name(s) checkbox and click **Delete**.

7. To update the permissions, click Update Permissions.

   The Group Detail >> Permissions >>Update Permissions page appears.

8. Select or de-select the desired permissions **Allow Insert**, **Allow Update**, or **Allow Delete**, and click **Update**, or click **Cancel**.

   The **Confirmation** page appears. This page displays all the updated permissions.

9. If the information on this page is correct, then click **Confirm Update**, otherwise click **Cancel**.

   The Group Detail >> Permissions page appears. The Group Detail >> Permissions page displays the fine-grained permission information for this user group. It also enables you to delete any permissions.

10. To delete a permission, select the desired permission name checkbox and click **Delete**.

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 appears.

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

   The Group Detail >> Reports page appears.

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

   The Group Detail >> Reports >> Assign Reports page appears. This page displays available report names and types.

4. Select the desired report checkbox and click **Assign**, or click **Cancel**.

   The **Confirmation** page appears.

5. lf this is the correct report you want to assign for this user group, then click **Confirm Assign**, otherwise, click **Cancel**.

   The Group Detail >> Reports page appears.

6. To delete a report, select the desired report name checkbox and click **Delete**.

11

Access Policies

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:

Creating an Access Policy

The Access Policy wizard helps you define an access policy for provisioning resources to user groups and users. When creating a policy, you can ensure that the policy issues a request for approval before provisioning a resource to a user. Or, when an access policy is applied, the resource can directly provisioned to the user without generating an approval request.

You can also determine if a user who is already part of a user group for which an access policy is being created will be provisioned with the resource specified by this access policy. This is called retrofitting the policy.

To create an access policy:

1. Click **Create** under **Access Policies**.

   The Create Access Policy page appears.

2. Enter information in the required fields indicated with an asterisk (*).

   You can specify whether this access policy should be provisioned **Without Approval** or **With Approval**. Select the **With Approval** option to require a defined approver (or proxy user) to approve the resource to be provisioned to the user or group. If no approval is required, select the **Without Approval** option.

3. Click the **Retrofit Access Policy** checkbox to retrofit this access policy when it is created.

   If retrofit check box is not selected, existing group memberships are not taken into consideration.

   Click **Continue**.

   The Create Access Policy - Step 2: Select Resources (to provision) page appears.

4. In the Create Access Policy - Step 2: Select Resources (to provision) page, you can specify the resource to be provisioned for this access policy.

   Search for resources using the filter search menu.

To select the name of the resource from the **Results** table, check the desired box and 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 un-assign the selected resources, highlight the resource in the **Selected** list and click **Remove**.

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 appears.

5. On the Create Access Policy - Step 2: Select Resources to Revoke page, you specify whether access policies are revoked if they no longer apply.

   Select the checkboxes for the resources you want to revoke automatically in the **Results** table.

   Click **Continue**. The Create Access Policy - Step 3: Selected Resources (to deny) page appears.

6. You use the Create Access Policy - Step 3: Selected Resources (to deny) page to select resources to be denied by this access policy.

   To select resources to be denied, first select resources from the Results table by checking the corresponding checkbox. 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 un-assign them from the resources to be provisioned selection. Similarly, in the previous step, assigning the same resources to be provisioned as you have already selected to be denied will automatically un-assign them from the resources to be denied selection. You can un-assign the selected resources to be denied by selecting the resources you have already selected in the Selected list and click **Remove**.

   Click **Continue**.

7. The **Create Access Policy - Step 4: Select Group** page appears.

   Use this page to associate a group to the access policy.

8. To associate a group with this access policy, select the name of the group from the Results table by checking the desired box and clicking **Add**.

   The name of the desired group name appears 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 your user groups by using the filter search dropdown menu.

   Select the name of the user groups from the **Results** table by checking the desired box and clicking on the **Add** button. You must select at least one user group. The names of the desired user groups appear in the **Selected** list.

   You can un-assign the selected user groups by highlighting the resource in the Selected list and click **Remove**. Click **Continue**.

9. The Create Access Policy - Step 5: Verify Access Policy Information page appears. Use this page to verify the information specified in the previous steps for the access policy.

10. Clicking on any of the **Change** link will jump to the corresponding step in the wizard where you can modify the information specified earlier.

    After making modifications, click **Continue** to bring you back to this page (Step 5). Click **Continue** to create the access policy in Oracle Identity Manager. A success page appears and displays the name of the access policy and its successful creation.

Managing Access Policies

The Oracle Identity Manager Administrative and User Console enables you to modify information in existing access policies.

To manage access policies

1. Click Manage under Access Policies.

   The **Manage Access Policies** page appears.

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

   The Manage Access Policies page appears with your search results.

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

   The **Access Policy Details** page appears.

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

   When you click the **Change** link, the page jumps to the corresponding page where the information was initially entered.

3. At this point you can make any modifications in this page. Once you have completed, click **Update Access Policy**.

   This access policy is updated and the page jumps back to the Access Policy Details page with the updated information.

12

Resource Management

The Resource Management feature enables you to mange resource objects for an organization or an individual user. Managing resources includes the following:

- Ability to search for a resource and view its details
- Ability to disable, enable, revoke a resource from users or organizations
- Manage Resource Administrator and Authorizer groups

This chapter covers the following topics related to managing resources:

Managing Resources

The following procedure describes how to manage resources.

> **Note:** As described in the following procedure, when performing a search, if you select a value from the drop-down list and do not enter a corresponding search value, an error occurs. Also, if you select the same value twice, from the drop-down menu, an error occurs.

To manage resources:

1. Click **Resource Management**, and then click **Manage**.

   The Resource Search page appears.

2. Use the boxes at the top of the page to select search criteria, and enter the corresponding attribute in the next field or use the asterisk (*) as a wildcard. To use the **Resource Type** and **Target** criteria, select a value from the corresponding box.

3. Click **Search**.

   The **Results** table appears.

4. Click the name of a resource, for example, you may select a resource named **Oracle Identity Manager User**.

The Resource Detail page appears.

5. To view detailed information about the resource, use the menu.

   If the resource target is set to **O** for organization, the **Organizations Associated with This Resource** option appears. The **Organizations Associated with This Resource** page shows a list of organizations to whom this resource is provisioned or is being provisioned (revoked, enabled, disabled, and so on).

   If the resource target is set to **U** for users the Users Associated with This Resource appears. The **Users Associated with This Resource** page shows a list of users to whom this resource is provisioned or is being provisioned (revoked, enabled, disabled, and so on).

   The additional details include the following options:

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

Working with an Organization Associated With a Resource

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. Select the **Organization Associated For the Resource** option.

   The **Organization Associated For the Resource** page appears.

2. Use the radio buttons to filter the list of associated organizations.

   The **All** radio button lists all the organizations. The **By Status** radio button filters the organizations on 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, do 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 Oracle Identity Manager Design Console using the Map Descriptive Field. This value lets you distinguish which mapping category is defined (**Process Type**, **Organization Name**, or **Request Key**) when the same resource has been provisioned several times to the same organization.

Using the Resource Administrator Option

In the Resource Detail page, select the **Resource Administrator** option. 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 a User Group as Administrators for Resources
- Creating a New Administrator Group
- Updating Permissions of an Administrative Group

Assigning a User Group as Administrators for Resources

To assign a user group as administrators for resources:

1. Click **Assign**.

   The Assign Administrators page appears.

   This page displays all group names that can be assigned to this resource. Select the check boxes to activate **Write Access** and **Delete Access** options and assign the group to this resource.

2. Click **Assign**.

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

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

   The Resource Administrators page appears with a list of all group names associated with this resource. You can make modifications to this information.

Creating a New Administrator Group

You can create a new group to administer a resource. A Delegated Admin Wizard is provided for this process.

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

To create a new group:

1. Click **Create New Group**.

   The Assign Administrators – STEP 1: Assign Administrators page appears.

   In the **Results** table, click the **User Login** names that you want in the administrative group and click the **Add** button.

   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 appears.

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

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

   The Assign Administrators – STEP 3: Specify Permissions page appears.

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

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

The Assign Administrators – STEP 4: Verify Delegation Information page appears.

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

   The corresponding step page appears.

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

   The Resource Administrator page appears. The new group is added to the **Results** table.

Updating Permissions of an Administrative Group

You can update the permissions of an administrative group.

To update the permissions:

1. Click **Update Permissions.**

   The Resource Detail >> Resource Administrators >> Update Administrators page appears.

2. To change the permission setting for an administrative group, click the desired checkboxes for Write Access and Delete Access.

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

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

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

Using the Resource Authorizers Option

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

To use the resource authorizers option:

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

   The Resource Detail >> Resource Authorizers page appears.

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

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

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

   The Resource Detail >> Resource Authorizers >> Assign Authorizers page appears.

5. Select the desired Group Name checkbox and click **Assign**, otherwise, click **Cancel.**

   The Confirmation page appears.

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

   The Resource Detail >> Resource Authorizers page appears. Note that the **Group Name** that you assigned to this resource is added to the **Results** table.

Using the Resource Workflows Option

The Graphical 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 make up the flow. You can edit and print the workflow view.

The Graphical Workflow Visualizer tool displays the Approval and Provisioning process types. You usually use the **Approval** type of 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 of 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 covers the following topics:

Launching the Workflow Visualizer

To launch the visualizer:

1. In the **Resource Detail** page, select the **Resource Workflows** option from the pull-down menu.

   The Resource Detail >> Resource Workflows page appears. This page displays the Resource Name and a table that lists all the names of the workflow definitions for this resource.

2. To render the workflow definition into a graphic flowchart, click the link of the desired Workflow Name.

   A new web browser window is launched and a graphical representation of the workflow definition appears.

Using the Workflow Visualizer

The **Approval Workflow Definition** is displayed as one flow that represents the entire approval process. The workflow details header shows no information on the form since the approval process has no form of its own. The Workflow Visualizer does not display the **Name of Process Form** information field.

The **Information Fields** of the Workflow Visualizer are the following:

Field Name	Description
Workflow Name	The name of the Process Definition.
For Resource	The name of the Object Name (resource object that is either approved or provisioned).
Workflow Type	The name of the Process Definition type (Approval or Provisioning). The type also indicates whether the workflow is the default for the resource.

The **Toolbar Menu Items** of the Workflow Visualizer are the following:

Field Name	Description
Display Option	**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 have the option of showing them (Unknown Response Code) or not. **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 on-screen. **Display Recovery Tasks:** You can display the recovery tasks for the tasks on-screen.
Generate Image	This option enables you to save the workflow view as an image that can be printed at a later time. Upon clicking on this menu item, a new browser window is launched and 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 mechanisms to save the image locally on your machine by right-clicking on the image and selecting **Save Picture As…** from the menu.
Reload Workflow	This option refreshes the workflow view.

Field Name	Description
Legend	This option provides an explanation of all visual components that are used to create the flowchart of the workflow definition. **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) help keep the workflow controllable by hidden significant sub-trees of responses nodes. Double click the Expansion Node marker and the workflow view will redraw the flowchart with the responses. **Tasks** The Tasks Nodes represent the tasks in the workflow. They are: Manual Tasks: The Manual Tasks represent any task in a process that requires user action in order to be completed. Approval processes are generally comprised of manual tasks. Automated Tasks: The Automated Tasks represent any task in a process that does not require user interaction for completion. Automated tasks always require a process task adapter. Provisioning processes are generally comprised 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 is set on the task. Completes Task: The process task has been completed and is indicated by a green color. Rejected Task: The process task has been rejected and is indicated by a red color. Cancels Task: The process task has been cancelled and is indicated by a blue color. **Links** Direction arrows 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. 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 is Completed. Generally, a new process task can then be triggered when the conditional task receives a particular response code in conjunction with the execution of the process task. Recovery Task: The Recovery Task is defined as process task that is triggered when the current process task is Rejected. Undo Task: The Undo Task is defined as process task that is triggered when the current process task is Cancelled. Dependent Task: The Dependent Task is defined as a process task that is dependent upon another process. Oracle Identity Manager can only initiate this type of task once the process task on which it is dependent is completed.

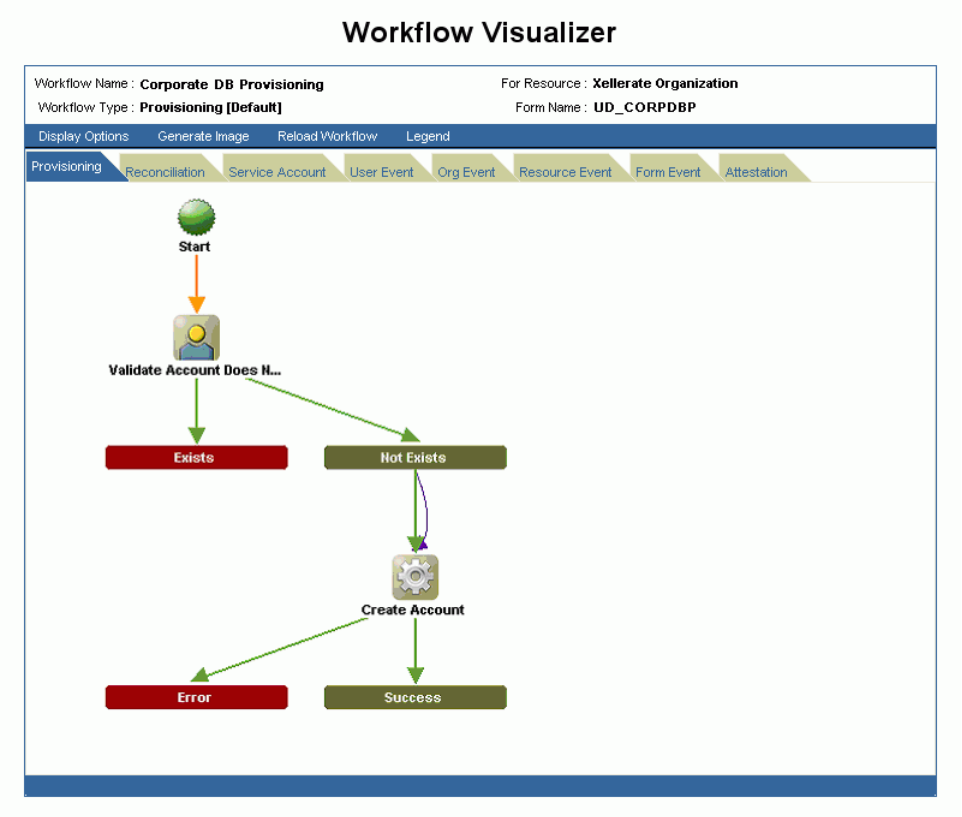
User Interface

The Workflow Visualizer enables you to manipulate the workflow view by using the following features:

- Drag and Drop
- Display Option (menu item)
- Task Node (right-click menu)
- Expansion Nodes (Response Sub-Tree)

For example, suppose that 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" on page 12-11.

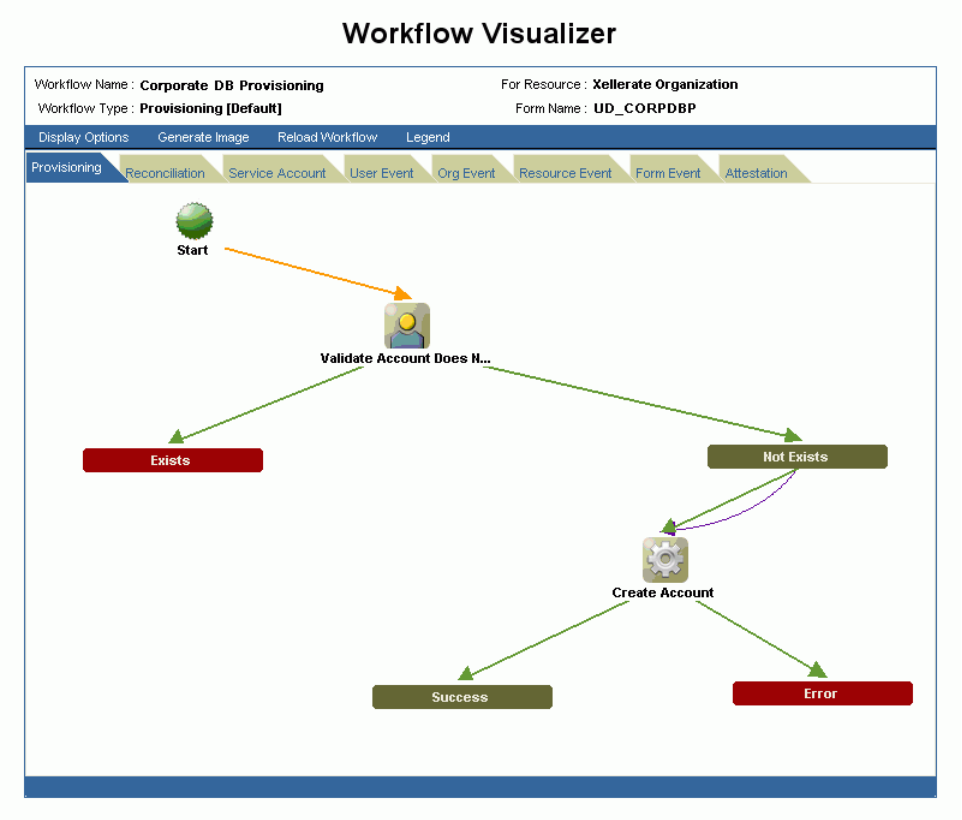
Figure 12–1 Using the Workflow Visualizer



Using Drag and Drop

You can rearrange the graphical workflow by dragging and dropping the icons that make up the workflow definition to any location in the workflow view. As you move an icon component, the direction arrow continues to associate the link.

Figure 12–2 Using Drag and Drop in the Workflow Visualizer



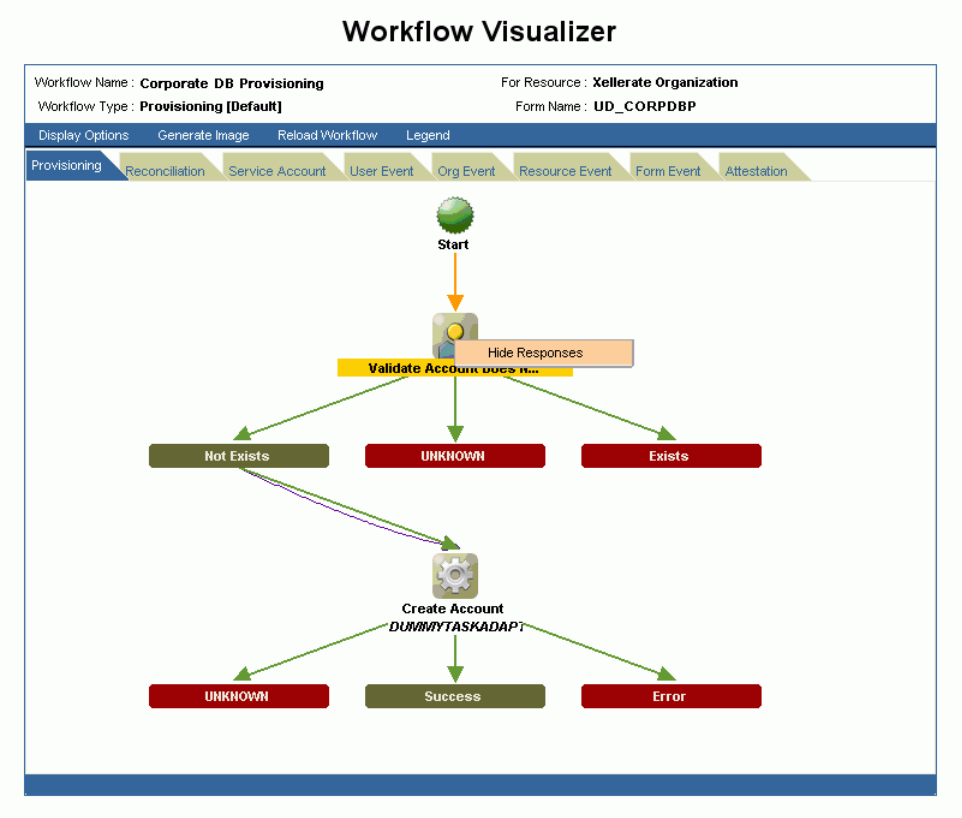
Using Display Options (menu item)

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 re-draws the workflow based on your criteria.

Using the Task Node (right-click menu)

When you right click the task node, the **Hide Responses** option appears. When you click this option the response sub-tree 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, the **Hide Responses** action option does not appear.

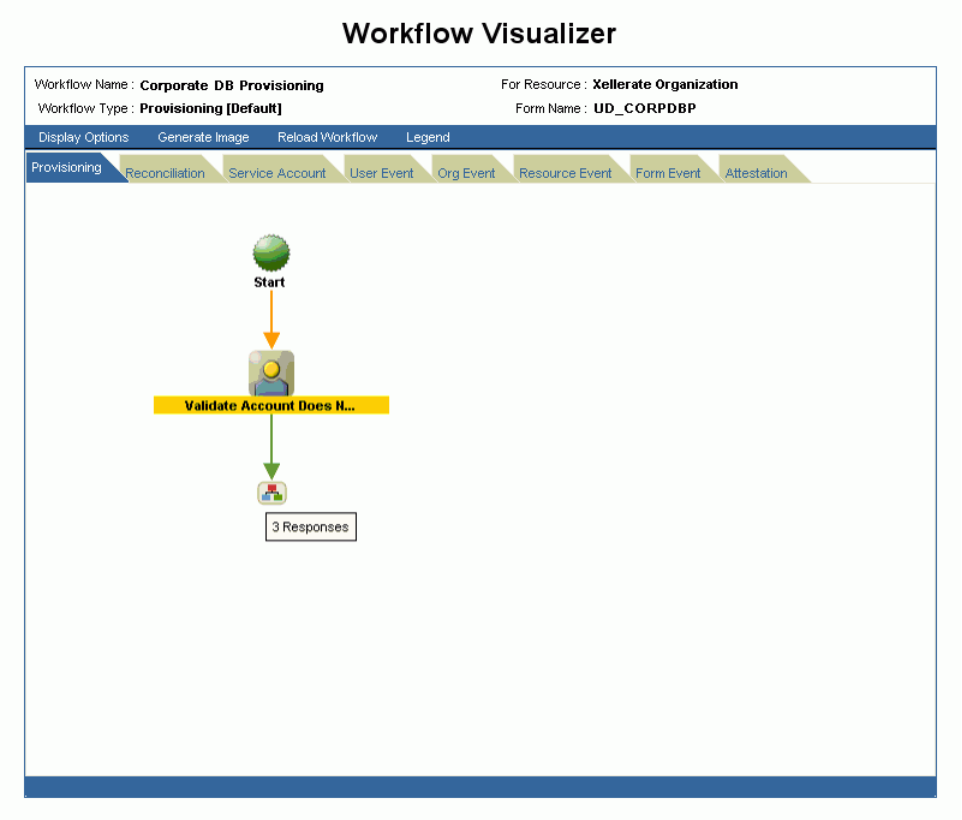
Figure 12–3 Using the Task Node (Right-Click Menu)



Using the Expansion Nodes (Response Sub-Tree)

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

Figure 12–4 Collapsed Response Subtree in the Workflow Visualizer



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

Using the Provisioning Workflow Definition Event Tabs

The Provisioning Workflow Definition is displayed with associated event tabs of the logical flow. The event tabs represent the various task sequences for a specific event in the workflow definition. By clicking an event tab, the tab displays the appropriate tasks for the workflow event of the process. You can arrange the flowchart to your desired view. If there is no task defined for the workflow event, the tab displays a blank view. If there is more than one task sequence for the workflow event type, the tab displays a pull-down menu where you can select the process flowchart that you want to view.

Provisioning Tab

The Provisioning tab shows the task that will provision a resource. When the process type is **Provisioning**, the process flowchart shows all task needed to provision a resource.

Reconciliation Tab

The Reconciliation tab shows the reconciliation event for the provisioning process with marker tasks inserted into it – either **Reconciliation Insert Received** or **Reconciliation Update Received**. These tasks can have adapters attached to them to initiate a provisioning action. If no adapters are attached to it, a response code of **Event**

Processed is assigned to that task. Additional provisioning process tasks can be generated based on this response code to initiate a provisioning flow due to the reconciliation event.

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 cancelled. Instead, a task is inserted into the provisioning process to removes the mapping from the user to the service account. The provisioning processes of service account are: **Service Account Changed**, **Service Account Alert**, and **Service Account Moved**.

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.

Org Event Tab

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

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.

Form Event Tab

The Form Event tab shows workflows that respond to data changes in the Process Form of the provisioned resource instance.

Attestation Tab

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

Accessing the Task Details

To view detailed information for a particular task, double click the task icon. The Task Detail window is similar to the task definition window in the Process Definition Form of the Oracle Identity Manager Design Console. The Task Detail window displays information about the task definition, which is presented in logical grouping of tabs. The tabs include:

- **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:** The 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.

General Tab

Field Name	Description
Task Name	The name of the process task.
Task Description	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 that 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** upon completion of all recovery tasks that are generated. This flag triggers other dependent process tasks.
Allow Cancellation While Pending	This field indicates whether the process task can be cancelled if its status is **Pending**.
Allow Multiple	This field indicates if the task is allowed to be inserted multiple times within a single process instance.
Required For Workflow Completion	This fields indicates that the process cannot be completed if the process task does not have a status of **Completed.**
Manual Insert	This field indicates whether a user can manually add the current process task to the process.

Automation Tab

Tasks belonging to provisioning processes are usually automated.

Note: If the task is not automated this tab does not appear.

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

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, since these tasks are usually completed manually. Tasks belonging to provisioning processes are usually automated. As a result, they do not need task assignment rules.

Depends On Tab

This tab displays the task name that the current task is dependent upon.

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

Field Name	Description
Task Status	One of the pre-defined provisioning status types.
Resource Status	The status can be one of the following: **Waiting**, **Provisioning**, **None**, **Ready**, **Enabled**, **Disabled**, **Revoked**, **Provisioned**, and **Provide Information**.

13

Deployment Manager

The Deployment Manager is a tool for exporting and importing Oracle Identity Manager configurations. The Deployment Manager enables you to export the objects that make up your Oracle Identity Manager configuration. You use the Deployment Manager to exchange Oracle Identity Manager items between environments. 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 Oracle Identity Manager Administrative and User Console.

The Deployment Manager saves your settings in an XML file. These items include:

- Adapters
- Error message and lookup definitions
- User group and administrative queue information
- User-defined field definitions
- Rule definitions
- E-mail definitions
- Password management
- Access policies
- IT Resources
- Resource objects
- User-created forms
- Organization and task scheduling information

You can save some or all of the objects in your configuration. This lets you develop and test your configurations in a test environment, then import the finished items into your production environment. You can import and export an object and all of its dependent and related objects at the same time, or you can export parts of it.

This chapter covers the following topics:

- Best Practices

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 enables you to build up 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. Once you add objects of one type, you can go back and add other objects to your XML files. When you have all the desired objects, the Deployment Manager saves them all at once into a single XML file.

Note: 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) the Deployment Manager will consider them as dependencies.
- If the user defined fields contain no values (the fields are blank), the Deployment Manager will not considered them as dependencies.

To export a deployment:

1. In the Oracle Identity Manager Administrative and User Console menu, click **Deployment Management**, then click **Export**.

   The Deployment Manager opens and the Export Wizard's Search Objects screen appears.

2. On the Search Objects, select an object type from the menu, and enter search criteria.

   If you leave the criteria field blank, an asterisk automatically appears to find all the objects of the selected type

3. Click **Search** to find objects of the selected type.

   To select an object, click its checkbox.

4. Click **Select Children**.

   The Select Children screen appears. The Select Children screen displays the selected objects and any of their children.

5. Select the children to export.

   To select or remove an item, click its checkbox.

   Click **Back** to go to the Search Objects screen.

6. Click **Select Dependencies**.

   The Select Dependencies screen appears. The Select Dependencies screen displays any objects required by the selected objects.

7. Select which dependencies to export.

   To select or remove an item, click its checkbox.

   Click **Back** to go to the Select Children screen.

8. Click **Confirmation**.

   The Confirmation screen appears.

9. Make sure all desired 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 screen.

   The Add More screen appears.

10. Use the wizard to add more items, or finish and exit the wizard.

    Select the desired radio button and click **OK**.

    If you selected **Add more**, repeat Steps 2 through 7. Otherwise, the Export screen appears.

    The Export screen 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. In the Unselected Dependencies pane, any dependencies or children of the selected objects that you chose not to export are listed.

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, to remove them all at the same time select **Remove including children** from the shortcut menu.
    - Click **Remove** to confirm. If the object is a child or dependency of a selected item, 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, right-click the object and select **Add**. Click to confirm.

12. Click **Export**.

    The Add Description dialog box appears.

13. Enter a description for the file.

    This description is displayed when the file is imported.

14. Click **Export**.

    The Save As dialog box appears.

15. Enter a file name.

    You can browse to find a location.

16. Click **Save**.

    The Export Success dialog appears.

17. Click **Close**.

Importing Deployments

You can import objects that were saved in an XML file using the Deployment Manager into your Oracle Identity Manager system. You can import all or part of the XML file, and you can import multiple XML files at once. The Deployment Manager checks to make sure 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.

This section includes the following subsections:

Note: Before importing data that contains references to menu items, you must first create the menu items in the target system.

Deployment Manager Behavior on Re-Imported Scheduled Task

Under normal circumstances, you would import a Scheduled Task into your Oracle Identity Manager environment and later change the values 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 re-imported XML file to any corresponding attribute values in the database.

The following table summarizes the Deployment Manager's behavior on Scheduled Task re-import.

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 timestamp)	No change in the database
Yes (Newer attribute values indicated by timestamp)	Yes	Update the database with the newest attribute values

Importing an XML File

1. In the Administrative and User Console menu, click **Deployment Management**, then click **Import**.
2. Choose a file.

   The Import dialog box appears.
3. Click **Open**.

   The File Preview screen appears.
4. Click **Add File**.

The Substitutions screen appears

5. To substitute a name, click in the **New Name** field adjacent to the item you want to replace, and enter the desired name.

   You can only substitute items that exist in the target system.

6. Click **Next**.

7. If you are exporting an IT Resource Instance, then the Provide IT Resource Instance Data screen is displayed.

   Otherwise you are redirected to the Confirmation screen.

8. 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 screen appears.

9. Check that the information is correct.

   To go back and make changes, click **Back**, or click **View Selections**.

   The Deployment Manager Import screen displays your current selections.

   The Import screen 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 the icons. The file names of any selected files, summary information about the objects you are importing, and substitution information is displayed on the left side of the screen. On the right, the **Objects Removed from Import** list displays any objects in the XML file that will not be imported.

10. Make any desired 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 to remove and select **Remove** from the shortcut menu, then click **Remove** to confirm.

      If the object has child objects, to remove them all at the same time, select **Remove including children** from the shortcut menu.The item is added to the Objects Removed From Import list.

    - To add an item back to the Current Selections list, right-click it and select **Add**.

      If the object has child objects, to add them all at the same time, select **Add including children** from the shortcut menu.

    - To make substitution, 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 screen appears and shows basic information about your import.

      To see more information, click the **Show Info Level Messages** checkbox, then click **Show Messages**. Click **Close** to close the Information screen.

11. To import the current selections, click **Import**.

    A confirmation dialog box appears.

12. Click **Import**.

    The import success dialog appears.

13. Click **OK**.

    The objects are added to your Oracle Identity Manager system.

Best Practices

The following are some of the suggested practices and pitfalls to avoid while using Deployment Manager.

> **See also:** For details on best practices related to using the Deployment Manager, refer to the *Oracle Identity Manager Best Practices Guide*.

- Understand the limitations of the Deployment Manager to effectively use all its functionality.
- 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.
- 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 UDF or form import
- Perform imports during periods of low activity in the system.

14

Reports

Based on whether you access current operational data or historical data, the reports you can generate using Oracle Identity Manager are divided into **Operational Reports and Historical Reports**. These reports describe the resources available to users.

This chapter discusses the following topics:

Overview of Operational Reports

The following sections describe the out-of-box operational reports in Oracle Identity Manager. These reports can be used by administrators and auditors for operational and compliance purposes.

Resource Access List

Queries all existing users provisioned to a resource.

Policy List

Displays a list of policies for a specified group.

Policy Detail

Displays complete details about specified policies.

Oracle Identity Manager Password Expiration

Lists user password expiration settings.

User Resource Access

Queries access rights for users that match specified query parameters.

Entitlements Summary
Lists the number of users for each status within each resource.

Attestation Requests by Process
Lists attestation requests by process.

Attestation Request Detail
Returns complete details of a specified attestation request.

Resource Password Expiration
Returns a list of users whose resource passwords are about to expire.

Group Membership
Lists the number of users in each group.

Attestation Process List
Lists all defined attestation processes.

Attestation Requests by Reviewer
Lists attestation requests by reviewer.

Group Membership Profile
Lists user group memberships.

Overview of Historical Reports

The following sections describe the out-of-box historical data reports in Oracle Identity Manager. These reports can be used by administrators and auditors for compliance and forensic auditing purposes.

User Membership History
Displays a istory of a user's group memberships.

User Resource Access History
Lists a user's resource access history over the lifecycle of the account.

Group Membership History
Displays a history of a group's memberships.

User Profile History
Lists a user's profile history over the lifecycle of the account.

Resource Access List History
Queries all users provisioned to a resource over its lifecycle.

Running Reports

To run a report:

1. Expand the **Reports** link and click **Operational Reports** or **Historical Reports**.

The resulting screen 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
Description	Provides a short description of the report

2. Select a report by clicking on its name.

   The **Report Input Parameters** screen appears. This screen displays the input parameters that need to be provided to run a report. In some cases, at least one or more input parameter fields will be required fields. If this is not the case, you must populate at least one of the fields to run a report.

3. Enter the information required to identify what information the report contains.

4. Click the **Submit** button to run the report.

   The Report Display page appears.

Report Display

This 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:

- Simple Table Format
- Sectional Format
- Sectional Format with Report Header

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.

Filters

You can use a filter to narrow the search criteria for a report. By default, three filters appear as a menu and a text field. Select the type of data from the menu, then enter a filter string in the text field. The asterisk (*) wildcard character can be used in the filter text box. 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, employee type, and so on 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 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]`, this 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 criteria of `[User`

`Status=Active]` returns all users who were active at some point in the past, even if they are currently disabled.

After creating the filter and clicking the **Filter** button, the resulting report is displayed on the same Report Display Page. The filter menu and text boxes will reflect the filter values that were provided. The **Clear** button clears the filter fields.

Change Input Parameters

The **Change Input Parameters** button returns you to the Input parameters page. The input parameter fields contain the information you already entered.

CSV Export

You can export all the report information as a single Comma Separated Values file, or CSV. Click the **CSV Export** button 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`.

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 on that resource or user id.

Creating Reports Using Third-Party Software

Oracle Identity Manager supports the creation of reports using third-party tools such as Crystal Reports. It supports the following out-of-the-box report types:

- **Who Has What:** This report lists the users and the resource objects with which they have been provisioned.
- **Direct Provisioned**: This report shows the following information:
  - The resource objects that have been directly provisioned to the target users.
  - The user who have directly provisioned the resource objects for the target users.
  - The users who received the resource objects.
- **Requests Made**: This report displays requests that have been created by users.
- **Active Queue**: This report is a sub-set of the Requests Made report. It lists the requests that have been approved by users.
- **Requests Executed**: This report is a sub-set of the Active Queue report. It shows the requests that have been executed by Oracle Identity Manager.
- **Reconciled Apps**: This report lists the successful reconciliation events. Reconciliation is the process whereby provisioning events outside of Oracle Identity Manager are made known to Oracle Identity Manager.
- **Reconciled Users**: This report displays the users who have been added to Oracle Identity Manager using reconciliation.
- **Unreconciled Data**: This report shows the reconciliation events that could not be matched to a specific user, organization, or provisioning process.

Note: To learn how to create reports using third-party software, refer to the software documentation.

15

Attestation

You can create, manage, and view attestation tasks.

This chapter discusses the following topics:

- Attestation Process Configuration
- Creating Attestation Processes
- Managing Attestation Processes
- Using the Attestation Dashboard

> **See also:** See Appendix A, "Understanding Attestation" for information on using attestation in the Oracle Identity Manager Administrative and User Console.

Attestation Process Configuration

A menu item in the Administrative and User Console provides access to the Attestation Process Configuration screens. Oracle Identity Manager administrators can use these screens to do the following:

- Define new attestation processes
- Manage existing processes
- Initiate ad-hoc attestation processes

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 Oracle Identity Manager Administrative 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.

System Control

Attestation has the following dependencies:

- The User Profile Audit feature must be enabled.
- Historical data must be collected at least down to the Process Form level.

If the auditing level is set below the required levels, clicking on 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`.

Creating Attestation Processes

The following procedures describes how to configure an attestation process.

Note: In the following procedure, the Oracle Identity Manager Permission model applies. This model restricts any list of targets, for example, users, to only those targets that the logged-in user has read access to.

To create a new attestation process:

1. Expand the **Attestation** link and click **Create.**

   The Step1: Define process identification page appears.

2. Enter values for the fields described in the following table and click **Next.**

Field	Description
Name*	Identifies a unique name for the attestation process. The name must be unique across disabled and deleted attestation processes.
Code	An identifying code (up to 32 characters) for the process. The code must be unique across disabled and deleted attestation processes.
Description	Detailed description of the attestation process.

3. On the Step 2: Define Attestation Scope and Review page, perform the following steps:

   a. Attestation scope defines the algorithm by which the targets of the attestation are selected. The first three options correspond to **User Entitlement Attestation** in which every financially significant entitlement for the determined users needs to be reviewed and attested. The algorithms determine how the users whose entitlements need attestation are to be selected – based on a reporting relationship, membership in a group, or on the organization that the user is defined in.

      The fourth option corresponds to **Resource Entitlement Attestation**, in which all access to a specific resource must be attested, irrespective of the user, and ignoring other entitlements that the user might have. In this option, the administrator must therefore select the resource whose access must be attested.

      Select one of the following types of attestation scope:

Users reporting to manager

Members of group

Users in organization

User access for a single resource

b. Click the magnifying glass next to the selected type of attestation scope to select a manager, group, organization, or resource.

c. Select one of the following attestation reviewers:

Each user's manager

In this case, multiple attestation tasks can be set up, one for each manager who has any reports that fall into the target user set.

A specific reviewer

This reviewer can be the reviewer for the entire target set.

d. If you selected a specific reviewer in the previous step, click the magnifying glass to select the reviewer.

e. Click **Next.** The Step 3: Define administrative details page appears.

4. Specify the following administrative details about the attestation process:

- The attestation schedule
- The process owner
- Optionally, notifications for Process Owner user groups if reviewers decline attestations.

On the Step 3: Define administrative details page, perform the following steps:

a. Select one of the following attestation schedules:

Run once

Run every specified number of months

Run every specified number of days

Run every specified number of years

b. If you decide to run the attestation process on a monthly, daily, or yearly schedule, you have to specify a frequency on the selected option's text box.

c. Select a starting date by clicking the calendar icon next to the Starting On field.

d. Specify a process owner group by clicking the magnifying glass next to the Process owner group box.

e. If desired, click clear the **Email process owner if reviewer refuses attestation request** box. In this case, notifications are not sent to the process owner users if a reviewer refuses to attest.

f. Click **Next.** The Step 4: Confirmation page appears.

5. On the Step 4: Confirmation page, click **Create Process** to create the attestation process. You are redirected to a screen with the following information:

You have successfully created an attestation process definition.

Clicking ***processname*** 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 Managing Attestation Processes.

Managing Attestation Processes

To manage attestation processes:

1. Expand the **Attestation** link and click **Manage.** The Attestation Search page appears.
2. On the Attestation Search page, enter the search criteria for the attestation process you want to manage. You can search by attestation process name, process code, reviewer type, scope type, or process owner. After you enter your search criteria, click **Search.** A results table appears with the attestation processes that match your search criteria. Only those attestation processes are displayed 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 results table contains the columns listed in the following table:

Column	Description
Process Names	Specifies the name of the process.
Process Code	Attestation process code.
Data Type	Identifies the type of data being attested.
Scope	Indicates whether the attestation scope is by manager, group, organization, or resource.
Last Start	Specifies the last time an attestation process was executed.
Last Completion	Specifies the last time an instance of this process was completed.
Next Start	Specifies when the process is scheduled to run next.
Status	Indicates whether the attestation process is active or disabled.

3. In the results table on the Attestation Search page, click the link of the process name you want to manage. The Attestation Process Detail page appears.

This rest of this section discusses the following topics:

- Editing an Attestation Process
- Disabling an Attestation Process
- Enabling an Attestation Process
- Deleting an Attestation Process
- Running an Attestation Process
- Managing Attestation Process Administrators
- Viewing Attestation Process Execution History

Editing an Attestation Process

To edit an attestation process:

1. On the Attestation Process Detail page, click **Edit.**

   The Edit Attestation Process page appears.

2. On the Edit Attestation Process page, make the desired changes to the attestation process and click **Save.**

   The fields on the Edit Attestation Process page are same as those displayed in the Creating Attestation Processes wizard.

Disabling an Attestation Process

A **Disable** button appears when a process is active. You can disable an active process.

To disable an attestation process:

1. On the Attestation Process Detail page, click **Disable.**

   Note that the **Disable** button only appears when a process is active.

   The **Disable Attestation Confirmation** page appears.

2. On the **Disable Attestation Confirmation** page, click **Confirm Disable**.

Enabling an Attestation Process

An attestation process can only be enabled 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 only appears when the process is disabled.

   The **Enable Attestation Confirmation** page appears.

2. On the **Enable Attestation Confirmation** page, click **Confirm Enable**.

Deleting an Attestation Process

Editing, disabling, and deleting an attestation process can only be done by process administrators with required permissions.

To delete an attestation process:

1. On the Attestation Process Detail page, click **Delete.**

   The **Delete Attestation Confirmation** page appears.

2. On the **Delete Attestation Confirmation** page, click Confirm **Delete.**

Running an Attestation Process

This feature enables you to run unscheduled attestation processes. To run an attestation process click **Run Now** on the Attestation Process Detail page. This initiates the attestation process independent of the attestation schedule.

Only users in the process owner group can initiate unscheduled attestation processes.

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 an attestation process's administrators, select **Administrators** from the Additional Details box on the Attestation Process Detail page. The Attestation Process

Details >> Administrative Groups page appears. You can use this page to add and remove administrators for an attestation process and update administrator permissions.

The permission model for 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
  - 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 appropriate write permissions in the Administrators.
- To delete the Attestation Process Definition, the user must be a member of a group that has the appropriate delete permissions in the Administrators.

Viewing Attestation Process Execution History

To view an attestation process's execution history, select **Execution History** from the Additional Details box on the Attestation Process Detail page. The Attestation Process Details >> Attestation Process Execution History page appears.

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
Scope Parameter	Parameter value chosen for the attestation scope selection
Reviewer	Name of the reviewer for the attestation process.
Initiated On	Date and time when the request was initiated
Completed On	Date and time when the request was completed. If the request is still pending, it shows Not Completed.

Using the Attestation Dashboard

You use the Attestation Dashboard to view the state of any attestation processes that are owned by any group of which you are a member. To use the Attestation Dashboard, expand the **Attestation** link and click **Attestation Dashboard.** The Attestation Dashboard page appears and displays a table listing the state of any 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	Attestation process code.
Process Names	Specifies the name of the process. Clicking on the link for an attestation process name link takes user to the Attestation Process Detail page
Last Completion	The date and time when the instance executed before the latest one was completed. If it doesn't exist, then the value should be None. It is a link that will take the user to the Attestation Request Detail page for the appropriate Attestation Request.
Current Request Date	The date and time when the last instance of this Process was executed. If it has never been run, then the value is New. It is a link that will take the user to the Attestation Request Detail page for the appropriate Attestation Request.

Column	Description
Current Completion	The date and time when the last instance executed was completed. If it hasn't been completed, then the value is Pending.
Total Records	Identifies the total number of entitlements identified for attestation and covered by an attestation task as part of the last process instance.
Certified	Specifies the number of entitlements certified in the last attestation process instance.
Rejected	Specifies the number of entitlements rejected in the last attestation process instance.
Declined	Specifies the number of entitlements declined in the last attestation process instance.
Delegated	Specifies the number of entitlements delegated in the last attestation process instance.

Viewing Attestation Request Details

The drill-down page accessed from the Attestation Dashboard 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	The user whose entitlement is being attested. The data is a link that pops up the user profile page showing user details as on the Attestation Date.
Resource	The resource that is the basis for the entitlement being attested. The data is a link that pops up a page with the process form data of the entitlement as on the Attestation Date.
Descriptive Data	The descriptive data field for the provisioned resource instance.
Attestation Result	The response that was finally provided for the attestation.
Reviewer	The user that provided the response. The data is a link that pops up the user profile page showing 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 happens, then it says None.
Comments	This shows reviewer comments. Long comments are truncated and a a rollover tool tip shows the entire comment

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 on the attestation request's delegation path.

   The **Data Attested** field shows details of the entitlement being attested to. 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 contains the following fields:

Column	Description
Reviewer	The reviewer to whom the entitlement for attestation is assigned. The data is a link that pops up the current user profile data.
Attestation Result	Action supplied by the reviewer. Except for the first record, it will always be Delegated.
Attestation Date	The date and time of the attestation response of the reviewer.
Comments	Reviewer comments. Long comments are truncated and displayed in full as a rollover tool tip.

Email Notifications

As part of the attestation process, the attestation engine sends email to concerned parties at various stages. You can configure email content, using email templates of type **General** in the Oracle Identity Manager Email Definition store.

In the templates, the form user is defined as XELSYSADM. You can change it another user. Make sure that email address is defined for the user selected to use these templates. Otherwise, the system may not be able to send out notifications.

The following email notification templates are available:

- **Notify Attestation Reviewer:** Used for sending email when an attestation task is assigned to a reviewer.
- **Notify Delegated Reviewers:** Used for sending email to reviewers when an attestation task is delegated to them.
- **Invalid Attestation Reviewers:** Used for sending email to users in the Process Owner group if attestation task generation results in invalid reviewers.
- **Notify Declined Attestation Entitlements:** Used for sending email to users in the Process Owner group if a reviewer declines any entitlements.
- **Attestation Reviewers With No Email Defined:** Used for sending email to users in the Process Owner group if an email address is not defined for any of the reviewers.

Scheduled Tasks

A system scheduled task called Initiate Attestation Processes is responsible for examining the Attestation Processes defined in Oracle Identity Manager and creating the necessary attestation tasks in the system.

Salient features of this scheduled task are:

- Out of the box, scheduled tasks are set to run every 30 minutes by default. Users can change this to suit their needs
- It examines all active attestation processes.
- It initiates a call to the Attestation Engine to initiate the any attestation process that needs to be run (its next scheduled start time is in the past).

16

Working with the Diagnostic Dashboard

This chapter describes the Diagnostic Dashboard feature of Oracle Identity Manager.

This chapter discusses the following topics:

Introduction to the Diagnostic Dashboard

You use the Diagnostic Dashboard tool to validate some of the Oracle Identity Manager prerequisites and to verify the installation.

You must have the appropriate system administrator privileges for your Application Server and Oracle Identity Manager environments to use this tool. Some database related tests need DBA privileges. If you do not have DBA privileges, give the URL to the test to a DBA and have the DBA send the results back to you.

The list of tests available and displayed depends on whether Oracle Identity Manager is installed or not and on what application server this tool and Oracle Identity Manager will be or are installed on.

The Diagnostic Dashboard tool and Oracle Identity Manager should be installed on the same application server.

Installation Checks

You use this tool 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 two reports are available:

- Java VM System Properties Report

- WebSphere Version Report

The following tests are only available after 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 two 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 these 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

Post Installation Check

The following are the post-installation tests:

- Database Encryption Key Verification
- Trust store verification
- SSO Diagnostics/Verification
- JMS Server availability on WebSphere
- Messaging Verification
- Scheduler verification
- Remote Manager Verification
- Reporting version numbers
- Packaging

Installing the Diagnostic Dashboard

The Oracle Identity Manager Diagnostic Dashboard tool is distributed on the installation CD with the Oracle Identity Manager installer. It is available as a WAR file under the **Diagnostic Dashboard** directory on the CD-ROM.

Oracle recommends that you deploy the Diagnostic Dashboard tool on the application server before installing Oracle Identity Manager.

Installing the Diagnostic Dashboard on OC4J

To install the Diagnostic Dashboard on the OC4J server:

1. Log in to the Oracle Administrative and User Console:

   `http://<xlserver_host_ip>:7777`

2. Click **Log on to Oracle Enterprise Manager 10g Application Server Control**.
3. Log in with your OC4J admin user name and password.
4. Click **Home** under the OC4J instance column under Groups.
5. Click **Application** on the OC4J 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:

   `<installer_home>\dashboard\`

   Click **Next**

9. In step 2, specify a name for the application (for example, `XIMDD`), and then click **Deploy** in step 3.

   You should be able to access the Diagnostic Dashboard at the following location:

   `http://<xlserver_host_ip>:7777/XIMDD`

Deploying on JBoss

To deploy Oracle Identity Manager Diagnostic Dashboard on JBoss, copy the `XIMDD.WAR` file to the following location:

`<JBOSS_HOME>/server/default/deploy`

Deploying on WebSphere

To deploy Oracle Identity Manager Diagnostic Dashboard on WebSphere:

1. Log in to the admin console.
   - Start the application server.
   - Type URL (`http://localhost:9090/admin`) on Internet Explorer.
2. Click **OK** to proceed.

   The WebSphere main screen appears.

3. Click **Applications** link on the left menu pane, then click the **Install New Application** link.

The Preparing for the Application Installation screen appears.

4. Specify the location of the WAR file as the value of the Path attribute & 'XIMDD' as the Context root.
5. Click **Next** to proceed, and then click **Next** on the Generate Default Bindings screen.

   The Install New Application screen appears.
6. Change application name to XIMDD. Click **Next** twice.
7. Choose the cluster or server, check the **XIMDD.war** check box and click **Apply.**
8. Confirm that the chosen cluster/server appears under the Server column and click **Next**.
9. Click **Finish**.

   The Installing... screen appears. After the application installs successfully, you see the following message: **Application XIMDD installed successfully**.
10. Click the **Save to Master Configuration** link, then click **Save**.
11. Click the **Applications** > **Enterprise Applications** link in the left menu pane.
12. Check **XIMDD** check box, then click **Start**.

    It displays a status, for example, if the installed application has been started successfully.

Deploying on WebLogic

To deploy Oracle Identity Manager Diagnostic Dashboard on WebLogic:

1. Log in to the administrative console.
   - Start the application server
   - In Internet Explorer, type the following URL:

     `http://localhost:7001/console`
2. Click the **Deployments** link on the left menu pane, then click **Web Application Modules** link in the left menu pane.
3. Click the **Deploy a new Web Application Module…** link, then click **Upload your file(s)** link to upload the XIMDD.war file.
4. Navigate to the location for uploading the WAR file. Typically this should be under the following:

   `WL_HOME\user_projects\domains\<your-domain-name>\<your-adminserver-name>\upload`.
5. Click the **Upload** button.

   Select the **XIMDD.war** radio button and click **Target Module**.
6. Click **Deploy** button.

   The next page displays the successful deployment of the application.

You can now use a browser and connect to the diagnostic dashboard.

Launching the Diagnostic Dashboard

Once deployed, you can access the Diagnostic Dashboard using the following URL template:

`http://<host>:<port>/XIMDD`.

In a clustered installation, you need to 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 tool indicates on which application server the tool is deployed. It also illustrates if Oracle Identity Manager is already installed in that application server or not. The tests displayed in the following table may vary, depending on whether the Oracle Identity Manager is installed or not and which application server is used. The following table displays the availability of these tests:

Test Name	Availability when Oracle Identity Manager is not installed	Application Servers
SQL Server JDBC Libraries Availability Check	Yes	JBoss
SQL Server Prerequisites Check	Yes	JBoss
Oracle Prerequisites Check	Yes	WebSphere/WebLogic/JBoss
WebSphere Embedded JMS Server Status	Yes	WebSphere
Database Connectivity Check	No	WebSphere/WebLogic/JBoss
Account Lock Status	No	WebSphere/WebLogic/JBoss
Data Encryption Key Verification	No	WebSphere/WebLogic/JBoss
Scheduler Service Status	No	WebSphere/WebLogic/JBoss
Remote Manager Status	No	WebSphere/WebLogic/JBoss
JMS Messaging Verification	No	WebSphere/WebLogic/JBoss
Target System SSL Trust Verification	No	WebSphere/WebLogic/JBoss
Java VM System Properties Report	Yes	WebSphere/WebLogic/JBoss
WebSphere Version Report	Yes	WebSphere
Oracle Identity Manager Libraries and Extensions Version Report	No	WebSphere/WebLogic/JBoss
Oracle Identity Manager Libraries and Extensions Manifest Report	No	WebSphere/WebLogic/JBoss
SSO Diagnostic Information	No	WebSphere/WebLogic/JBoss

Using the Diagnostic Dashboard

The Diagnostic Dashboard main screen includes the sections listed in the following table:

Items	Description
System Information Application Server	Displays the name of application server.
Oracle Identity Manager Installation	Display installation details 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	Display testing parameters if required for verifying the test.

To get the result:

1. Select the tests by clicking on the check box on the Diagnostic Dashboard main screen.
2. Enter necessary parameters if required.
3. Click **Verify** to see the result.

   The Diagnostic Dashboard Test Result screen appears and displays the status information listed in the following table:

Test Results	Description
Result Summary	The result summary shows all the selected test(s) with icons (pass/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 description of the test being verified.
Input Parameters	Displays the test parameters of the test being verified.
Result	Displays if the test has passed or failed.
Details	Details about pass/fail of test.
Back to Top	Takes you back to top of the page.

4. Click **Diagnostic Dashboard** link on the left menu pane to get back to previous test page.

Test Details and Parameters

The following tests are available for different application servers:

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: SQL Server Driver should be found.

Microsoft SQL Server Prerequisites Check

Application Server: JBoss

Prerequisite: The following are the prerequisite for verifying this test:

Prerequisite	Description
Database Server	Enter the location for database server.
Port	Enter the Port number.
Database Name	Enter the database name.
Oracle Identity Manager Database User Name	Enter Oracle Identity Manager database user name.
Oracle Identity Manager Database User Password	Enter Oracle Identity Manager database user password.

Description: Checks if the specified SQL server instance satisfies the prerequisites necessary for Oracle Identity Manager installation

Result: It will display the following information:

- Necessary privileges for user
- XA support should be enabled.
- SQL Server Version.

Oracle Prerequisites Check

Application Server: JBoss/ WebSphere/WebLogic

Prerequisite:

Prerequisite	Description
Database Server	Enter the location for 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 System User Name.
System User Password	Enter system user password.

Description: Checks if the specified Oracle instance satisfies the prerequisites necessary for Oracle Identity Manager installation. This test requires SYSTEM privileges.

Result: It will display the following information:

- Necessary privileges for user
- XA support enabled.
- JVM enabled.
- Oracle Version Information.

WebSphere Embedded JMS Server Status

Application Server: WebSphere

Prerequisite:

Prerequisite	Description
Host	Enter Host name.
Port	Enter Port number.
User Name	Enter User name.
Password	Enter Password.

Description: Checks the status of JMS Server. This test is valid for WebSphere only and requires Oracle Identity Manager to be installed.

Result: Displays the status of JSM Server.

Database Connectivity Check

Application Server: Jboss\ WebSphere\ WebLogic

Prerequisite: None

Description: Run this test to verify if Oracle Identity Manager is able to connect to the database or not. 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.

Account Lock Status

Application Server: Jboss\ WebSphere\ WebLogic

Prerequisite:

Prerequisite	Description
User Name	Enter User name

Description: Oracle Identity Manager locks an account when there are successive multiple invalid login attempts. This test checks if a given account is locked or not.

Result: Checks for locked/unlocked accounts in database.

Data Encryption Key Verification

Application Server: Jboss\ WebSphere\ WebLogic

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 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 database key is present in Oracle Identity Manager configuration directory

Scheduler Service Status

Application Server: Jboss\ WebSphere\ WebLogic

Prerequisite: None

Description: Checks the status of the Oracle Identity Manager Scheduler Service running on this server.

Result: Displays the status of scheduler service.

Remote Manager Status

Application Server: Jboss\ WebSphere\ WebLogic

Prerequisite: None

Description: Reports the status of the Remote Managers that this Oracle Identity Manager installation is all set to work.

Result: Displays the status of Remote manager.

JMS Messaging Verification

Application Server: Jboss\ WebLogic

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 JMS message.

Target System SSL Trust Verification

Application Server: Jboss\ WebSphere\ WebLogic

Prerequisite:

Prerequisite	Description
Host	Enter Host name
Port	Enter Port number.
Trust Store Location	Enter location for storage.
Trust Store Password	Enter password for storage.

Description: Oracle Identity Manager should be setup to trust the Target System certificates if the connectivity is over SSL. Enter the Host name and the port where a Target System is listening for SSL connections.

Result: It displays the following information:

- Valid/Invalid Host and Port address
- Trusted Certificates.

Java VM System Properties Report

Application Server: WebSphere

Prerequisite: None

Description: Prints out all the Java VM system properties

Result: It displays all the Java VM system properties

WebSphere Version Report

Application Server: Jboss\WebSphere\WebLogic

Prerequisite: None

Description: Obtains the WebSphere Application Server version information along with a list of all the fix packs and components installed in the application server

Result: Displays WebSphere version information

Oracle Identity Manager Libraries and Extensions Version Report

Application Server: Jboss\WebSphere\WebLogic

Prerequisite: None

Description: Reports the version of the Oracle Identity Manager libraries and extensions

Result: Displays the versions of the Oracle Identity Manager libraries and extensions

Oracle Identity Manager Libraries and Extensions Manifest Report

Application Server: Jboss\WebSphere\WebLogic

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.

SSO Diagnostic Information

Application Server: Jboss\ WebSphere

Prerequisite: None

Description: Provides information pertaining to SSO setup. Also, provides instructions needed to setup Oracle Identity Manager to enable retrieving run-time diagnostic information related to SSO logins.

Result: Displays if the SSO setup is enabled for related Oracle Identity Manager installation.

A

Understanding Attestation

Attestation enables reviewers to be notified of a report they must review that describes the provisioned resources that certain users have. The reviewer can attest to the accuracy of the entitlements by providing a response. This attestation action, along with the response the reviewer provided, any associated comments, and an audit view of the data that the reviewer viewed and attested 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 a business process that is hard-coded with configuration parameters in Oracle Identity Manager that creates an attestation task for a user in Oracle Identity Manager. 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 kicked off, 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 sub-flows in the provisioning processes defined in Oracle Identity Manager.

Attestation activity can be initiated on a periodic or an ad-hoc basis.

A reviewer can delegate particular entitlements in an attestation task to someone else for review. This creates another attestation task that is assigned to the delegated user.

This appendix discusses the following topics:

Definition of an Attestation Process

An **attestation process** is the mechanism by which an attestation task gets set up. It therefore needs to know how to define all the components that make up the attestation task, and associate it with a schedule at which it needs to occur. This definition is also the basis on which the same attestation task can be initiated on an ad-hoc basis. Thus, an attestation process definition will include:

- **Attestation Type**: There are two types of attestation processes:
  - User Entitlement Attestation: This conforms with the user-based attestation scope
  - Resource Entitlement Attestation: This conforms with the resource-based attestation scope
- **Attestation Scope**: This defines the algorithm by which the target user entitlements of the attestation process will be calculated. This will be based on the type
- **Reviewer Setup**: Who the reviewer needs to be
- **Definition of Attestation Schedule**: When attestation process should be kicked off on a scheduled basis
- **Process Owner**: This is a designated group of users that are responsible for monitoring any activities related to the process.
  - They will be notified of any issues that occur when the process executes.
  - They will have privileges to view the Process Definition, but will not have admin privileges by default
  - They will have the ability to execute the process in an ad-hoc manner
- **Process Administrators**: These are the groups of users that have administrative privileges over the process definition. This essentially maps to our normal 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.

Attestation Process Control

The following sections describe how you can control attestation processes.

Disabling Processes

Any attestation process can be disabled in order to prevent it from running at its preconfigured schedule. This control gives an administrator better control over the environment. A disabled attestation process can be enabled, but it cannot be enabled if its next run time is in the past. A user who enables an attestation process must set its next run time in the future.

Deleting Processes

Any attestation process can be deleted. This is be a soft-delete. It does not actually delete the records, since these must be maintained for audit purposes. Instead, the attestation process will be marked as deleted.

A deleted process no longer appears in the administrative interfaces. Since process names and codes are unique, a name once used is no longer available, and no new attestation process may be created with the same name.

Components of an Attestation Task

The basic purpose of the attestation process is to set up an attestation task in Oracle Identity Manager. The attestation task appears in a user's attestation inbox. The following are the basic components of an attestation task

- **A Reviewer**: The user who performs the attestation.
- **Task Source**: This specifies whether the attestation task came about as 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 was the source of the entitlements.
- **Attestation Scope**: Defines what the reviewer has to attest to. This is a list of user provisioned resource instances defined as follows:
  - **Resource-Based**: All user provisioned resource instances being attested to are for the specified resource. The scope is any user who has a non-revoked instance of the specified resource.
  - **User-Based**: The user entitlements being attested to are for a specific set of users. The reviewer attests to all the appropriate entitlements for the users in the set.
- **Attestation Data**: Detailed data for the user entitlements in the attestation scope. This is basically data from the process form of the provisioned resource instance
- **Attestation Date**: Defines the date on which the attestation task was initiated, and the point in time with respect to the attestation data that the user must attest to. Note that the reviewer does not attest to what the user has today. They attest to what the user had on the date specified in the attestation task. Usually, the two dates are the same. But the distinction eliminates complexities due to activity lag.
- **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 should 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 where processes have been configured incorrectly, and is useful in early stages of a rollout.
  - **Delegate**: The reviewer wants to reassign the attestation of this entitlement to another qualified person.

Important 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, proxy management, and so on.

The Attestation Inbox

The attestation inbox enables you to manage attestation tasks that are assigned to them.

From this inbox, you can see the attestation tasks assigned to you, view the details of the tasks, and provide responses and comments.

Attestation Request

When an attestation process is executed, an attestation request is created and recorded in the Oracle Identity Manager data store. This request acts as an audit record of the times that an attestation process is executed. The attestation request record consists of basic identifying 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

Financially Significant Resources

An administrator can mark each resource object definition in Oracle Identity Manager as being financially significant or not.

The role of this property is to flag resources that should have some kind of attestation coverage. This can then be used in determining the following:

1. What resources that do not have an attestation process defined should have one
2. What resource entitlements that have not been attested to should have been

When determining the user entitlements that need attestation as part of an Attestation Process that has user-based attestation scope, only those entitlements of a user will be considered that are for a resource marked as being financially significant.

When a resource is created, this flag will default to **off** (not financially significant).

Delegation

If 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:

- There may be too many entitlements covering too many users in the attestation task
- The reviewer does not have enough visibility into the users that the entitlements pertain to

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. The new task that 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 did the delegation, which task it was spawned from, and all the other usual information, for example, the request ID, and so on. The new attestation task is treated in the same manner as any other attestation task. It can even be delegated.

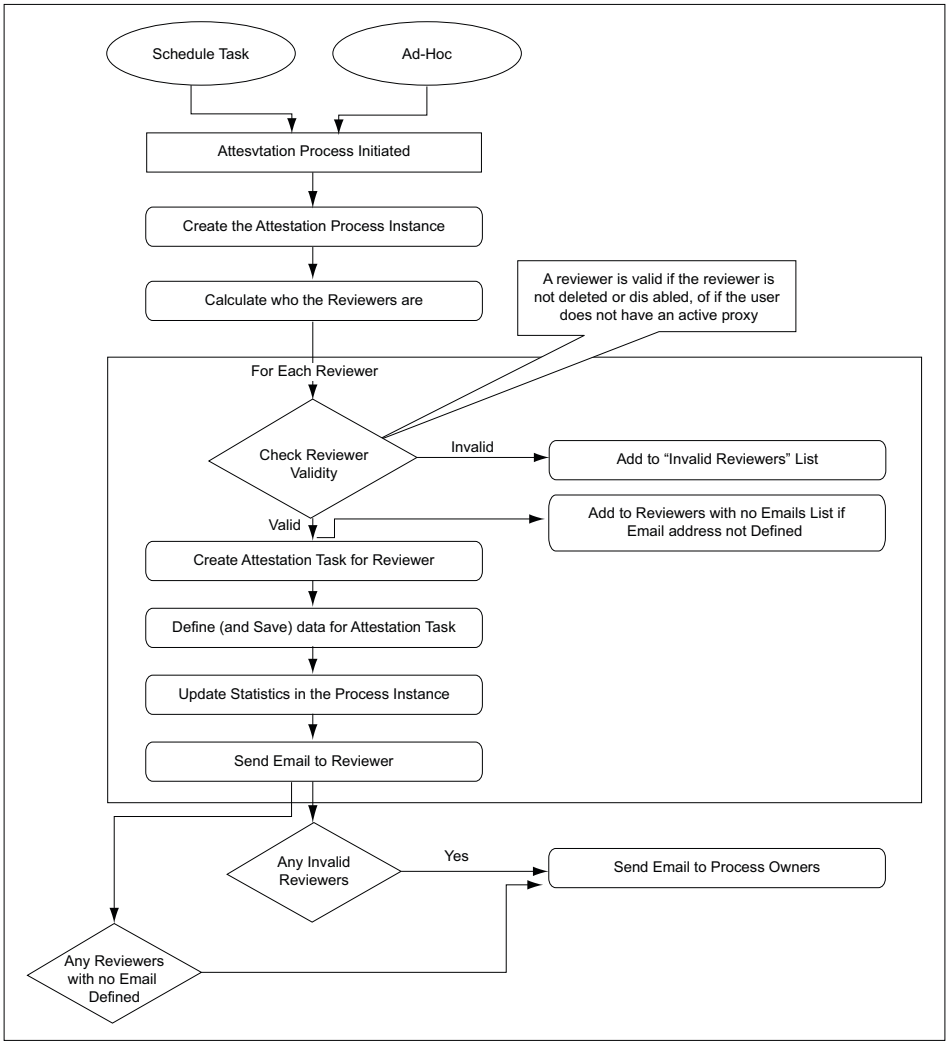
The Attestation Lifecycle Process

The following is a description of the attestation lifecycle in Oracle Identity Manager.

Stage 1 - Creation of Attestation Task(s)

This is the stage starts when an attestation process is run. The flowchart in Figure A–1 describes the workflow.

Figure A–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, but there can be a set of reviewers.

For each reviewer, the process creates an attestation task, and sets its associated attestation date. If the reviewer is invalid, the process adds the name and other details of the reviewer to a list of bad reviewers. A reviewer is invalid if the Oracle Identity Manager User record is disabled or deleted, or if the user has a proxy that is currently active. It also computes a list of reviewers with no email address defined.

For each valid reviewer, the process calculates all the user entitlements that the reviewer needs to attest to as part of that task, as determined by the attestation scope defined in the process. If the attestation scope is user-based, it retrieve only the resources that are marked as being financially significant. The process then adds a reference and any related information regarding those user entitlements to the attestation data of the task. It also takes the number of entitlements covered by that task, and adds it to the statistical field for **Total Number of Entitlements identified for Attestation** in the process instance. The process then sends an email message to the reviewer.

After examining each reviewer, the process checks for invalid reviewers and emails a list of invalid reviewers, if there are any, to the process owner. It also sends email to process owners about the reviewers with no email address defined.

At the end of this stage, all the attestation tasks are in the attestation inboxes of the reviewers.

Stage 2 - Acting on an Attestation Task

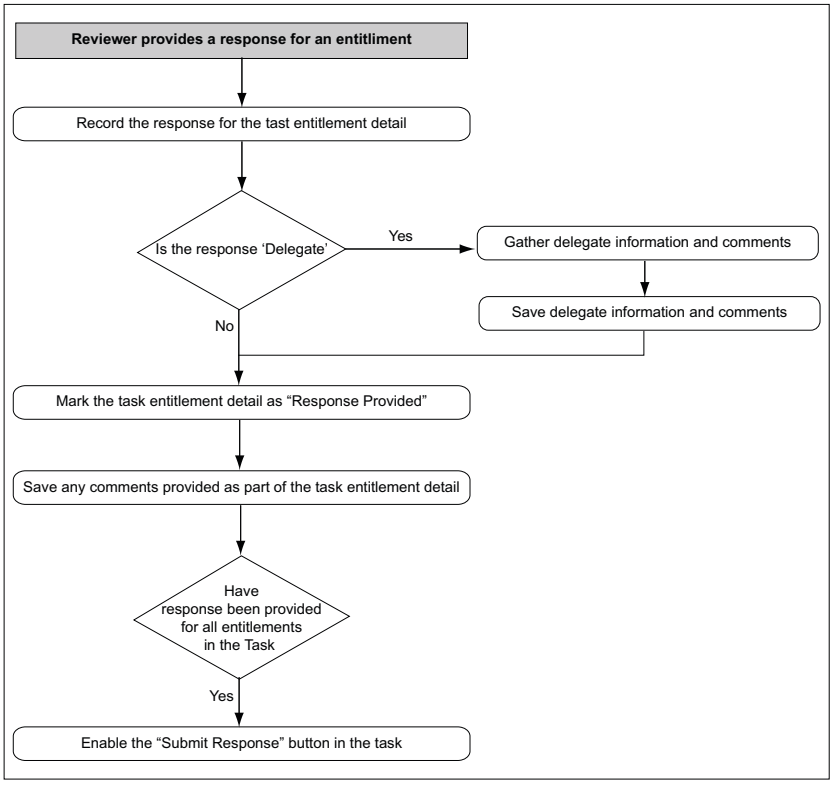
When an attestation task is assigned to a reviewer, they receive an email, and the task appears in their attestation inbox. The reviewer views task details in their attestation inbox.

From the task details page, the reviewer provides a response and an optional 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, the reviewer must provide a delegated user. Optionally, the reviewer can provide comments regarding why they are delegating the attestation activity to that user.

After the reviewer provides responses to all entitlements, he or she can commit their action for the attestation task by submitting all responses.

Figure A–2 Flow of Events when Reviewer Responds to Entitlement



At this point, the next stage of the Attestation Business Process would kick off.

Stage 3 – Processing a Submitted Attestation Task

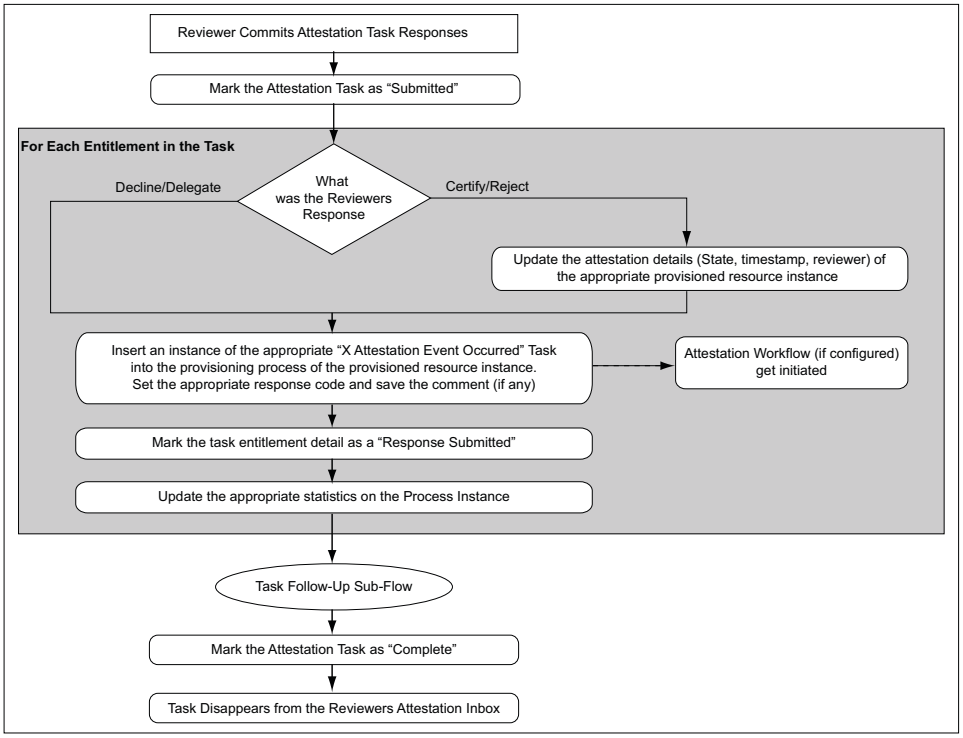
The Attestation Task is marked as **Submitted**. At this point the attestation task is frozen, and cannot be acted on further. For each entitlement in the attestation task, the response is examined.

If the response is either to certify or reject, 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, the attestation detail at the provisioned resource level is not changed.

Depending on the attestation process type, the **User Attestation Event Occurred** or the **Resource Attestation Event Occurred** task is inserted into the provisioning process of the resource instance. This kicks off any attestation driven workflows that may have been defined. Any comments are saved to the task's notes field.

The attestation entitlement detail in the task is marked as **Response Submitted**.

Figure A–3 Flow of Events After Attestation Task Response is Submitted



The following statistics are updated on the process instance:

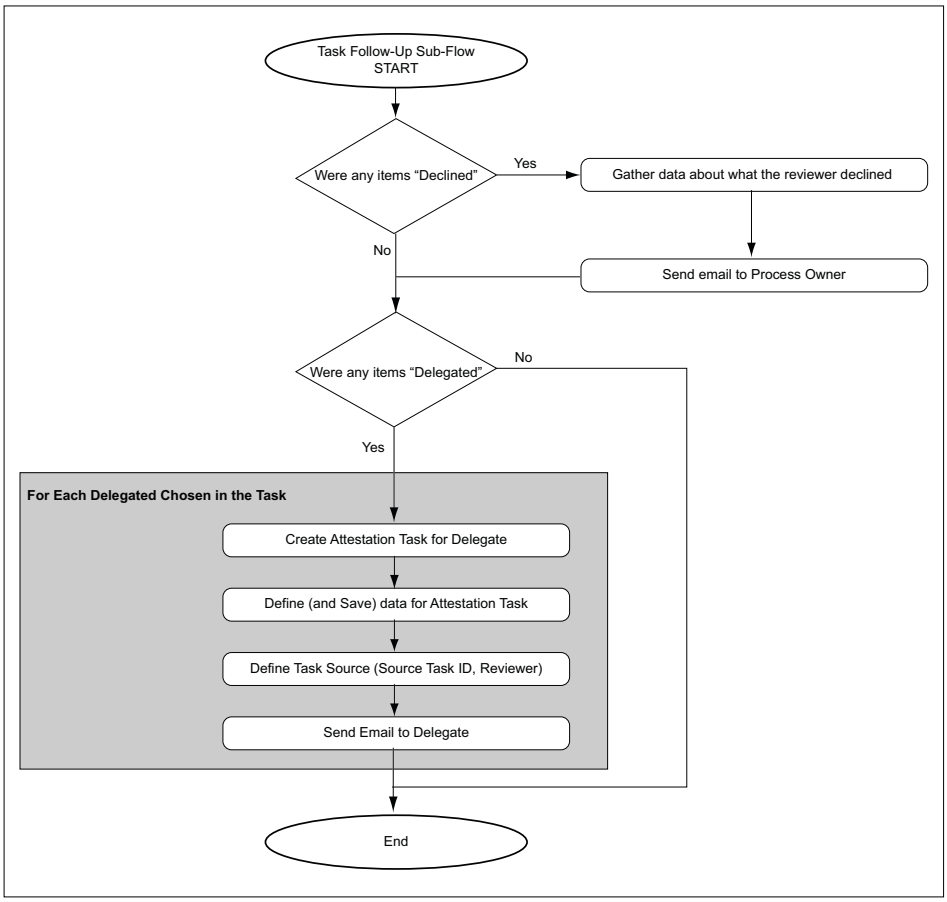
- Number of Entitlements certified
- Number of Entitlements rejected
- Number of Entitlements declined
- Number of Entitlements delegated

After all entitlements are covered, a sub-flow 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 email to the Process Owner outlining the details of the refusal.

Next, the process examines if the response for any of the entitlements in the task was delegated. If there were any such entitlements, the process identifies all users the reviewer selected as a delegate, and creates an attestation task for each. Each attestation task is for just only the entitlements that the reviewer delegated to the user. The delegated user receives email notification of the delegation.

After all the delegated attestation tasks are created, the sub-flow finishes and joins back into the main flow.

Figure A–4 Follow Up Action Sub-Flow



With the follow-up flow complete, the attestation task is marked as **Complete**.

The 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 ad-hoc execution. It supports both drivers for initiation of attestation processes.

The attestation engine uses messaging to off-line processing when appropriate to create transaction separation, and ensure that there are no end-user performance issues.

Attestation Scheduled Task

A new system scheduled task that is responsible for examining the Attestation Processes defined in Oracle Identity Manager, and creating the necessary attestation tasks in the system.

Salient features of this scheduled task are:

- Out of the box, this scheduled task will be set to run every night. This is just the default value we provide; the customer will be able to change this to their needs
- It will examine the attestation process definition table for all active (not disabled) attestation processes
- For any process it finds that needs to be run (its next scheduled start time is in the past), it will initiate a call to the Attestation Engine to initiate the attestation process.

Attestation Driven Workflow Capability

The provisioning processes defined in Oracle Identity Manager will be enhanced to listen to triggers coming from Attestation activity. In this way, a customer could 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 – either "User Attestation Event Occurred" or "Resource Attestation Event Occurred" – would provide the audit trail for the attestation history of the specific user entitlement.
  - There would be one instance of this task for each time that resource instance was attested by the appropriate type of attestation process
  - The response code set on the task would indicate what the response provided by the reviewer was
  - The user tagged as the person creating the task would indicate who the reviewer was
  - Any comment provided by the user would be in the notes field for the task
- Using response-generated tasks, the default task can kick off workflow to respond to a particular attestation response received. So, for a particular resource, the customer could configure that the "Reject" response should kick off the appropriate workflow tasks in the provisioning process for disabling the account, as an example.

Emails

As part of the Attestation Processes, the Attestation Engine will send out emails to various interested parties. In order to make the emails configurable by the customer with respect to content, they will be made available as email templates of type 'General' in the Oracle Identity Manager Email Definition store. For context-sensitivity, the emails will support a set of email variables, that will be replaced by the appropriate values.

Notify Attestation Reviewer

This template is used to build the email to send to the reviewer when an attestation task is assigned to him or her.

Variables

The following are variables in the Notify Attestation Reviewer template:

Variable Name	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

Subject Line

The following is the Subject line of email 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
```

Body

The body of the email 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>
```

Notify Delegated Reviewers

This template is used to build the email to send to a reviewer when an attestation task is delegated to him or her.

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 was Assigned
<Attestation Task.Delegated By First Name>	First Name of reviewer that did the delegation
<Attestation Task.Delegated By Last Name>	Last Name of reviewer that did the delegation
<Attestation Task.Delegated By User Id>	User ID of reviewer that did the delegation

Subject Line

The following is the Subject line of email 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*>

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*>]

Notify Process Owner about Invalid Attestation Reviewers

The Invalid Attestation Reviewers template is used to build the email to send to process owners notifying them of any invalid reviewers found while generating attestation tasks within a process.

Variables

The following are variables in the Notify Process Owner about Attestations Reviewers template:

Variable	Definition
<*Attestation Request.Request Id*>	ID of the Attestation Request
<*Attestation Definition.Process Name*>	Name of the Attestation Process
<*Attestation Request.Request Creation Date*>	Date the Attestation Request was created
<*Attestation Task.Reviewer First Name*>	First Name of reviewer that was invalid
<*Attestation Task.Reviewer Last Name*>	Last Name of reviewer that was invalid
<*Attestation Task.Reviewer User Id*>	User ID of reviewer that was invalid
<*Attestation Task.Reviewer Invalid Reason*>	Reason the reviewer was invalid

Subject Line

The following is the Subject line of email messages defined by the Notify Process Owner about Attestations Reviewers template:

Some of the reviewers are invalid for the attestation process <*Attestation Definition.Process Name*>, request <*Attestation Request.Request Id*>

Body

The body of the message contains the following information:

The following attestation process generated some invalid reviewers.

Attestation process: <*Attestation Definition.Process Name*>
Attestation Request ID: request <*Attestation Request.Request Id*>
Request date: <*Attestation Request.Request Creation Date*>

Invalid Reviewers: <*Attestation Task.Reviewer First Name*> <*Attestation Task.Reviewer Last Name*> [<*Attestation Task.Reviewer User Id*>] - <*Attestation Task.Reviewer Invalid Reason*>

Special Comments

Each reviewer detail will appear in a new line if there are more than one.

Notify Process Owner about Declined Attestation Entitlements

The Notify Declined Attestation Entitlements template is used to build the email to send to process owners notifying them of any declined entitlement attestations.

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 reviewer
<*Attestation Task.Reviewer Last Name*>	Last Name of reviewer
<*Attestation Task.Reviewer User Id*>	User ID of reviewer
<*Attestation Data.Provisioned User First Name*>	First Name of user being attested
<*Attestation Data.Provisioned User Last Name*>	Last Name of user being attested
<*Attestation Data.Provisioned User User Id*>	User ID of user being attested
<*Attestation Data.Resource Name*>	Name of resource being attested
<*Attestation Data.Entitlement Descriptive Data*>	The descriptive data of the entitlement being attested

Subject Line

The following is the Subject line of email 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*>

Body

the following appears 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*>

Special Comments

Each entitlement data will appear in a new line.

Notify Process Owner About Reviewers with No Email Defined

The Attestation Reviewers With No Email Defined template is used to build the email to send to process owners notifying them of any reviewers where there is no email address defined

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 the Attestation Request was created
<Attestation Task.Reviewer First Name>	First Name of reviewer that was invalid
<Attestation Task.Reviewer Last Name>	Last Name of reviewer that was invalid
<Attestation Task.Reviewer User Id>	User ID of reviewer that was invalid

Subject Line

The following is the subject line for emails defind by the Notify Process Owner About Reviewers with No Email Defined template:

```
Email address is not defined for some of the reviewers in attestation process
<Attestation Definition.Process Name>, request <Attestation Request.Request Id>
```

Body

The following is the body of the message:

```
The following attestation reviewers do not have email addresses defined.
Attestation requests have been generated for these reviewers and can be accessed
by logging into Oracle Identity Manager. However, notification emails 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>]
```

Special Comments

Each reviewer detail will appear in a new line if there are more than one.

B

System Configuration Considerations for Administrators

This appendix describes settings that you may want to enable and records that you may need to create, depending on what features of the Administrative and User Console that you want to enable. This includes configuring resource definitions, process forms, approval processes, and other records that affect provisioning in the Oracle Identity Manager Design Console and editing the relevant configuration files to support the functionality in the Oracle Identity Manager Administrative and User Console. Not all of these settings are relevant for all users.

Review this section prior to deploying your Oracle Identity Manager Administrative and User Console to ensure that you have configured the product to function as intended.

> **Note:** To customize the Oracle Identity Manager Administrative and User Console user interface, see the *Oracle Identity Manager Administrative and User Console Customization Guide*.

Administration and User Console function	Description
Registration functions for users	
To allow users to self register in Oracle Identity Manager	Set the **Is Self-Registration Allowed** property in the System Configuration form to **true**. The System Configuration form is available in the Oracle Identity Manager Design Console.
To require users to select their verification questions and provide answers to these question when registering	Set the **Does user have to provide challenge information during registration** property in the System Configuration form to **true**. The System Configuration form is available in the Oracle Identity Manager Design Console.
To designate the number of verification questions that the user must answer	Set the **Number of Questions** property in the System Configuration form to the number of questions that you want users to answer. Be sure that the number of questions you supply in the **Lookup.WebClient.Questions** lookup definition is equal to or greater than the value of the **Number of Questions** property. You may need to create additional questions. The System Configuration form is available in the Oracle Identity Manager Design Console.

Administration and User Console function	Description
To designate the list of questions that users select from when setting their verification questions and answers.	Define a row on the **Lookup.WebClient.Questions** lookup definition for each question in the **Lookup Definition** form. The Lookup Definition form is available in the Oracle Identity Manager Design Console.
To require an approval for self registration	Define an approval task in the **User Registration** approval process.
To configure different workflow approvals for self registration depending on user profile information	Define additional approval processes for the **Request** resource definition and create a rule of type **process determination** with a rule element that at least requires that the request object action is **Create Entity**. Associate the new rule with the approval process on the **Request** resource definition to enable Oracle Identity Manager to determine which process to select.
To automatically add a user to groups based on self registration	Define rules of type **general** and attach them to the user group definitions to which you want users to be added upon registration. This enables Oracle Identity Manager to determine which groups to add users to based on the criteria they enter upon registration. The criteria in the rules must match the user-entered criteria.
Access privileges	
To designate the pages to which all users are to be allowed access	Specify these pages on the Menu Items tab of the **All Users** user group.
To designate the pages to which various administrative groups are to be allowed access.	Specify these pages on the Menu Items tab of the applicable administrative user groups, for example, System Administrators, AdminGroup1, and so on.
Account creation functions for administrators	
To allow administrators to create an Oracle Identity Manager account for other users	Ensure that the groups that these administrators belong to are added to the Administrators tab of the organizations that contain the users they are to administer.
To configure fields for administrators to supply data when creating the user account.	Create these fields in the `FormMetaData.xml` file. See the *Oracle Identity Manager Administrative and User Console Customization Guide* for details.
To specify fields that are required when creating a user account.	Create these fields in the `FormMetaData.xml` file. See the *Oracle Identity Manager Administrative and User Console Customization Guide* for details.
To specify the groups of which a user is automatically made a member.	Define rules of type **general** and attach them to the user group definitions to which you want users automatically added upon registration. This enables Oracle Identity Manager to determine which groups to add users to based on the criteria entered when their account was created. The criteria in the rules must match the entered criteria.

Administration and User Console function	Description
To designate the groups to which administrators can add users who they administer	Ensure that the groups of which these administrators are members are added to the Administrators tab of the group definitions to which you wish to allow them to add users.
Profile editing functions for users	
To require an approval for user-initiated Oracle Identity Manager profile updates	Define an approval task in the **User Profile Edit** approval process
To configure different workflow approvals for user-initiated profile updates	Define additional approval processes for the **Request** resource definition and create a rule of type **process determination** with a rule element that at least requires the request object action to be **Modify Entity**. Associate the rule with the approval process on the **Request** resource definition to enable Oracle Identity Manager to determine which process to select.
To control which fields users can edit in their own profiles	Configure the fields in the `FormMetaData.xml` file. See the *Oracle Identity Manager Administrative and User Console Customization Guide* for details.
Account modification functions for administrators	
To control which users can edit the profiles of other users	You must designate the forms to which members of the various administrative groups are to have access. You must also add these groups to the **Administrators** tab of the Organizations that contain the users they are to administer.
To control which Oracle Identity Manager system fields (for example user ID, first name, and so on) administrators can edit.	You must designate which fields you want to allow administrators to edit for other users. The fields you want to make editable must be specified in the *FormMetaData.xml* file. See the *Oracle Identity Manager Administrative and User Console Customization Guide* for details.
To control which User-Defined fields (for example Social Security number, local identity, and so on) administrators can edit.	You must designate which fields you want to allow administrators to edit for other users. Depending on the pages in the Administrative and User Console on which these fields will appear, you may need to edit the *FormMetaData.xml* file to add attribute definitions and references for these fields. See the *Oracle Identity Manager Administrative and User Console Customization Guide* for details.

Index

A

C

D

E

G

H

J

M

O

P

R

S

T

U

V

W