Oracle® Identity Manager

Administrative and User Console Guide

Release 9.0

B25936-01

May 2006

ORACLE®

Oracle Identity Manager Administrative and User Console Guide, Release 9.0

B25936-01

Primary Authors: Deepa Aswani, Don Gosselin

Contributors: Jatan Rajvanshi, Raj Kuchi, Semyon Shulman

Contents

5 My Resources

6 Requests

7 To-Do List

8 Users

9 Organizations

10 User Groups

11 Access Policies

12 Resource Management

13 Deployment Manager

14 Reports

15 Attestation

16 Working with the Diagnostic Dashboard

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 and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *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 Best Practices Guide*

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, yet flexible, provisioning system for automatically granting and revoking access to enterprise applications and managed systems. Oracle Identity Manager is used to provide access to enterprise resources to staff and partners and enforce any access policies that may be associated with these resources

With Oracle Identity Manager, you can:

- View your Oracle Identity Manager user account (group memberships, e-mail address, and so on).
- Modify your profile.
- Review the resources to which you have been granted access.
- View requests that have been made by you and for you.
- Make requests for additional resources for yourself.
- Reset 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 the rights that have been granted to you within Oracle Identity Manager, you may also be able to:

- Update passwords and user IDs for accounts on resources with which 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 remainder of this manual will describe the various actions you can perform within Oracle Identity Manager in the following sections:

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

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

If you wish to customize additional functionality associated with your *Oracle Identity Manager Administrative and User Console*, refer to the *Oracle Identity Manager Administrative and User Console Customization Guide*.

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 is responsible for management of users, organizations, user groups, resources, and policies.
Approver	A person who is responsible for approving and denying access to resources.
End-User	A person using self-service features of Oracle Identity Manager and who is not an administrator.

Overview of the Resource Model

Oracle Identity Manager allows for resources to be requested and provisioned to enterprise users. The resource you or your users are provisioned with can be an application, access to a database, and rights to a directory structure on a network, or any other entity to which access is vital. The manner in which access to that resource is granted and the rights and permissions you will ultimately be provided with on that resource are all governed by the provisioning processes defined by your Oracle Identity Manager Administrator. Access to a resource may be provisioned uniformly for all users or in a unique fashion, based on variables such as your role (for example, administrator, accountant), location, employment status (for example, full time, consultant), group or department designation or other criteria that have been deemed relevant by the resource-specific and Oracle Identity Manager administrators.

Once a resource is successfully provisioned to you, you will be able to 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 would then be able to login to that application directly, 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. As a result, Oracle Identity Manager has two

different types of resource-related processes: approval processes and provisioning processes.

Approval Processes

An approval process is used to determine whether a resource is to be approved or not for provisioning to the user(s) or organization(s) for whom it was requested. Approval processes are comprised 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 will be assigned to an approver or a group of approvers.

Approvers are able to act upon all tasks within an approval process that are assigned to them. In addition, if an approver has a task within a request assigned to them, he/she will be able to view all tasks within that request. If you are an approver on a request, that request ID will be displayed 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 would be granted as soon as the request was submitted.

Provisioning Processes

A provisioning process is the process used to actually provision the resource to the user(s) or organization(s) for whom it was requested. Provisioning processes are comprised 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 utilize a special form to prompt users for, and capture, data required to grant access to a resource.

2

Self-Registration

This chapter describes how to create an account in Oracle Identity Manager and then log in and out of Oracle Identity Manager using that account in the following sections:

Creating an Oracle Identity Manager Account

If you do not already have account in Oracle Identity Manager, you will need to create one.

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

1. To create an account for yourself, access your corporate portal link to Oracle Identity Manager.

> **Note:** The user ID cannot include the following characters: , # + \ ; ' \ " < > /

2. Click **Create Request** under **Self-Register**. The User Self-Registration page will be displayed. Enter all the required data and be sure to select and specify answers to your password challenge questions (if your system is set to require them).

> **Note:** Depending on how your system administrator has configured Oracle Identity Manager, you may be required to specify answers to a number of challenge questions. You will then need to provide the correct answers to these questions in the event you forget your password.

3. Click **Submit Request**. Oracle Identity Manager will inform you that the request has been submitted and display the numeric ID of the request so that you can

track it. In addition, a link to the request will be displayed. To track the request, click **Track Request**. The Track Self-Registration request page appears.

Note: Depending on how your system is configured, requests for self-registration may require approvals. If your system administrator has set Oracle Identity Manager to require approvals for self-registration requests, you can track the status of that request using the Track Request link. As soon as the required approvals are obtained, your account will be ready for use. If approvals are not required, your account will be created and available for use as soon as Oracle Identity Manager has processed your self-registration request.

Resetting Your Password

If you have forgotten your Oracle Identity Manager password, click the **Forgot Password**? link in the left-hand panel. You will be prompted to answer several validation questions. If you supply the correct answers to these questions, Oracle Identity Manager will allow you to reset your password.

1. Click the **Forgot Password** link. The Oracle Identity Manager Verify User ID page will be displayed.
2. On the Oracle Identity Manager Verify UserID page, enter your ID in the **User ID** field and click **OK**. The Oracle Identity Manager **Reset Password** page will be displayed.
3. The questions that you will be presented with under these circumstances (as well as the answers) are specified in your account options. You will be required to select which questions you wish to be presented with (for forgotten passwords) the first time you login to Oracle Identity Manager Administrative and User Console. You will be required to supply the correct answers to your password challenge questions. Then, enter your new password (in both fields) and click **Submit**.

Note: f you have forgotten your Oracle Identity Manager User ID, you will need to contact your Oracle Identity Manager system administrator.

If you have exceeded the maximum number of retry attempts, your Oracle Identity Manager account will be automatically locked to prevent further attempts at login. If you account is locked, you must contact your system administrator to have your account unlocked. Alternately, you can click the **Forgot Password**? Link and provide the answers to your challenge questions. You will then be able to reset the password (the account will be unlocked automatically). However, if you exceed the maximum number of attempts to correctly answer your challenge questions, your account will be locked and can only be unlocked by your Oracle Identity Manager system administrator.

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 for self-registration within Oracle Identity Manager, you can track the status of that approval and

self-registration process using Oracle Identity Manager. To track the status of a self registration request:

1. 1.Click **Track Request** under **Self-Registe**r. The **Oracle Identity Manager Track Self-Registration** page appears.
2. 1.On the Oracle Identity Manager Track Self-Registration page, enter the ID of the request associated with your self-registration in the Request ID field. Then, click **Track Request**. Oracle Identity Manager will display the details regarding the date on which the request for self-registration was submitted and it's current status.

Logging In to the Administrative and User Console

To log in to the Oracle Identity Manager Administrative and User Console, you must first ensure that you have an account within that application. If you do not currently have an account, you will need to create an account for yourself (using the **Create Request** link under **Self Register** on your corporate portal to Oracle Identity Manager) or contact your manager to have an account created for you.

1. Once you have an account, 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

1. Click **Logout**. Oracle Identity Manager will prompt you to with a confirmation message.
2. Click **Logout** or **Cancel**. Once you have logged out of Oracle Identity Manager, you can choose to return to your company's Web site or close your browser.

Note: You may be automatically logged out of Oracle Identity Manager due to inactivity after a specific period of time.

This Logout button is only available in a non-Single Sign On (SSO) environment.

3

Using Oracle Identity Manager

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

- Searching in Oracle Identity Manager
- Understanding Special GUI Behavior

Searching in Oracle Identity Manager

Many fields within Oracle Identity Manager pages come with lookup capabilities. These capabilities are very useful when you need to locate a record (a particular user account) or assign a particular entity to a record (for example, adding users to requests). Some fields come equipped with pre-defined menu choices, others provide full search capabilities (also referred to as a query function).

This section covers the following topics related to searching:

- Constructing a Search Query
- Using Wildcards
- Understanding Search Behavior

Constructing a Search Query

When searching for a particular record, there may be one or more fields in which you can supply information before clicking **Search**. Enter as much information as is available to you about the record you are trying to locate. For example, if you are only able to remember a user's first name, enter that and leave the other fields blank. Oracle Identity Manager will then display 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 will display all records of that type. If you wish to restart a search, click **Clear**. Some screens also provide a Cancel button that you can click to cancel a search.

Using Wildcards

In additional to using the various fields to limit the records retrieved by your search, you can also use wildcard characters with the values you enter in a particular search field. This will cause Oracle Identity Manager to further filter your search.

The asterisk (*) wildcard character is used to represent unspecified portions of field values in a search. You can use the asterisk at the beginning, middle, or end of the value you are entering within a given field. For example, if you enter b* in the **User ID** field and execute a search, Oracle Identity Manager will display 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 will display 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 will retrieve all records that end in A (for example, laura, maria, and so on).

Understanding Search Behavior

Depending on the type of search you are performing, the manner in which the search is constructed and executed will differ. In addition, the results you retrieve will vary based on the context in which you are executing the search. A brief explanation of these differences is provided here.

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

If you are performing a user record search while creating or tracking a request, Oracle Identity Manager will only show users for whom you are the manager or administrator. In addition, the search parameters you enter will be combined to retrieve results. For example, if you enter John in the First Name field and **NYoffice** in the **Organization** field, Oracle Identity Manager will display 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 GUI Behavior

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

- Displaying Text Entries with Three Dots
- Displaying Process Forms with Child Tables

Displaying Text Entries with Three Dots

The Administrative and User Console will display text entries as truncated followed with three dots (…) at the end to indicate that the field length is insufficient for the entire entry. Here are two example when this occurs:

The web page, **User Detail >> Resource Profile >> Resource Provisioning Detail** displays some names in the Task Name field as partial entries.

During direct provisioning or request provisioning through the use of the Provisioning wizard (**Provision Resource to User** page), the Child table is displayed when you click Add to add child objects. The text entries in the Child table are partially displayed.

This display of entry is normal behavior. You can customized the field to show the entire entry name by modifying the global.property.tableColumnSize in xlWebAdmin.properties file and changing the default of 25 characters to a larger string value. The xlWebAdmin.properties file is located inside the xlWebApp.war file, which is located in the XellerateFull.ear file. You can find the xlWebAdmin.properties file in the

<XL_HOME>/xellerate/webapp/precompiled/jsp-temp/WEB-INF/classes directory.

Displaying Process Forms with Child Tables

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

To display a child table with more than 10 columns, change the value of the global.property.NumberOfChildTableColumns property in the xlWebAdmin.properties file, which is set to 10 by default. Set this value to the number of columns you want displayed.

Here are some Administrative and User Console page examples, which will display the child table with 10 columns at a time:

- The **User Detail >> Resource Profile**: Click the Edit and View links for the Resource and Process Form.
- The **User Direct Provisioning Wizard >>Step 3** through **Step 6**.
- The **Organization Detail >> Resource Profile**: Click the Edit and View links for the Resource and Process Form.
- The **Organization Direct Provisioning Wizard >>Step 3** through **Step 6**.

In the **Resource Detail >> Organizations Associated with this Resource**, click the Edit and View links for the Resource and Process Form.

4

My Account

This section describes how to access information related to your Oracle Identity Manager. When you first log in, you will see the Welcome to Oracle Identity Manager page. To view your account information, click the **My Account** link. The following sections describe the tasks associated with managing your account in Oracle Identity Manager:

Viewing and Modifying Your Account Profile

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

> **Note:** The fields you will be able to edit within your own user profile will depend on how your administrator has configured Oracle Identity Manager.

1. Click **My Account** in the Explorer Menu. Then click the **Modify Account Profile** button in the **Account Profile** page. Oracle Identity Manager then displays the account information.
2. Make the desired changes and click **Save Profile**. If approvals are required for changes to the user profile, a request for this change will be submitted and you will be able to track the approval of that change using the request ID displayed. Otherwise, the change will take effect as soon as Oracle Identity Manager has processed your user profile edit request (depending on the load on your system, this may require several minutes) and the request is also created in Oracle Identity Manager for auditing purposes.

Resetting Your Password

Oracle Identity Manager provides you with the ability to change your system password. Also, depending on local system settings, you may be required to periodically reset your password (for example, to maintain system security).

1. Click **My Account** in the **Explorer** Menu. Then click **Reset Password**. Oracle Identity Manager then displays the Reset Password page.

2. Enter your current password in the **Old Password** field. Then enter your new password and confirm that password. When done, click **Save**. If your password satisfies the system-defined criteria, your Oracle Identity Manager password will be changed.

Specifying Challenge Questions and Answers

Oracle Identity Manager provides you with the ability to select personal verification questions and specify the answers to these questions. These questions are used to verify your identity if you have forgotten your password and would like to change it to a new one or are required by the system to reset your existing password. The number of questions you must answer and the list of potential questions from which you may select are defined by your Oracle Identity Manager system administrator.

Note: You will be prompted to select the questions to use and supply the answers the first time you log in with your Oracle Identity Manager account.

You can choose to change the questions you would like to supply answers to, change the answers to the questions or both.

1. Click **My Account** in the Explorer Menu. Then click **Challenge Q&A**.
2. You will then be prompted to enter your password. Enter it and click **Continue**.
3. The Select Challenge Question page appears.
4. Select your challenge questions (make sure you select at least the minimum number of questions). Then, click **Select**.
5. Oracle Identity Manager will display the **Provide Challenge Answers** page. Enter the correct answer to each question listed. Be sure to specify answers that you can easily remember. Click Save.
6. Click **OK** to confirm your answers. If you forget your password, you will be prompted to provide the correct answers (as specified here) to the questions you selected.

Specifying a Proxy

Use the **My Proxy** option to designate a user to whom to delegate your task approval responsibilities while you are unavailable due to illness, vacation, and so on. As an approver, you can select another user as a proxy for yourself. Thereby, any task that is normally assigned to you will be routed to the delegated proxy user.

When a proxy user is defined, the tasks that would be normally be assigned to a user, would be displayed in the proxy user's **Pending Request** list. Refer to the Pending Request section for more information. Also, when the proxy user logs into Oracle Identity Manager, the **Home** page will display the user for whom the logged in user is a proxy.

To use My Proxy, perform the following steps:

1. To assign a proxy user, click **My Account** in the Explorer Menu. Then click **My Proxy**.
2. The **Proxy Details** page appears. If no proxy is defined at this time, then click Assign to delegate a user. The **Assign Proxy** page appears.

3. Select either **Your Manager** or **Other User** radio button to define the Proxy Name. By default the Manager is selected if the user has a Manager defined. You can lookup other users by clicking on the magnifying glass icon at the end of this field. The **Lookup Form** page appears. It displays all the user names that are available for defining a proxy user.
4. Select the desired **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. Highlight the desired date you want to activate the proxy user. Optionally, you can define an **End Date** by clicking on the calendar icon. Highlight the desired date you want to de-activate the proxy user. Afterwards, click **Assign**. If the end date is not specified, the proxy functionality is active until the user removes the proxy. The **Confirmation** page appears with the selected **User ID** as defined for the proxy user.
6. If information in the Confirmation page is correct, then click **Assign**. The **Proxy Details** page appears with the proxy user information that you defined.
7. If you want to make changes to the information for this proxy user, click **Modify**. If you want to delete this user as a defined proxy user, then click Re**move Proxy.**

5

My Resources

The **My Resource** option enables you to make a request for resources for yourself and others. This chapter describes how to work with resources in the following sections:

- Viewing Your Resources
- Viewing Your Resource Requests
- Requesting New Resources

Viewing Your Resources

1. To view the resources that have been provisioned to you, click **My Resources** in the Explorer Menu. Then, click **My Resource**s. The **My Resources** page appears.

   This page shows all provisioned resources associated with this user. The resource information is displayed in the information table. It shows:

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

2. This page also enables you to request a new resource for yourself. Click **Request New Resources** and the Create a Request to Provision Resource(s) - Step 1: Provision Resources page is displayed.
3. Select the resources you wish to request by checking the Resource Name check box then clicking **Add** to add them in the **Selected** list. Click **Remove** to delete the resource from the Selected list. Otherwise, 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 is displayed.
5. On the **Create a Request to Provision Resource(s) - Step 3: Verify Information** page, enter data into the fields, which are 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. You can add a comment if desired. By clicking on 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 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.
8. You can still modify the information for this resource request by either clicking on the **Change** link to change the resource or add another comment by clicking on the **Add** link. These links will jump to the corresponding page where the initial information was entered, respectively.
9. Once the information has been verified, 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. If you wish to activate this request at a later time, then click **Schedule for Later**.

    If you click **Scheduled for Later**, then the request will be created, the approval process will be initiated, and approvers can approve the approval tasks and complete the approval process. However, the provisioning process will not be initiated until the scheduled date. In other words, the actual resource will not be provisioned until the defined 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 request for resources that you have made for yourself as well as those made by other users for you.

1. To view all your request for resources, click **My Resources** in the Explorer Menu. Then click **My Request**. The **My Request** page appears.

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

   - Request ID (default)
   - Request Type

   Then enter a value to match this search criteria.

   The Results table displays the following information:

Field	Description
Request ID	This is the identification number of the request.
Request Type	This is the type of the request.
Requester	This is the name of the person who made the request **Note:** The Requester information is not displayed when the Raised By Me option is selected since the requester is the user, (same person).
Request Preview	This is the summary of the user and the associated resource for this request

2. If you wish to view the list of request made by another user (proxy user) for you, select the **Raised for me** option. The **My Request** page appears.

   This page is similar to the **Raised by me** page in that the information table are the same, but the exception that it displays resources that were raised on your behalf.

   When you select the **Raised for me** option, you are the beneficiary (entitling one to receive) of the request. Therefore, by making a provisioning request as the administrator, your goal is to add resources to users or organizations. So, 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. Therefore, no **Requester** column will be displayed for this option. You will see all your requests under this option.

Requesting New Resources

To make a new request for resources use the **Request New Resources** option. Click **My Resources** in the Explorer Menu. Then, click **Request New Resources**. The Create a Request To Provision Resource(s) page appears.

1. Select the resources you wish to request by checking the Resource Name check box then clicking the **Add** button to add them in the **Selected** list. Use the **Remove** button to delete the resource from the **Selected** list. Click **Continue**.
2. The Create a Request To Provision Resource(s) – Step 2: Provide Resource Data page appears.

Note: If the resource you are requesting does not have a form (a dialog for additional information) then Step 2 will be skipped.

This page displays the resource object for the target user. Click **Continue** to provide additional information about the resource object you wish to provision. Otherwise, click **Back** or **Exit**.

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

   Enter the additional information in the field. Click **Continue**. Otherwise click **Back** or **Exit**.

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

   The Users Selected table displays the following information:

Field	Description
User ID	This is the log in 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.

5. You can add a comment if desired. By clicking on the **add a comment** link, the **Add Request Comment** page appears.

6. 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.

7. You can still modify the information for this resource request by either clicking on the **Change** link to change the resource or add another comment by clicking on the **Add** link. These links will jump to the corresponding page where the initial information was entered, respectively.

8. Once the information has been verified, 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	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.

Field	Description
Date	This is when the request was executed.

9. If you wish to activate this request at a later time, then 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**.

6

Requests

Oracle Identity Manager enables you to create and track requests for resources you have requested for users and organizations. In addition, if you are an administrator, you will be able to create requests to provision the users you manage with resources. If you are an approver, you will be able to view and act on (for example, approve, reject) the tasks assigned to you. If you are both an approval and an administrator, you will be able to perform the functions associated with both roles.

This chapter includes the following subsections

- Creating and Managing Requests
- Tracking Requests

For a list of the various roles and their associated Oracle Identity Manager capabilities refer to Understanding User Roles and Capabilities.

Creating and Managing Requests

Oracle Identity Manager enables you to create and manage requests for the provisioning of resources to yourself and other users as well as organizations. Additionally, you can search on the following criteria:

- User IDs
- Request ID
- Date the request was created
- Resource Name
- Status of the request

The Resource option lets you choose the following options:

- Grant Resources – is used to allow resources to a target.
- Disable Resources – is used to temporarily disable resources.
- Re-enable Resources – after the resources are disabled, you can re-enable resources.
- Revoke Resources – is used to delete resources permanently. You cannot re-enable the resource back once you have revoked it.

This section includes the following subsections:

- Granting Resources
- Disabling Resources

- Re-enabling Resources
- Revoking Resources

Note: If you are a Oracle Identity Manager administrator, you will be able to create requests to provision other users with resources. Certain resources may be configured to allow users to request the resource for themselves.

If a resource allows self-service requests, Oracle Identity Manager will not require you to be an administrator in order to request it for yourself. In addition, if the resource is set to be allowed for all users, Oracle Identity Manager will not require you to be an administrator in order to request it for another user. If a resource is not set as allowable for all users then only those users associated with departments or organizations for which it is allowed will be able to have the resource requested for them. To determine whether a resource may be requested for you, contact your Oracle Identity Manager administrator or the administrator of the particular resource.

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

Granting Resources

To create a request for the provisioning of resources, click **Requests** in the Explorer Menu, then click **Resources**. The **Make a Request** page appears.

1. This page defaults to the **Grant Resource** option. Use this option to grant a resource to a specific user or organization. Click **Continue**. The **Create a Request To Provision Resource(**s) – **Step 1: Select Type** page appears.
2. Click **Users** option to assign a resource to one or many users. Otherwise, select the Organization option to provision a resource to one or many organization(s).

Note: Since requesting resources for an organization is similar to requesting resources for a user, this example will only includes the steps for requesting for resources for a user.

In this case, the Users option is selected. Click **Continue**. 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	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.

3. Select the User's checkbox then click **Add** to place the user name(s) in the **Selected** list. Use the **Remove** button to delete any user(s) in the **Selected** list. Then click **Continue**. The **Create a Request To Provision Resource**(s) – Step 3: Provide Resource page appears.

Note: If the request system form has any user-defined fields, then those fields are displayed on the STEP 2: Provide Additional Information page in the wizard. These fields are created using the User Defined Field Definition form for Form Name=Requests.

For more information on this, refer to the Oracle Identity Manager Design Console Guide.

4. 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. Then click **Continue**. The **Create a Request To Provision Resource(s) – Step 4: Provide Resource Data** page appears.
5. This page displays information about the resource and the user for this request. If the information is correct, then click **Continue**. Otherwise, click **Back** to make the appropriate corrections. Any associated Forms will be displayed in the next page.
6. Enter the information requested in the Forms field, then click **Continue**. Otherwise, click **Back** to make the appropriate corrections. The **Create a Request To Provision Resource(**s) – Step 5: Verify Information page appears.

Note: You can provision the same resource multiple times if the resource is configured for such usage.

7. You can add a comment if desired. By clicking on 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. Once the information has been verified, 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	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. If you wish 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 is commonly used for new employees that will start on some future date. Once you defined a date, the request is created, and the approval process will be initiated, approvers can approve the tasks, approval process can be complete. However, the provisioning process will not initiate until the scheduled date.

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

Disabling Resources

1. To disable a request for the provisioning of resources, click **Requests** in the Explorer Menu, then click Resources. The **Make a Reques**t page appears.
2. Select the Disabled Resource radio button. Click **Continue**. The Create a Request To Disable 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 Disable Resources – Step 2: Select User(s) page appears.
4. Select the user's name(s) checkbox then click **Add** to place the user name(s) in the **Selected** list. Use the **Remove** button to delete any user(s) in the **Selected** list. Then click **Continue**. The Create a Request To Disable Resources – Step 3: Provide Resources page appears.
5. Select the resource(s) checkbox that you wish to disable from the user, then click **Add** to place the resource(s) in the **Selected** list. Use the Remove button to delete any resources(s) in the **Selected** list. 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.
6. If the Create a Request To Disable Resources – Step 4: Resolution page appears, select the resource instance you want to disable, and then click **Continue**. The **Create a Request To Disable Resources – Step 5: Verify Information** page appears.
7. 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	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.
Resource Name	This is the name of the resource you are requesting/provisioning.
Details	This is any additional detailed information about the resource.

8. You can add a comment if desired. By clicking on the **add a commen**t link, the **Add Request Comment** page appears.
9. 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. The Verify Information page will now displays the added comment.

You can still modify the information for this resource request by either clicking on the **Change** link to change the resource or add another comment by clicking on the **Add** link. These links will jump to the corresponding page where the initial information was entered, respectively.

10. Once the information has been verified, 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	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.

11. If you wish to activate this request at a later time, then 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**.

Re-enabling Resources

1. To create a request to re-enable a resources, click **Requests** in the Explorer Menu, then click **Resources**. The **Make a Request** page appears.
2. This page defaults to the **Grant Resource** option. Use the **Re-enable Resource** option to provide access to resources that were earlier disabled for this user. 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 case, the Users option is selected. 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	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.

4. Select the User's checkbox then click **Add** to place the user name(s) in the **Selected** list. Use the Remove button to delete any user(s) in the **Selected** list. Then click **Continue**. The **Create a Request To Re-enable 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. 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.

6. 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.
7. You can add a comment if desired. By clicking on 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. Verify the information on the Create a Request To Re-enable Resources – Step 5: Verify Information page, and 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	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.

   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.
10. If you wish to activate this request at a later time, then click **Schedule for Later** to define a date when the request becomes active. The Schedule for Later page appears.
11. Use the calendar icon to define a date to activate your request, and then click **Submit**.

Revoking Resources

1. To create a request for revoking access to resources, click **Requests** in the Explorer Menu, then click **Resources**. The **Make a Request** page appears.
2. Select the Revoke Resource radio button. 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 name(s) in the **Selected** list. Use the Remove button to delete any user(s) in the **Selected** list. Then click **Continue**. The **Create a Request To Revoke Resources – Step 3: Provide Resources** page appears.
5. Select the resource(s) checkbox that you wish to revoke access for from the user, then click **Add** to place the resource(s) in the Selected list. Use the Remove button to delete any resources(s) in the Selected list. 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	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.

8. You can add a comment if desired. By clicking on the **add a comment** link, the **Add Request Comment** page appears.
9. 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. The **Verify Information** page will now displays the added comment.

   You can still modify the information for this resource request by either clicking on the **Change** link to change the resource or add another comment by clicking on the **Add** link. These links will jump to the corresponding page where the initial information was entered, respectively.
10. Once the information has been verified, 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	This is the status (state) of the request.

Field	Description
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.

11. If you wish to activate this request at a later time, then 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 within 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 will be able to track are comprised of three 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 will be governed by characteristics of your account within Oracle Identity Manager. In addition, if you are assigned to approve a task within a request, you will be able to approve any tasks assigned to you when tracking that request. For a list of the various roles and their associated capabilities refer to the Understanding User Roles and Capabilities section.

In this section, you will see how to perform the following tasks related to tracking requests:

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

Searching for Requests

1. To track a request, click Requests in the Explorer Menu, then click **Track**. The **Track Requests** page appears. To locate the request you wish to track, you must first query for existing requests. You can search for existing requests according to the options listed as radio buttons. You may only select one of these options (for example, **User ID** or **Request ID**, not both). If your 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.

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 perform searches 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 (usually a numeric value). Select this option, and then enter the ID of the request. You can use a wildcard character (for example, *) to perform searches for requests beginning or ending with specific characters or numbers.
Creation Date	Enables you to track requests by date on which 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 will then display 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.

Note: If you select a Request ID or Resource Name and leave the fields associated with that option blank, Oracle Identity Manager will display all requests.

2. Click Search to execute the search. Oracle Identity Manager will display 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, Next, and Last links to help you navigate through that result set.
3. To view the details of a request, click the request ID link in the Results table. The Request Details page appears.

Note: You may cancel an entire request by selecting the checkbox next to it and clicking Cancel Request.

Viewing Approval Details

Search for a resource request, as described in Searching for Resource Requests, and then select **Approval Details** option from the Additional Details box. The **Approved Task(s)** page appears. The Approval Details shows all tasks associated with the approval processes.

This page displays all approvals for this request including process and pending task(s). The Request ID number is an active link that jumps back 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	Contains Approve, Deny, and Re-assign buttons that you select to determine the action for the request. The Action column has a checkbox for each request. The last row contains Approve, Deny, and Re-assign buttons. Selecting the requests and clicking on Approve or Deny takes the user to a confirmation page where the tasks selected are listed along with the Confirm and Cancel buttons. If the user clicks Re-Assign, the console displays a list of all the users that the logged-in user can see to whom the task can be re-assigned by the user. That page also has a radio button which, when selected, lists all the groups that the logged in user can see to whom the task can be re-assigned.

Viewing Provisioning Details

Search for a resource request, as described in Searching for Resource Requests, and then select **Provisioning Details** option from the Additional Details box. The **Provisioning Task**(s) page appears. The Provisioning Details shows all tasks associated with the provisioning processes.

You can choose to view the provision tasks either by User/Organization (depending on whether the request was created for a user or organization) or Resource. Select the desired radio button and the page will display the appropriate information.

Viewing by User/Organization

When selecting the User/Organization button, the page will display all the tasks for users/organizations who will be provisioned. If a request has multiple users/organizations, then the page will display a corresponding table for each user.

The information table shows:

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

When selecting Resource (radio button), the page will display all the resources and information related to this resource. If a request has multiple resources, then the page will display a corresponding table for each user.

The information table shows:

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

Search for a resource request, as described in Searching for Resource Requests, and then select **Request Comments** option from the Additional Details box. Clicking on the Request ID number jumps back to the **Request Details** page. If there is no comment on this page, then you can add a comment by clicking on the **add a comment** link.

The request is viewed by any user who has privileges. To allow other users to understand the specific request, the request comments are used in providing in-depth information about the request. Users, as well as the System, can add comments to the request so that other can see how the request has been processed.

If there is a comment added to this request, then the Request Details >> Request Comments page appears with the comment.

This page displays the following information in the table:

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

Search for a resource request, as described in Searching for Resource Requests, and then 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. 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 (approval task) or a system action (an adapter).

Whenever an action is executed, the status of the workflow is changed and it transitions to the next state. Request History is a supplemental view of understanding the state of the current workflow.

This page displays the following information in the 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

The approval processes by which requests and their associated resources are approved and made available for provisioning are comprised of tasks. These tasks must be approved by the user to whom they have been assigned before the resources in the request can be provisioned to the target users. In addition, if you have set Oracle Identity Manager to require approvals for self-registration, the approval tasks associated with user's self-registration requests will also appear (and require action by the assigned approver in order to complete the registration process).

If you are an approver for any of the tasks within a request, you will be able to view all tasks in the request but only approve those assigned to you. You can also view pending request(s) to users who you manage.

To approve (or deny) the tasks assigned to you, click **Pending Approvals**. A list of all requests that contain one or more tasks for which you are an approver will be displayed.

The **Open Tasks** option are tasks that are defined for the provisioning process. When defining the process using the **Process Definition** form of the **Oracle Identity Manager Design Console**, you must specify the type, which is either "**Provisioning**" or "**Approval**". By selecting the Provisioning type, the process is then a provisioning process. Thereby, each resource has one mandatory provisioning process associated with it. Tasks can then be assigned to users.

Note: Only users who are task approvers, assigned to provisioning tasks, or administrators of the organizations to which the target users belong will be able to view tasks within a request.

This section covers the following topics:

- Reviewing Pending Approvals
- Managing Open Tasks
- Managing Attestation Requests

Reviewing Pending Approvals

1. To view and complete the tasks assigned to you, click **Pending Approvals** under **To-Do List**.
2. The Pending Approval page appears. You can display all requests that contain tasks to which you are assigned or view request assigned to users that you manage. By default, the page opens with pending request(s) that are **Assigned to you**. However, you can view pending requests that are assigned to users that you

manage. Select the **Assigned to user(s) you manage** radio button and the page will display the appropriate pending requests.

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

- Request ID
- Request Type
- Requester
- Assign To

The **Results** table has a description of these search criteria. Enter the appropriate value in the corresponding field. The **Results** table displays the fields described in the following table:

Field	Description
Request ID	This is the request's unique, system-generated identification number.
Request Type	The Request Type can be: Self-Registration Modify Profile Grant/Enable/Disable/Revoke Resources for Users or Organizations.
Requester	This is the Oracle Identity Manager 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 on desired checkbox in the **Approve/Deny** column, then click **Approve**. When complete, the request ID is removed from the **Results** table.

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

4. To reassign a pending request, select on desired checkbox in the **Re-Assign** column, then click **Re-Assign**.The **Re-Assign Pending Approvals** page appears.

5. Select the desired checkbox for the user or group you want to re-assign this request to. Click **Re-Assign**. The Confirm Page appears.

Managing Open Tasks

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

1. To view the provisioning tasks assigned to you, click **Open Task** under **To-Do List**.
2. The **Open Tasks page** appears. You can set the display for this page to show all open tasks that are assigned to you, or the users and the user groups that you manage.
3. Use the **Filter By** search criteria to sort the provisioning tasks by the following categories:
   - Task Name
   - Task Status
   - Resource Name
   - Organization Name
   - User ID
   - Resource Type
   - Assign Before (enter date – yyyy-MM-dd)
   - Assign After (enter date – yyyy-MM-dd)

   Enter the appropriate value in the corresponding field. Then click **Go**. The **Results** table will display the appropriate information.

   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	This is the name of the resource associated with this provision task.
Resource Type	This is the type of resource defined in the Resource Object form. There are three categories for resource type: Generic, System, and Application
Date Assigned	This is the date that the provisioning task was assigned.
Assigned To	This is the user name that the provisioning task is assigned to.
Re-Try	If the Re-Try checkbox is activated, then it indicates that the Status of the provisioning task was Rejected. Use this checkbox to Re-Try the provisioning task.
Re-Assign	Use the Re-Assign checkbox to assign this provisioning task to another user or user group.
Set Response	Use the Set Response checkbox to set a response for this provisioning task.
Complete Manually	Use the Complete Manually checkbox to manually complete the provisioning task.

Reassigning an Open Task

1. To re-assign an open task to another user, select the desired provisioning task name checkbox(es), then click **Re-Assign**. The **Re-Assign** Open Tasks page appears
2. Select the desired User ID or Group ID (only one user or group can be selected), and then click **Re-Assign**. The **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. If this is correct, click **Confirm Re-assign** Tasks. Otherwise, click **Cancel**. The **Open Tasks** page appears.

   Note that the provisioning task that you have re-assigned is no longer in the **Results** table.

Setting a Response to an Open Task

1. To set response to an open task, select the desired provisioning task name(s) checkbox, then click **Set Response.** The **Specify Task Responses** page appears.
2. Select a response for the provisioning task, then click **Set Response**(s). Otherwise, click **Cancel**. The Confirmation page appears.

   This page displays the response for this particular provisioning task.
3. If this is correct, click **Confirm Response for Tasks**. Otherwise, click Cancel. The **Open Tasks** page appears.

   Note that the provisioning task that you have set response to is no longer in the **Results** table.

Managing Attestation Requests

The Attestation option displays all open attestation tasks that are assigned to you. Use the Attestation option to certify, reject, decline, or delegate attestation tasks. This is described in the following sections:

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

Viewing Attestation Requests

1. Expand the To-Do List link and click **Attestation**. The Attestation Request Inbox page appears with a results table that lists your pending attestation process requests. The results table contains the columns listed in the following table:

Column	Description
Process Names	Specifies the name of the process.
Process Code	Specifies the code of the process.
Data Type	Identifies the type of data being attested.

Column	Description
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.

To display only records for which actions are not specified already, select the **Hide records where action has already been specified** option, which is present above the results table.

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 will show the entitlements that the user needs to attest as a part of the task and all the associated details. This is also the page where the reviewer would be able to see the actual details (process form data) of the entitlement that they are supposed to attest. The results table contains the columns listed in the following table:

Column	Description
User	Specifies the whose entitlement is being attested
Resource	Specifies 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	Contains a description of the provisioned resource instance
Last Attested	Stores the date and time when this entitlement was last attested
Comments	Contains 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. If desired, select the check box to hide records where action has already been specified.
4. To view additional rows in the results table, click **Next >>**.

Saving Attestation Actions

1. Follow the procedures in Viewing Attestation Requests to select the attestation process you want to submit.
2. On the Attestation Request page, select any actions you want to take for the listed entitlements, and then 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 entitlements for which you selected an action of "delegate" also allow 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**.

> **Note:** Clicking Save does not submit the attestations. To submit attestations, you must follow the procedures in Submitting Attestations.

Updating Comments and Delegations

1. Follow the procedures in Viewing Attestation Requests to select the attestation process you want to submit.
2. Follow the procedures in Saving Attestation Actions 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 you want to update. Then, enter any new comments and select a delegated reviewer.
5. Click **Save**.

Submitting Attestations

1. Follow the procedures in Viewing Attestation Requests to select the attestation process you want to submit.
2. Follow the procedures in Saving Attestation Actions 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.

> **Note:** The Submit Attestation button is active only if you have designated an action for each entitlement in the current attestation process request.

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

8

Users

The Users option is used to create and manage the user records (for example, Oracle Identity Manager accounts) that your employee will require.

Oracle Identity Manager enables you to create Oracle Identity Manager accounts for other users. This chapter describes how you can create and manage users in the following sections:

- Creating Users
- Managing Users

> **Note:** Although you may allow users to self-register, you may still wish 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.

Creating Users

1. Click **Users** in the Explorer Menu, then click **Create.** The Create User page appears.
2. Enter the data required for user registration (as indicated by the fields marked with an asterisk).
3. In the Organization field, you can click the magnifying glass icon to display the Lookup Organization pop-up.
4. Select an organization from the list and click **Select.**
5. When complete, click Create User. Oracle Identity Manager will create the user account and display the **User Details** page with the user's account information.

> **Note:** If you select any of the options in the additional details box, you will see limited information since you have just created the user. However, in viewing the details of each search criteria, you are able to add/assign the user with the desired resource.

In the **User Detail** page, you can:

- **Edit –** make changes to the user profile
- **Disable –** disable the user from being provisioned
- **Unlock –** unlock user when locked out from login re-try

- **Delete –** delete the user account
- **Change Password –** change the current password

Editing the User Profile

You can make changes this user's profile by clicking **Edit.** The **Edit User** page appears. Make modifications then click **Save.** Otherwise, click **Cancel Edit** to end the edit.

Disabling the User

To disable the user from being provisioned, click **Disable.** Depending on your role (status), this page allows the disable button to toggle between **Disable** and **Enable**.

> **Note:** The Unlock button is activated when the user attempts to log in to their account and is unsuccessful. After a number of retries, the user is locked out.

Changing the User's Password

You can change the user's password by clicking **Change Password**. The **Change Password** page appears. Enter a new password and confirm. Then click **Save Password**. Otherwise, click **Cancel.**

Managing Users

To edit information in another user's Oracle Identity Manager record.

1. Click **Manage** under **Users.**
2. Oracle Identity Manager will prompt you to query the record of the user for whom you wish to edit details.

   Use any or all of the fields shown to enter information related to the user. The more information you provide, the more precise the list of user records retrieved will be. Use the pull-down menu to define a search criteria.

   After making a selection, you can enter the corresponding information in the next field or use a wildcard asterisk (*) for your search. When ready, click Search User.
3. Oracle Identity Manager will then display the list of users who match the criteria you entered.

   To disable, enable, unlock or delete an account, select the appropriate checkbox and button (in that order). For example, to disable the user accounts of BGATES and SJOBS, select the **Disable** check box in applicable rows and click **Disable.**

   > **Note:** A user account must be in a status of disabled to be eligible for enabling. In addition, only locked accounts can be unlocked. An account becomes locked if a user has exceeded the maximum number of login retry attempts. If a user account is locked, the **User Locked** checkbox will be selected.

   To edit a specific user's account, click the user ID for that account.
4. Oracle Identity Manager will display the user's profile.

5. 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.

   - Clicking on the **Resource Profile** option displays any resources that the user is provisioned. **The Resource Profile** page displays resources that are provisioned to the user. You can also provision resources in this page by clicking on the **Provision New Resource** button.
   - Clicking on the **Group Membership** option in the drop-down menu selection displays 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.
   - Clicking on the **Proxy Details** option in the drop-down menu selection displays 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

The Organization option provides System Administrators with the tools necessary to create and manage information pertaining to your company's organization. This section describes how you can create and manage organizations in Oracle Identity Manager in the following sections:

- Creating Organizations
- Managing Organizations
- Managing Organization Details

Creating Organizations

1. Click Create under Organizations.
2. Oracle Identity Manager will display the **Create Organization** page.
3. Enter the 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. Click **Select**. The organization name is entered into the **Create Organization** page. Click **Create Organization**. The Organization Detail page appears. The Organization Detail page is described in Managing Organization Details.

Managing Organizations

Use the **Manage** option to manage existing organizations. This page lets you enable, disable, and delete the organization. This is described in the following sections:

- Searching for and Viewing Organizations
- Enabling an Organization
- Disabling an Organization

- Deleting an Organization

Important: 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 menu option in the Oracle Identity Manager Design Console.

Searching for and Viewing Organizations

To use search for and view existing Organizations in Oracle Identity Manager:

1. Click **Organization** in the Explorer Menu. Then click **Manage**. The **Manage Organization** page appears.
2. Use the drop-down menu to select a search criteria for querying on an organization. The search criteria are:
   - **Organization Name** - This is the name of the organization.
   - **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).
   - **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.

   Then enter the appropriate value that corresponds with the search criteria. Otherwise, use the asterisk (*) wildcard to query for all the organizations. The search **Results** table appears. This page lets you Disable and Delete an organization.

Enabling an Organization

To enable an organization:

1. Select the **Enable** check box. Click **Enable**. The **Confirm Enable** page appears.
2. Click **Confirm Enable** to complete enabling this organization. Otherwise, click **Cancel**.

Disabling an Organization

1. To disable an organization, select the **Disable** check box. Click **Disable**. The **Confirm Disable** page appears.
2. Click **Confirm Disable** to complete disabling this organization. Otherwise, click **Cancel**.

Deleting an Organization

1. To delete an organization, select the **Delete** check box. Click **Delete**. The **Confirm Delete** page appears.
2. Click **Confirm Delete** to complete disabling this organization. Otherwise, click **Cancel**.

Managing Organization Details

1. Create a new organization as described in Creating Organizations

   OR

   a. Search for an organization as described in Managing Organizations

   b. Click an organization name in the Results table. The Organization Detail page appears.

2. The **Organization Detail** page appears. In the **View Additional Detail about the Organization** pull-down menu, you can view the information associated with this organization based on:

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

   In the Organization Detail page, you can:

   - **Edit** - make changes to the organization profile
   - **Disable** - disable the organization from being provisioned
   - **Delete** - delete the organization

3. If you select to view information based on **Resource Profile** for this organization, then 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 select to view information based on Users for this organization, then 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 select to view information based on **Sub-Organization** for this organization, then the **Organization Information >>Sub-Organization** page appears. In the Sub-Organization page, you can move sub-organizations to a different organization.

6. If you select to view information based on **Administrators** for this organization, then 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 select to view information based on **Permitted Resources** for this organization, then 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

The User Groups option is used to create and manage records of collections of users to whom you may assign some common functionality, such as access rights, roles, or permissions. These collections of users are known as **user groups**.

User Groups can be organizational-independent (spanning across multiple organizations) or contain users who belong to a single organization.

A group serves as a central mechanism by which to accomplish any of 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 are used to determine whether a resource object is to automatically be provisioned to or requested for a member of the user group.
- Assign/remove membership rules to/from the user group. These rules will 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. In addition, you can create additional user groups, as needed.

Members of the *System Administrators user* group have full permissions to create, edit, and delete records within Oracle Identity Manager (except for system records). Also, 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 limited functionality within these forms

Members of the All Users user group have minimal permissions, which include, but are 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: There is a fourth user group definition, SELF OPERATORS, which is added to Oracle Identity Manager, by default. This user group contains one user, XELSELFREG, who is responsible for modifying the privileges that users have when performing self-registration actions within the Oracle Identity Manager Administrative and User Console.

Oracle Identity Manager strongly recommends that you do not modify the permissions associated with the SELF OPERATORS user group. In addition, you should not assign any users to this group.

Creating Groups

To create a User Group:

1. Click **User Groups** in the Explorer Menu, the click **Create**.
2. The **Create User Group** page appears. Enter information in the required fields indicated by an asterisk (*).
3. Enter the name of the user group to be created in the **Name** field.
4. Click **Create**. Otherwise, click **Cancel**.
5. The **Group Detail** page appears.

Note: Since you have just created a new User Group, the Group Detail page will not show any additional information for this group. However, you can begin adding (or Assigning) more information by using the additional detail drop-down menu. Refer to the **Manage** section for detailed instructions on using the additional detail drop-down menu items.

---

6. Click **Edit** to modify the Group Name. Otherwise, click **Delete** to delete the user group.

Managing Groups

Use the **Manage** option to administrate existing User Groups. This option enables you to do the following:

Searching for User Groups

1. Click **User Group** in the Explorer Menu. Then click **Manage**. The **Manage Group** page appears.
2. Use the drop-down menu to select the Group Name search criteria (the name of the User Group) for querying on the User Group. Then enter the appropriate value that corresponds with the search criteria. Otherwise, use the asterisk (*) wildcard to query for all the user groups. The search **Results** table appears. This page enables you to delete User Groups.

Deleting User Groups

1. Search for a group as described in Searching for User Groups.
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. Otherwise, click **Cancel**.

Viewing and Administering a User Group

After selecting the user group you like to view, you can view the details of that particular user group by using the additional details drop-down menu. Each of these menu items also provides the ability to modify the user group. This menu contains the following search criteria:

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

Member and Sub-Groups

The **Member and Sub-Group** search criteria display all members and sub-group(s) associated with this User Group. The Member and Sub-Group option also enables you to assign a new member (user) or sub-group.

1. Search for a group as described in Searching for User Groups, and 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.

> **Note:** Since the Assign Users and Assign Sub-groups options are similar in functionality, the Assign Users is used as an example in this section.

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. Otherwise, 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.

1. Search for a group as described in Searching for User Groups, and 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 G**roup 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 checkbox(es), 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** is displayed 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(s) checkbox, then click **Delete**. The menu item is no longer associated with this user group.

Administrative Groups

The **Administrative Groups** search criteria displays all administrative groups associated with this user group. The **Administrative Groups** option enables you to assign a new administrative group for the user group.

From the additional detail drop-down menu, select **Administrative Groups**. The **Group Detail >> Administrative Groups** page appears. This page displays the existing administrative group associated with this user group along with their permission to write and delete accesses. This page also enables you to:

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

Assigning an Administrative Group

1. Search for a group as described in Searching for User Groups, and 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.
4. This page displays all administrative groups available to be associated with this user group. Select the desired administrative group name(s) checkbox and respective permission settings for write and delete accesses. Then click **Assign**. The **Confirmation** page appears.
5. If this is the correct administrative group name(s) you want to assign to this user group, then click **Confirm Assign**. Otherwise, click **Cancel**. The **Result table** is displayed with the administrative group that can administrate this user group. This page also enables you to delete an administrative group from this user group.

Creating a New Administrative Group

1. Search for a group as described in Searching for User Groups, and 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 desired user name(s) checkbox you wish to be in this new administrative group. Click **Add**. The User Login names appear in the Selected list. Click **Continue**. Otherwise click Back or Exit to end the wizard. The **Assign Administrators – Step 2: Specify Alias** page appears.
5. Enter an alias name for the new administrative group. Click **Continue**. Otherwise, click **Back** to go to the previous page or Exit to end the wizard. The **Assign Administrators – Step 3: Specify Permissions** page appears.
6. By default the Read permission checkbox is activated. 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 name of the administrative group, the users who belong to this administrative group, and the permissions for the group.
7. To make modifications for this administrative group, use the **Change** link. Clicking on 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

1. Search for a group as described in Searching for User Groups, and 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. Click **Update** to make the modifications. Otherwise, click **Cancel**. The **Confirmation** page appears.
5. This page displays the administrative group names that you have updated. If these are the correct names, then click **Confirm Update**. Otherwise, click Cancel. The **Group Details >> Administrative Groups** page appears.

   The updated administrative group(s) is displayed with their modified Write or Delete access permissions.
6. You can delete an administrative group by selecting the desired group name checkbox(es) then click **Delete**.

Access Policies

The **Access Policies** search criteria displays all available access policies for this user group. The **Access Policies** option enables you to assign a new access policy for the user group.

1. Search for a group as described in Searching for User Groups, and 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

The **Membership Rules** search criteria displays all available membership rules for this user group. The **Membership Rules** option enables you to assign a new membership rule for the user group.

1. Search for a group as described in Searching for User Groups, and 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 rule(s) 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, then click **Confirm Assign**. Otherwise, click **Cancel**. The **Group Detail >> Membership Rules** page appears.

6. To delete this membership rule, select the desired membership rule checkbox(es) and click **Delete**.

Permissions

The **Permissions** search criteria displays all available permissions for this user group. The **Permissions** option enables you to assign or update new permissions for the user group.

1. Search for a group as described in Searching for User Groups, and 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(s) checkbox and respective permission settings, then click **Assign**. Otherwise, click **Cancel**. The **Confirmation page** appears.
5. If this is the correct permission you want to assign for this user group, then 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, Allow Delete), then click **Update**. Otherwise, click **Cancel**. The **Confirmation** page appears.
9. This page displays all the updated permissions. If this is correct, then click Confirm Update. Otherwise click Cancel. The **Group Detail >> Permissions** page appears.
10. The **Group Detail >> Permissions** page displays the fine-grained permission information for this user group. It also enables you to delete any permissions. To delete a permission, select the desired permission name(s) checkbox and click **Delete**.

Allowed Reports

The **Allowed Reports** search criteria lists the reports that group members are allowed to run.

1. Search for a group as described in Searching for User Groups, and 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 then click **Assign**. Otherwise, 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 you can create and use access policies for users, organizations, and resources in Oracle Identity Manager in the following sections:

Creating an Access Policy

The Access Policy wizard helps you define an access policy for provisioning resources to user groups - in particularly, to users.

1. Click **Create** under Access Policies
2. The **Create Access Policy** page appears. 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**. Selecting the **With Approval** option will require a defined approver (or proxy user) to approve the resource to be provisioned to the user or group. Whenever the access policy is applied, a request is created to provision the resource to the user for approval by this approver. If the **Without Approval** option is selected, then whenever the access policy is applied, the resource is directly provisioned to the user without any request being generated.
3. Clicking on the **Retrofit Access Policy** checkbox would retrofit this access policy when it is created. This means that if a user is already part of a user group for which this access policy is being created, then that user will be provisioned by the resource specified by this access policy. If retrofit check box is not selected, then existing group memberships are not taken into considerations. 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 your resources by using the filter search dropdown menu. Select the name of the resource from the **Results** table by checking the desired box. Click **Add**. The names of the desired resources to provision appear in the **Selected** list. If you intend to create an access policy that will only deny resources, click **Continue** without selecting a resource and the Request Wizard will prompt you to select resources to be denied in the next step. You can un-assign the selected resources by highlighting the resource in the Selected list and click **Remove**. Click **Continue**. If there is a Form associated with this resource, then the next subsequent pages will 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 can specify whether access policies should be revoked if they no longer apply. Select the checkboxes for the resources you want to automatically revoke 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 manage existing access policies in the system by making the appropriate modifications.

1. Click Manage under Access Policies.

   The **Manage Access Policies** page appears. Use the pull-down 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 instantaneously 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 entire organization or an individual user. Managing resources include:

- Ability to search for a resource and view its details
- Ability to disable, enable, revoke a resource from user(s) or organization(s)
- Manage Resource Administrator and Authorizer groups

This chapter covers the following topics related to managing resources:

Managing Resources

To manage resources:

1. Click **Resource Management** then on the **Manage** link. The **Resource Search** page appears.

   Note: When searching, if you select a value from the drop-down list and do not enter a corresponding search value, an error will occur. Also, if you select the same value twice, from the drop-down menu, an error will occur.

2. Use the pull-down menu to select search criteria. In the next field, enter the corresponding attribute. In this example, the wildcard asterisk (*) is used. Click **Search**.

   This page displays the **Results** table.

3. Select a resource by clicking on the name. The **Resource Detail** page appears. In this example, the resource name, Oracle Identity Manager User is selected.

4. You can view additional detail information about the resource by using the pull-down menu.

   In this example, the resource target is set to **"O"** for organization, meaning that when you make a selection for additional details, the child table that appears will

be for organization results. Likewise, if the resource target is set to "U" for users, any child table that appears based on your selection for additional details will be for user results.

Therefore, depending on the value of the resource target (**O** or **U**) the pull-down menu will display either **Users Associated with This Resource** or **Organizations Associated with This Resource** option.

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). This page will only display the organization details.

Likewise, 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). This page will only display the user details.

The additional details include the following options:

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

Using an Organization Associated For a Resource Option

1. In this example, the **Organization Associated For the Resource** option is selected for the Oracle Identity Manager User resource.
2. The **Organization Associated For the Resource** page appears. The display radio buttons provide a way to filter through the list of associated organizations. The **All** radio button lists all the organizations, while 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. For example, the Resource Status in this case, indicates that the resource is provisioning for each of the organizations listed. You can then modify the resource for the organization by either:
   - 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 who are assigned as administrators to this resource. This page also displays the **Write Access** and **Delete Access** permissions. The Write Access and Delete Access permissions are permissions that the administrator groups have on the resource (but not with resource parameters). The Write Access permission allows the group to make changes to the resource, while the Delete Access permission 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 Administrator Group

Assigning a User Group as Administrators for Resources

To assign a user group as administrator for a resource, do the following:

1. Click **Assign**. The Assign Administrators page appears.

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

2. Afterwards, click **Assign**. The **Confirm Assign** page appears.

3. This page displays the new user group(s) assigned to this resource. If you need to make changes to the information, click **Cancel.** Otherwise, click **Confirm Assign.**

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

Creating a New Administrator Group

The Create New Group option enables you to create a new group to administrate the resource. Clicking this button initiates the "**Delegated Admin Wizard**".

1. Click **Create New Group**. The Assign Administrators – STEP 1: Assign Administrators page appears.

   In the Results table, click the desired User Login (names) that you want in your administrator group. Then click the **Add** button. The names will appear in the **Selected** display panel. Click **Continue.** Otherwise click **Exit** to end the wizard.

2. The Assign Administrators – STEP 2: Specify Alias page appears.

   Enter the alias name for the administrator group. Then click **Continue.** Otherwise click **Back** to return to the previous page or **Exit** to end the wizard.

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

   Click **Write** and **Delete** checkboxes to enable the administrator group to have these permissions. Then click **Continue.** Otherwise click **Back** to return to the previous page or **Exit** to end the wizard.

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

   This page enables you to make any changes to the delegated information displayed. To make a change, click the desired category **Change** link and the corresponding (step) page will appear. However, if you verified that there is no change, then click **Continue.** Otherwise click **Back** to return to the previous page or **Exit** to end the wizard.

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

Note: If a user creates a new group, and the user belongs to certain other groups with Write and Delete access, then these other groups become administrative groups for the new group. This is also true when the user creates a new organization.

Updating Permissions of an Administrator Group

The **Update Permissions** option enables you to update the permissions of an administrator group.

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. Click **Update** to make the modifications. Otherwise, click **Cancel.** The **Confirmation** page appears.
3. The Confirmation page displays the administrative group names that you have updated. If these are the correct names, then click **Confirm Update.** Otherwise, click **Cancel**.

Using the Resource Authorizers Option

1. In the **Resource Detail** page, select the **Resource Authorizer** option from the pull-down menu. The **Resource Detail** >> **Resource Authorizers** page appears.
2. The **Resource Detail** >> **Resource Authorizers** page lists all of the user groups that are authorized to provision the resource. You can also set the level of priority for authorizing this resource by selecting on the **Increase/Decrease Priority** radio button. If you wish to delete the authorizer of this resource, you can select the appropriate **Group Name** checkbox and click **Delete**.
3. To add additional user groups to authorize resources, click **Assign.** The **Resource Detail** >> **Resource Authorizers** >> **Assign Authorizers** page appears.
4. Select the desired Group Name checkbox, then click **Assign.** Otherwise, click **Cancel.** The **Confirmation** page appears. 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 in the **Results** table.

Using the Resource Workflows Option

The Graphical Workflow Visualizer tool provides a visual representation of your task sequences, dependencies, and other components that make up your workflow definition. The tool takes your complex workflow definition and renders it into an easy-to-understand visual representation. The graphic representation gives you an intuitive overview of the workflow, its relationships, and the task components that make up the flow. You can manipulate the workflow view and arrange it to your desire. Also, this tool enables you to print the workflow view.

There are two Oracle Identity Manager process types that the Graphical Workflow Visualizer tool will display; the Approval and Provisioning types. The **Approval** type of process is generally used to approve the provisioning of Oracle Identity Manager resources to users or organizations. Unlike provisioning processes, approval processes

are usually comprised of tasks that must be manually completed. The other process type is the **Provisioning** type. This 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
- Using Drag and Drop
- Using Display Options (menu item)
- Using the Task Node (right-click menu)
- Using the Expansion Nodes (Response Sub-Tree)
- Using the Provisioning Workflow Definition Event Tabs
- Accessing the Task Details

Launching the Workflow Visualizer

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.

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 is displayed.

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. Therefore, the Workflow Visualizer **does not** display the **Name of Process Form** information field.

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

Field Name	Description
Workflow Name	This is the name of the Process Definition.
For Resource	This is the name of the Object Name (resource object that is either approved or provisioned).
Workflow Type	This is 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:

Field Name	Description
Display Option	**Display Unknown Response Code** – The "Unknown" response code is defined for every single task in the workflow. It is not used within 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 name. **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 the "Save Picture As…" in the menu item.
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 – The Start Maker represents the logical start point within the workflow. It is not an actual task within the workflow definition. On-Page Reference – The On-Page Reference 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 represents any task within a process that requires user action in order to be completed. Approval processes are generally comprised of manual tasks. Automated Tasks – The Automated Tasks represents any task within 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.

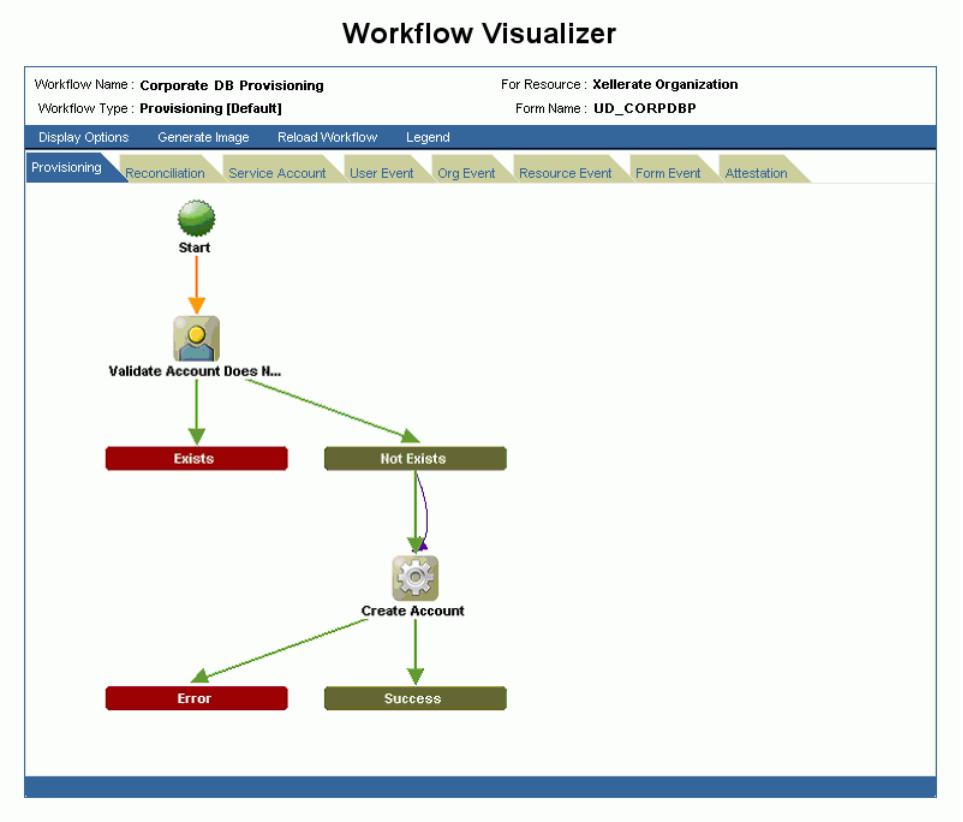
User Interface

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)

To illustrate how you can manipulate your workflow definition, the Corporate DB Provisioning workflow definition is shown. Selecting an event tab displays the appropriate sequence of task(s) for that event. These event tabs are discussed in the Using the Provisioning Workflow Definition Event Tabs.

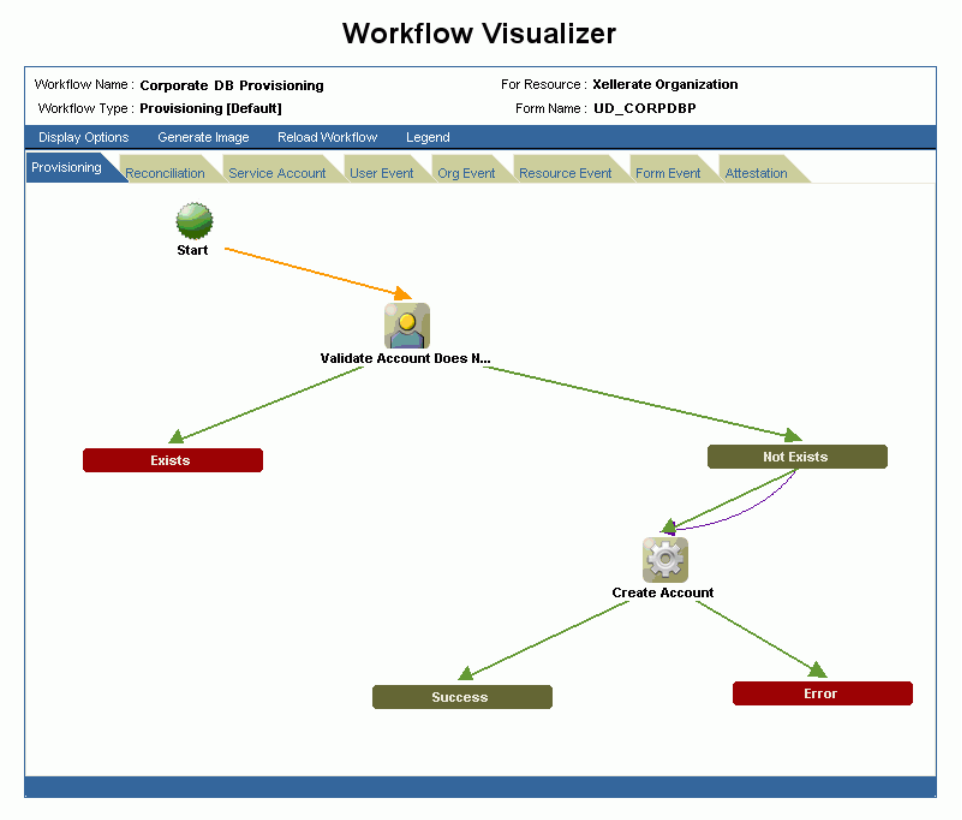
Figure 12–1 Using the Workflow Visualizer



Using Drag and Drop

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

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



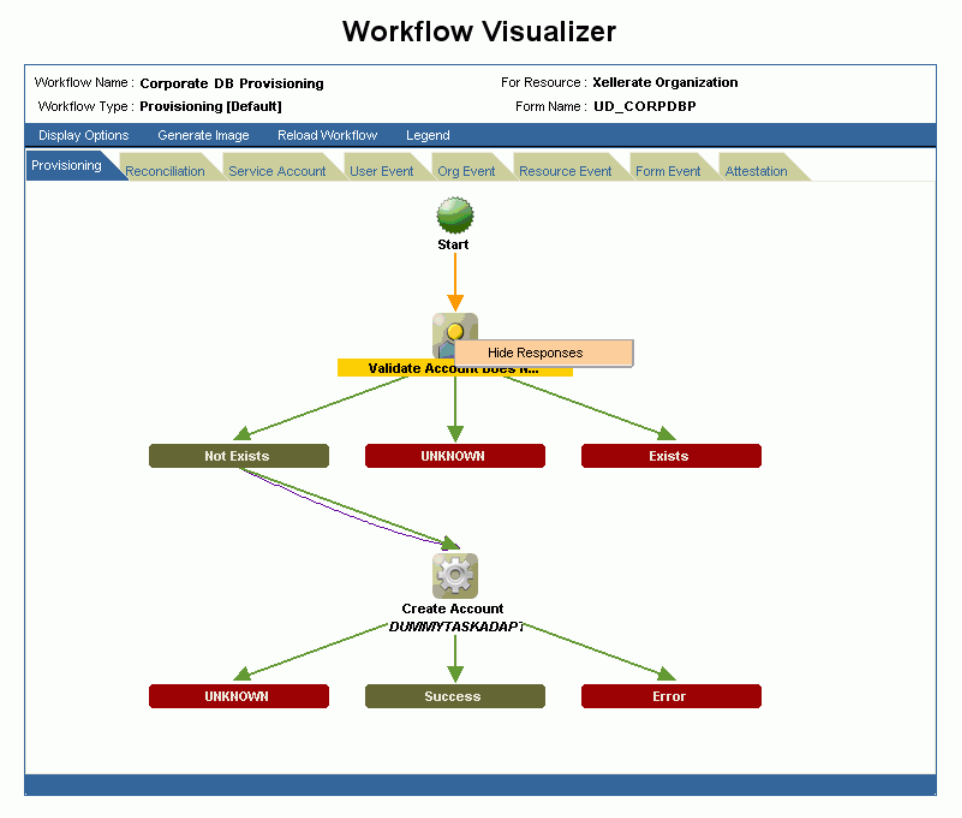
Using Display Options (menu item)

You can also use the Display Options toolbar menu item to display or hide Unknown Response code, Adapter Name, Undo Tasks, and Recovery Tasks. Thus, the workflow will automatically display (paint) 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 will collapse and replace it with an expansion node. The task node name (label) is highlighted in yellow to denote that it was collapsed. Once collapsed, the Hide Responses action option will not appear.

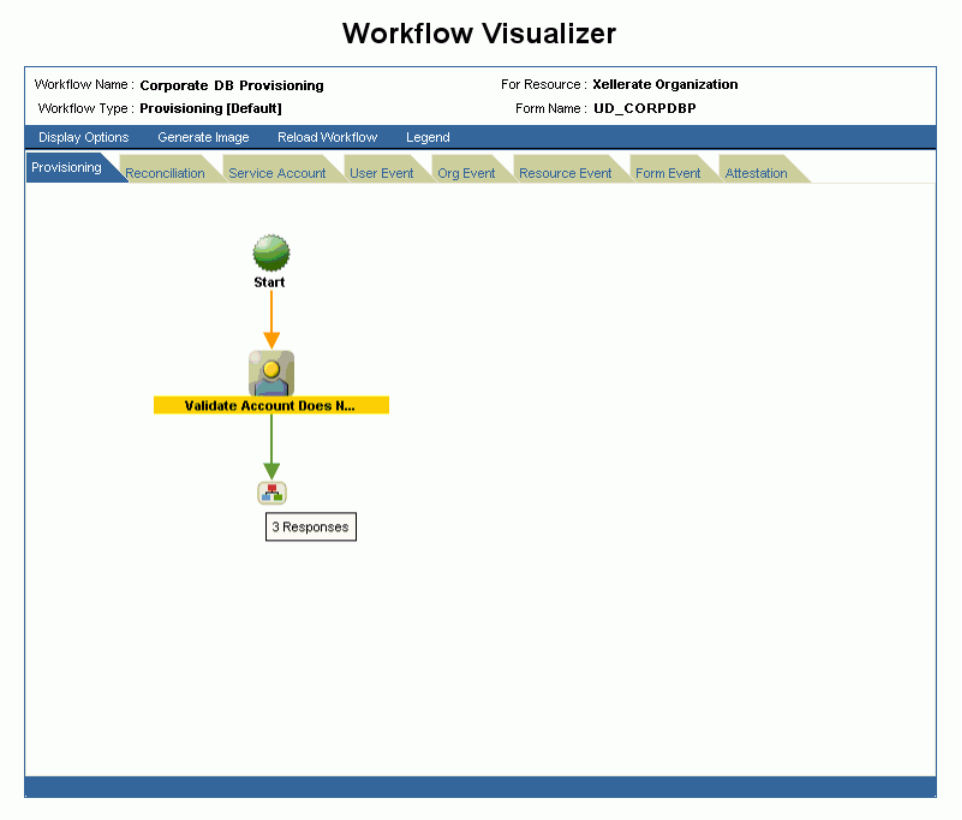
Figure 12–3 Using the Task Node (Right-Click Menu)



Using the Expansion Nodes (Response Sub-Tree)

Task Nodes with more than five response codes (not including the "Unknown Response" code) will 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 will be 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 will indicate how many response codes are associated with it. Unknown Response Codes are hidden by default.

Using the Provisioning Workflow Definition Event Tabs

As previously mentioned, 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 of the workflow definition. By clicking on a event tab, it will display the appropriate task(s) 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 will display a blank view. On the other hand, if there are more than one task sequence for the workflow event type, then the tab will display a pull-down menu where you can select the desired process flowchart.

Provisioning Tab

The Provisioning tab shows the task that will provision a resource. Since the process type is Provisioning, the process flowchart will show all task in order 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 could have adapters attached to them to initiate some provisioning action. If no adapters are attached to it, then a response code of "Event

Processed" is assigned to that task. Additional provisioning process tasks could be generated based on this response code in order 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 gets "deleted", the provisioning process for the service account does not get 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 the user record (such as updating the password and updating the user ID).

Org Event Tab

The Org Event tab shows the workflows that respond to changes to the organization record (such as updating the organization name and updating the organization's parent name or 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 the workflows that respond to state changes of the provisioned resource instance, such as being enabled or disabled.

Form Event Tab

The Form Event tab shows the 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 the detailed information of a particular task, double click the desired task (icon). The Task Detail pop-up window is similar to 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 the Task Information, such as 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 controlling on how the task gets assigned and all associated information.
- **Depends On –** The tab lists all task 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.

Field Name	Description
Adapter Name	This is 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.

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

Task Assignment Tab

This tab specifies the assignment rules for the process task. These rules will determine how the process task will be 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 pre-defined provisioning statuses, which represent the various statuses of the resource object throughout its lifecycle as it is being 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	This is one of the pre-defined provisioning status.
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 your Oracle Identity Manager configurations. Deployment Manager enables you to export the objects that make up your Oracle Identity Manager configuration. 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 back up 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. Use the Deployment Manager to exchange Oracle Identity Manager items between environments. 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

The Deployment Manager lets you save your Oracle Identity Manager configurations in XML files. You can save some or all of the items (objects) in your configuration. This lets you develop and test your configurations in a test environment, and 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 just parts of it. This chapter covers the following topics related to Deployment Manager usage:

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 (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: Exporting Resource Objects with User Defined Fields

When user defined fields are associated with a specific resource object, then 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.

---

1. In the Oracle Identity Manager Administrative and User Console menu, click **Deployment Management** > **Export**. The Deployment Manager opens and the Export Wizard's Search Objects screen appears.
2. Use the Search Objects screen to locate and select objects to export.

   To search for objects:

   a. Use the drop-down menu to select an object type.

   b. Enter a search criterion (leave blank, an asterisk automatically appears, to find all the objects of the selected type).

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

   To select an object, click its checkbox. Click **Cancel** to quit the Wizard.
3. Click **Select Children**. The Select Children screen appears.

   The Select Children screen displays the selected objects and any of their children. Select which children to export.

   To select or remove an item, click its checkbox.

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

   b. Click **Cancel** to quit the Wizard.
4. Click **Select Dependencies**. The Select Dependencies screen appears.

   The Select Dependencies screen displays any objects required by the selected objects. Select which dependencies to export.

   To select or remove an item, click its checkbox.

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

   b. Click **Cancel** to quit the Wizard.

5. Click **Confirmation**. The Confirmation screen appears.
6. Make sure all desired items are selected.
   a. Click **Back** to go to the Search Objects screen.
   b. Click **Cancel** to quit the Wizard.

   Click **Add for Export.** The Add More screen appears.

   Note: After you click **Add for Export**, you can still add more items to this export file.

7. You 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. In the Summary information pane, the objects you are exporting are displayed. In the Unselected Dependencies pane, any dependencies or children of the selected objects that you chose not to export are listed.
8. Make any desired adjustments to your export by using the appropriate options:
   a. Click Reset to clear the form.
   b. Click Legend to see icon definitions
   c. Click Add Object to restart the Wizard and add more items to your export file.

   To remove an object from the Current Selections list:
   a. Right-click the object to remove and select Remove from the shortcut menu.

   Note: If the object has child objects, to remove them all at the same time, select Remove including children from the shortcut menu.

   b. Click **Remove** to confirm. The object is removed from the Current Selections list. If the object is a child or dependency of a selected item, it is added to the Unselected Children, or Unselected Dependencies list.
   c. 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**. The object is added through the Wizard screens. Click to confirm and select any children or dependencies, as needed.
9. Once all the desired items are selected, click **Export**. The Add Description dialog box appears.
10. Enter a description for the file.

    Note: This description is displayed when the file is imported.

11. Click **Export**. The Save As dialog box appears.

    Enter a file name. You can browse to find a location.

12. Click **Save**. The Export Success dialog appears.
13. Click **Close**.

Importing Deployments

You can import objects, saved in an XML file using the Deployment Manager, into your Oracle Identity Manager system. When you import an XML file, you can import all or part of the file. The Deployment Manager also allows you to 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 import, you are given the option to 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:

- Deployment Manager Behavior on Re-Imported Scheduled Task
- Importing an XML File

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

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** > **Import**.
2. Then choose a file for 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.

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

6. After making the desired substitutions, 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.
9. The Confirmation screen appears. 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-hand 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 to your import:
    a. Click **Reset** to clear the form.
    b. Click **Legend** to see icon definitions
    c. To remove an object from the Current Selections list:

       1) Right-click the object to remove and select **Remove** from the shortcut menu.

       2) Click **Remove** to confirm. The item is added to the Objects Removed From Import list.

       Note: If the object has child objects, to remove them all at the same time, select **Remove including children** from the shortcut menu.

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

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

e. To make substitution, click **Add Substitutions**.

f. To add objects from another XML file, click **Add File** (and repeat Steps 2. through 7).

g. Click **Show Information** to see information about your import.

   The Information screen appears and shows basic information about your import.

h. To see more information, click the Show Info Level Messages checkbox, to select it.

i. Click **Show Messages**.

j. 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

Some of the suggested practices and pitfalls to avoid while using Deployment Manager are as follows:

- 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.
- Specify intuitive Export Descriptions.
- 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.

Note: For detailed information on best practices related to using the Deployment Manager, refer to the *Oracle Identity Manager Best Practices Guide*.

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**. This section describes how to run reports detailing the resources available to the users. There are two kinds of reports; Operational Reports and Historical Reports.

This chapter describes the standard operational and historical reports supported by Oracle Identity Manager in the following sections:

Overview of Operational Reports

The following sections describe the out-of-box operational reports in Oracle Identity Manager.

Who Has What (Users' Entitlements)

This report provides administrators or auditors the ability to query entitlements for users that match the query parameters. This report can be used for operational and compliance purposes. This is an operational report, not a historical report.

Resource Access List

This report provides administrators or auditors the ability to query all existing users provisioned to a resource. This report can be used for operational and compliance purposes. This is an operational report, not a historical report.

Overview of Historical Reports

The following sections describe the out-of-box historical data reports in Oracle Identity Manager.

User Access History (Who Had What)

This report provides administrators or auditors the ability to view user's resource access history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user access profile snapshot report. This is a lifetime report showing entire history of user's entitlements.

Resource Access List History

This report provides administrators or auditors the ability to query all users provisioned to a resource over its lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a resource access list snapshot report. This is a lifetime report showing entire history of resource's access list / entitlements.

User Profile History

This report provides administrators or auditors the ability to view user's profile history over user's lifecycle. This report can be used for compliance and forensic auditing purposes. This is not a user profile snapshot report. This is a lifetime report showing entire history of user's profile.

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 hyperlink to the 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. The **Report Input Parameters** 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, that is these fields must be filled. If this is not the case, then 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 content. Three different display formats are available. The format information is included in the report meta data associated with each report. The three 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, then the **First, Previous, Next,** and **Last** navigation links at the top and bottom of the page are active.

Filters

The filter capability is to narrow the search criteria for a report. By default, three filters appear as a drop-down and a text field. Select the type of data from the drop-down, then enter a filter string in the text field. The asterisk (*) wildcard character can be used in the filter text box. An asterisk will represent any number of characters. For example, S*t will match Slashdot and Sat.

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*] (returns all records where the first name starts with 'j'), and then it is filtered again with [Last Name=Smith], this will return only those records which have first name starting with j, and last name as Smith.

Once the filter input is provided and the **Filter** button is clicked, the resulting report will be displayed on the same Report Display Page. The filter dropdowns 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. Clicking on the **CSV Export** button prompts the user with a popup window to save the CSV file locally on the user's 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 like 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:
  - The resource object(s) that have been directly provisioned to the target user(s).
  - The user who have directly provisioned the resource object(s) for the target user(s).
  - The user(s) who received the resource object(s).
- Requests Made. This report displays the 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

This chapter describes how to create, manage, and view attestation tasks in the following sections:

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

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

Attestation Process Configuration

A new 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

Under the top-level menu called Attestation, are the following three menu links:

- Create
- Manage
- Dashboard

These menu items are governed by the same delegated admin permission controls that currently 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 with audit compliance components 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 attestation feature expects this value to be set to at least `Resource Form`.

Creating Attestation Processes

To create a new attestation process:

1. Expand the **Attestation** link and click **Create.** The Step1: Define process identification page appears.
2. On the Step1: Define process identification page, enter values for the fields described in the following table, and then click **Next.**

Field	Description
Name*	Identifies a unique name for the attestation process.
Code	An identifying code (up to 32 characters) for the process.
Description	Detailed description of the attestation process.

Note: The Code and Name must be unique across both disabled and deleted attestation processes.

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.

Note: The Oracle Identity Manager Permission model applies in this scenario, which restricts the displayed list to just those users, organizations, groups, and resources that the logged-in user is allowed read access to.

---

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.

Note: In this scenario, the Oracle Identity Manager Permission model applies, which restricts the displayed list to just those users that the logged-in user is allowed read access to.

---

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

4. In this step, the user specifies 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 Attestation Process Definition *processname*.

   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 section includes the following subsections:

- 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

To disable an attestation process:

1. On the Attestation Process Detail page, click **Disable.** The Disable button only appears when the process is active. The **Disable Attestation Confirmation** page appears.
2. On the **Disable Attestation Confirmation** page, click **Confirm Disable**.

Enabling an Attestation Process

To enable an attestation process:

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

> **Note:** An attestation process can only be enabled if its next start time is in the future.

Deleting an Attestation Process

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.**

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

Running an Attestation Process

This feature supports unscheduled attestation needs. To run an attestation process click **Run Now** on the Attestation Process Detail page. This initiates the attestation

process independent of the attestation schedule. Unscheduled initiation of attestation processes can only be performed by users in process owner group.

Managing Attestation Process Administrators

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.

Note: 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.

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.

Attestation process execution history table contains the columns listed in the following 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 quickly 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.
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.

Column	Description
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 required delegation will include a link in the Delegation Path column. Clicking the link displays a Delegation Path page containing more detailed 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 the User information, the Resource name, and the 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 tooltip

Email Notifications

As part of the attestation process, the attestation engine sends out emails to the concerned parties at various stages. 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.

In all the templates, the form user is defined as XELSYSADM. If desired, you can change it another user. Make sure that email address is defined for the user picked 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 out emails when an attestation task is assigned to a reviewer.
- **Notify Delegated Reviewers:** Used for sending out emails to reviewers when an attestation task is delegated to them.

- **Invalid Attestation Reviewers:** This template is used for sending out emails to users in the Process Owner group if attestation task generation results in invalid reviewers.
- **Notify Declined Attestation Entitlements:** This template is used for sending out emails to users in the Process Owner group if a reviewer declines any entitlements.
- **Attestation Reviewers With No Email Defined:** This template is used for sending out emails to users in the Process Owner group if an email address is not defined for any of the reviewers

Scheduled Tasks

The 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 in the following subsections:

Introduction to the Diagnostic Dashboard

The Diagnostic Dashboard tool is used to validate some of the Oracle Identity Manager pre-requisites. It is also used to verify the installation.

Before you begin, make sure that you have the appropriate system administrator privileges for your Application Server and Oracle Identity Manager environments. Some database related tests need the DBA privileges. If the user doesn't have those privileges, the URL to the test can be provided to a DBA and have the DBA send the result back to the user.

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

It is important to note that the Diagnostic Dashboard tool and Oracle Identity Manager should be installed on the same application server.

Installation Checks

There are three broad scenarios under which this tool will be used: 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.

Tests performed/available 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 to these, the following two reports are also 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

These tests can be run at anytime to check the status of the Oracle Identity Manager installation.

- Displaying 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 check:

- 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 CD media along with the Oracle Identity Manager installer. It is available as a WAR file under the "Diagnostic Dashboard" directory on the CD-ROM.

It is recommended that the Diagnostic Dashboard tool should be deployed on the application server before Oracle Identity Manager is installed.

Installing the Diagnostic Dashboard on OC4J

To install the Diagnostic Dashboard on the OC4J server, do the following:

1. Login 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 `<installer_home>\dashboard\` directory, and then 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 `<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, and 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. Click **Apply.**
8. Confirm that the chosen cluster/server appears under the Server column. Click **Next**.
9. Click **Finish**. The Installing... screen appears. After the application installs successfully, you will see the following message: ***Application XIMDD installed successfully***.
10. Click the **Save to Master Configuration** link, and then click **Save**.
11. Click **Applications** > **Enterprise Applications** link on the left menu pane.
12. Check **XIMDD** check box, then click start. It will display the status that application installed has been successfully started.

Deploying on WebLogic

To deploy Oracle Identity Manager Diagnostic Dashboard on WebLogic:

1. Log in to the administrative console.
   - Start the application server
   - Type the URL http://localhost:7001/console on Internet Explorer.
2. Click **Deployments** link on the left menu pane, and then click **Web Application Modules** link on the left menu pane.
3. Click Deploy a new Web Application Module… link, and 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 `WL_HOME\user_projects\domains\<your-domain-name>\<your-adminserver-name>\upload`).
5. Click **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, the user needs 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 test(s) 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.
Oracle Identity Manager Database Name	Enter Oracle Identity Manager database name
Oracle Identity Manager Schema Name	Enter Oracle Identity Manager scheme 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 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 user can then attest to the entitlements accuracy with an appropriate response. This attestation action, along with the response the reviewer provided, any associated comments, and an audit view of the actual data that the reviewer viewed and attested to, is tracked and fully audited to provide a complete trail of accountability. The way in which all of this manifests itself in Oracle Identity Manager will be in the form of an Attestation Task.

Attestation will be supported in Oracle Identity Manager through the definition of Scheduled Attestation Processes. It is important to understand that an attestation process is not a workflow in itself, as we know and understand workflows in the Oracle Identity Manager context. Instead, it is a business process set up (hard-coded with configuration parameters) in Oracle Identity Manager that creates an Attestation Task for a user in Oracle Identity Manager. The user (the reviewer) must accomplish this process in order to provide correct audit information.

Tracking of attestation activity for a particular provisioned resource instance will be done through tasks in the provisioning processes of resource objects, and the customer has the ability to initiate workflow activity based on these attestation actions. In this way, the framework provides for additional activities to be kicked off (and therefore actual workflow that can be modeled in the process definition form/workflow designer to be initiated) based on the initial attestation action. Thus there will be Attestation Sub-Flows within the provisioning processes defined in Oracle Identity Manager.

Any attestation activity could be kicked off on a periodic basis, or in a completely ad-hoc manner (kick-off now), with the former being the more common use case.

Delegation provides a mechanism by which a reviewer can select certain entitlements within an Attestation Task, and assign them to someone else for review. This in effect creates another Attestation Task assigned to the delegated user.

This appendix includes the following information:

- Attestation Scheduled Task
- Attestation Driven Workflow Capability
- Emails

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. Any disabled attestation process can be enabled, of course. However, it cannot be enabled if its "next run time" is in the past (since that would cause it to run almost immediately). So any user enabling an attestation process will first have to set its next run time into the future.

Deleting Processes

Any Attestation Process can be deleted. This would be a soft-delete, since it would not actually delete the records (must be maintained for audit purposes). Instead, the Attestation Process will be marked as deleted.

Any Process deleted will no longer appear in the administrative interfaces. Since Process names and codes need to be maintained as unique, a name once used will not be available. Hence even though an Attestation Process may have been deleted, 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. This attestation task would show up in a user's Attestation Inbox. The following are the basic components of an Attestation Task

- **A Reviewer**: The user that has to do the attestation activity
- **Task Source**: This defines the way in which 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 which reviewer did the delegation, and which task was the source of the entitlements
- **Attestation Scope**: Defines what the reviewer has to attest to. This is essentially a list of user provisioned resource instances. There will be two ways in which scope can be defined:
  - **Resource-Based**: In this algorithm, all user provisioned resource instances being attested to are for the specified resource. Thus, the attestation scope is any user who has a non-revoked instance of the specified resource.
  - **User-Based**: In this algorithm, the user entitlements being attested to are for a specific set of users. The reviewer will be attesting all the appropriate entitlements that the users that fall within the set have
- **Attestation Data**: Detailed data for the user entitlements that fall within 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. This is important to understand. The reviewer is not attesting to what the user has today. They are attesting to what the user had on the date that the attestation task is asking the reviewer to attest to. Usually, the two dates (today and the attestation date) will be the same. But the distinction is important to eliminate complexities due to activity lag
- **Attestation Actions**: These are the actions that the reviewer can take on the attestation scope. Again, it is important to note that the action is not at the overall attestation task level, but rather against each entitlement in the attestation scope. The framework supports four attestation actions:
  - *Certify*: The reviewer has looked at the details of the user entitlement, and certifies that the user being reviewed is allowed to have this entitlement in the form as it exists (with the data/fine-grained permissions that it has)
  - *Reject*: The reviewer has looked at the details of the user entitlement, and does not think that the user should have this entitlement in the form as it exists
  - *Decline*: The reviewer does not feel qualified to attest to this entitlement, and therefore does not want to accept the responsibility of attesting to the

entitlement. This will mostly be used in cases where processes have been wrongly configured, and will be valuable in early stages of a rollout

– *Delegate*: The reviewer wants to reassign the attestation of this entitlement to someone who they feel is more qualified to make the appropriate judgment

---

Important Note: It is important to remember that the attestation tasks are not workflow tasks in the Oracle Identity Manager definition, since they are not created as part of workflow. This is a completely separate task concept, and as such, will not support all the task management features that our workflow engine supports, like dynamic assignment, escalation, proxy management, and so on.

The Attestation Inbox

The Attestation Inbox is a new concept being introduced in Oracle Identity Manager. While it will look and behave just like the other two inboxes we currently have ("Pending Approvals" and "Open Tasks"), it is not based upon tasks in Oracle Identity Manager workflows. Instead it enables the user to manage attestation tasks (as described earlier) that are assigned to them.

From this inbox, the user will be able to see the attestation tasks assigned to him, view the details of the tasks (in a drill-down manner) and provide responses and comments.

Attestation Request

Any time 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 all the times that an attestation process was executed. The Attestation Request record is composed of some basic identifying and audit data, and also some statistical data that is used in reports. The data includes

- A Request ID
- Date & Time of execution of the process
- Date & Time of completion of the process
- Total Number of Entitlements identified for Attestation
- Number of Entitlements certified
- Number of Entitlements rejected
- Number of Entitlements declined

Each Attestation Task created as a result of this Request will record the Request ID as part of its record.

The Date & Time of completion of the process is considered to be the date and time when for that Request:

```
Total Number of Entitlements = Number Certified + Number
Rejected + Number Declined
```

Financially Significant Resources

Each Resource Object Definition in Oracle Identity Manager would have an extra property that would allow an administrator to mark it as being "financially significant" or not.

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

1. Which resources that should have an attestation process defined do not have one
2. Which resource entitlements that should have been attested to have never 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

There may be cases where the reviewer assigned an Attestation Task cannot realistically attest to all the entitlements contained within that task. There may be multiple reasons for this:

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

In such cases, rather than declining the attestation, the reviewer may want to get other people involved in the review - either as a way of "dividing-and-conquering" the work, or because those people are better equipped to answer the questions that attestation is asking. In other words, the reviewer would like to delegate attestation of certain entitlements within the task to other reviewers. This is supported through delegation.

When a reviewer wants to delegate attestation, they would select a set of entitlements within the task and specify another user to assign those entitlements to for review. This would result in the creation of a new Attestation Task, one that is assigned to the selected reviewer, and 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 Attestation Task it was spawned off from, and all the other usual information (Request ID, and so on). The new Attestation Task is treated as any Attestation Task, and can even be further delegated.

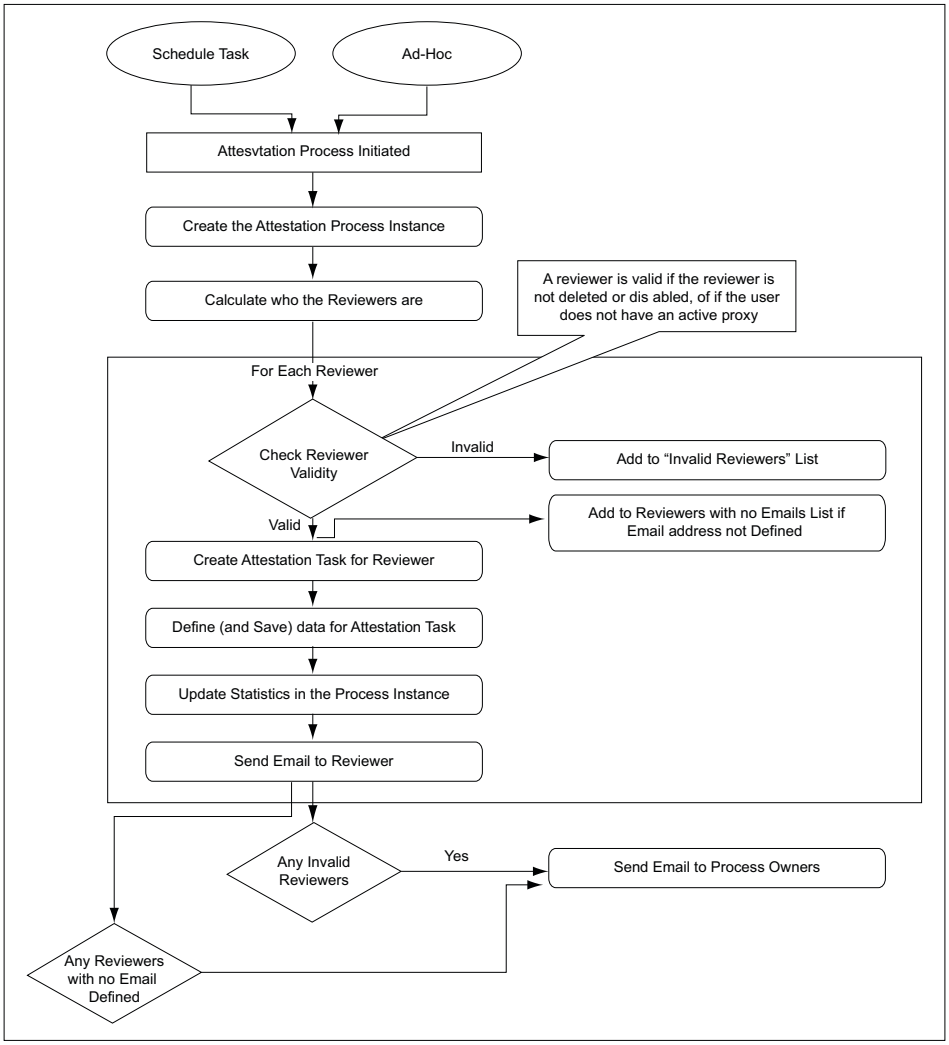
The Attestation Lifecycle Process

The following is a description of the Attestation Lifecycle Process that will be implemented in Oracle Identity Manager. Due to the elements of human interaction, it can be divided into multiple stages.

Stage 1 - Creation of Attestation Task(s)

This is the stage that is kicked off 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 (executed), it will first create a corresponding Attestation Process Instance. It will then look at its definition to figure out who the reviewers for this run of the Attestation Process are. In most cases, it will be just one reviewer, but there are use cases where the reviewer definition could result in a set of reviewers.

For each reviewer found, the process would create an Attestation Task, and set its associated Attestation Date. If the reviewer happens to be invalid, the process will add 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 either disabled or deleted, or if the user has a proxy set up that is currently active. It also computes a list of reviewers with no email address defined.

For each valid reviewer, the process will calculate 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 will retrieve only those resources that are marked as being financially significant. The process would then add a reference and any related information regarding those user entitlements to the Attestation Data of the task. It will also take the number of entitlements covered by that task, and add that to the statistical field for "Total Number of Entitlements

identified for Attestation" in the Process Instance. The process would then send an email to the Reviewer.

After going through each reviewer, the process would check to see if there were any invalid reviewers. If there were, then the list of invalid reviewers will be emailed to the process owner. It also sends email to process owners about the reviewers with no email address defined.

After this stage, all the attestation tasks will be in the attestation inboxes of the reviewers.

Stage 2 - Acting on an Attestation Task

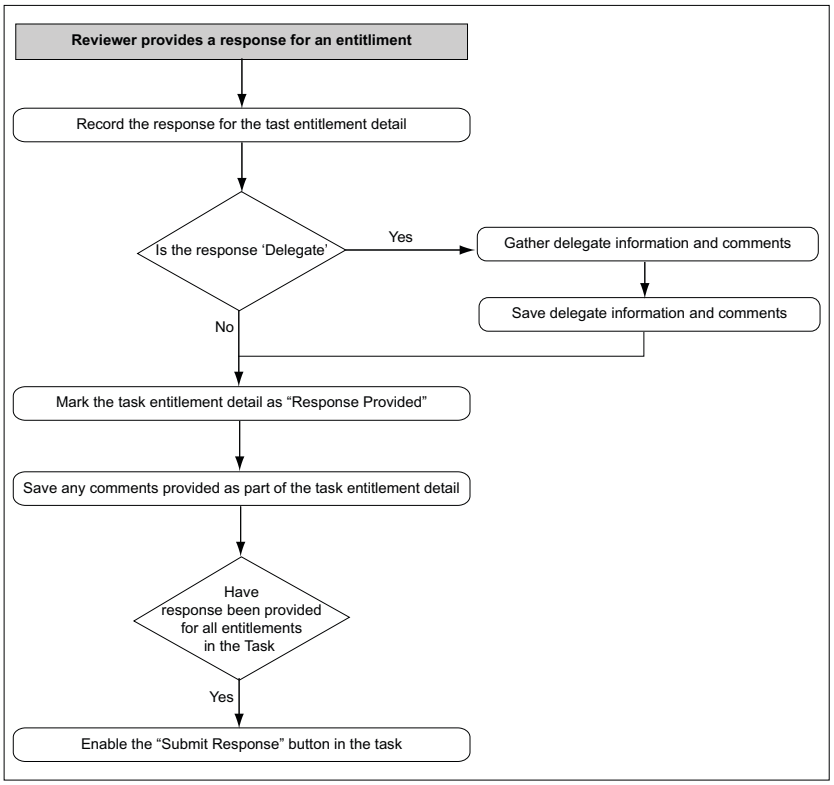
When an Attestation Task is assigned to a reviewer, they will receive an email, and the task will show up in their Attestation Inbox. The reviewer would then go to their Attestation Inbox and look at the task details.

From the task details page, the reviewer would provide a response (optionally, with a comment) for each entitlement. This would also mark that attestation entitlement detail (within the task) as "*Response Provided*".

In case the reviewer's response to any of the entitlements was to "Delegate", then the reviewer would be taken through additional steps of providing the user to delegate the attestation activity to for those specific entitlements. Optionally, the reviewer could provide comments regarding why they are delegating the attestation activity to that user.

Once the reviewer has provided responses to all entitlements, they will be allowed to submit their action (commit) 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

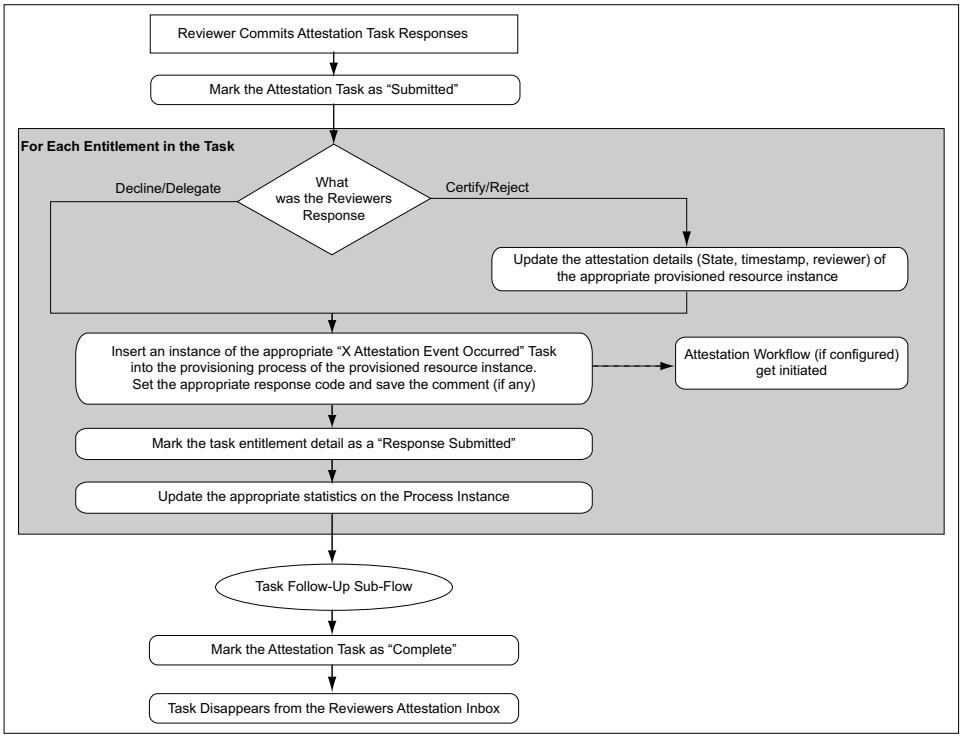
First, the Attestation Task would be marked as "Submitted". At this point the attestation task is frozen, and cannot be acted on any further. Then, for each user entitlement in the attestation task, the response provided will be examined.

If the response was either to certify or reject, then the provisioned resource instance (corresponding to that entitlement) will be updated with this fact. At the provisioned resource instance level, the last attestation result, the time at which last attestation occurred, and who the reviewer was, will be recorded. So if the response was to decline or delegate, then the attestation detail at the provisioned resource level will not be changed.

Irrespective of the response, either the "User Attestation Event Occurred" or "Resource Attestation Event Occurred" task (depending on the attestation process type) will be inserted into the provisioning process of the resource instance. This would kick off any kind of attestation driven workflows that the customer may have defined. Any comment provided will be saved to the task's notes field.

The attestation entitlement detail (within the task) will be marked as "Response Submitted".

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



Irrespective of the response, the appropriate statistics will be updated on the Process Instance. The statistics being updated would be:

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

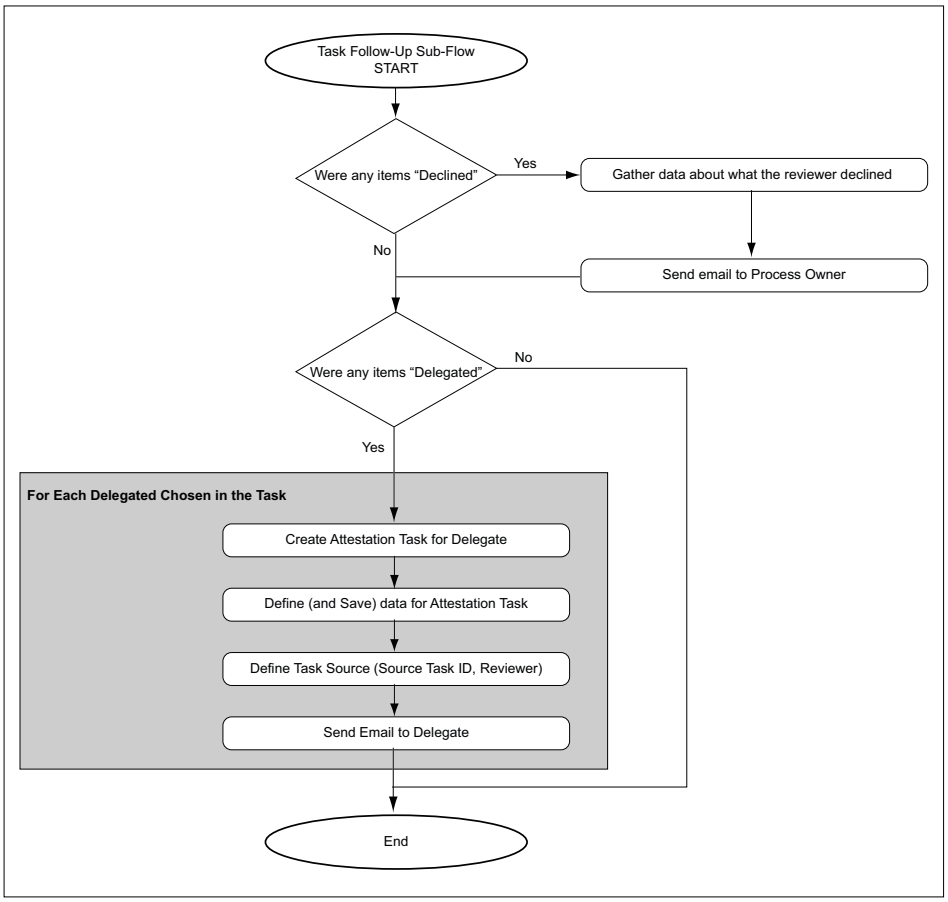
- Number of Entitlements delegated

Once all entitlements are covered, a sub-flow for follow-up action will be initiated. In this flow, the process will examine if the response for any of the entitlements in the task was “declined”. If there were any such entitlements, then the process will create an email to send to the Process Owner outlining the details of the refusal.

Next, the process will examine if the response for any of the entitlements in the task was “delegated”. If there were any such entitlements, then the process will identify all users the reviewer selected as a delegate, and create an Attestation Task for each. Each Attestation Task will be for just those entitlements that the reviewer delegated to the user. The delegated user will receive an email notifying them of the delegation.

Once 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 will be marked as “Complete”.

The Attestation Engine

The Attestation Engine is the engine that implements the Attestation Lifecycle Process. It will be 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). Thus it supports both drivers for initiation of Attestation Processes.

The attestation engine will make use of messaging to off-line processing in the appropriate places, thereby creating transaction separation, and ensuring that there are no end-user performance issues.

Attestation Scheduled Task

There will be a new system scheduled task that will be 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/her.

Variables

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

A new attestation task for attestation process <Attestation Definition.Process Name> has been added to your attestation inbox

Body

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/her.

Variables

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

<Attestation Task.Delegated By User Id> has delegated to you an attestation task from attestation process <Attestation Definition.Process Name>

Body

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 template 'Invalid Attestation Reviewers' 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

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

Some of the reviewers are invalid for the attestation process <Attestation Definition.Process Name>, request <Attestation Request.Request Id>

Body

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

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

User access rights in attestation request <Attestation Request.Request Id> have been declined by <Attestation Task.Reviewer User Id>

Body

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 template 'Attestation Reviewers With No Email Defined' is used to build the email to send to process owners notifying them of any reviewers where there is no email address defined

Variables

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

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 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 is designed to provide information relevant to settings that administrators may want to enable and records they may need to create depending on the features of the Administrative and User Console they plan to enable within their environment. This includes the configuration of resource definitions, process forms, approval processes (and other records that will affect provisioning) within the Oracle Identity Manager Design Console and the editing of the relevant configuration files to support the desired functionality within Oracle Identity Manager Administrative and User Console. Not all of these settings will be 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 "look and feel" of Oracle Identity Manager Administrative and User Console within your environment, refer to the *Oracle Identity Manager Administrative and User Console Customization Guide*.

Administrative and User Console functionality	Configuration Items
If you want to allow users to Self register within Oracle Identity Manager	
To allow users to self register within 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**.

Administrative and User Console functionality	Configuration Items
To designate the number of verification questions to which the user must provide answers.	Set the *Number of Questions* property in the System Configuration form to the number of questions to which you want to require users to provide answers. Be sure that the number of questions you supply within 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.
To designate the list of questions from which user may select when setting their verification questions and answers.	Define a row on the *Lookup.WebClient.Questions* lookup definition for each question you wish to allow (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	You must define an approval task in the *User Registration* approval process.
To allow separate workflow approvals for self registration depending on user profile information	You must define additional approval processes for the *Request* resource definition. You must also create a rule (of type *process determination*) containing a rule element that (at least) requires that the request object action is *Create Entity*. You must then associate the rule with the particular approval process on the *Request* resource definition to allow Oracle Identity Manager to determine which process to select.
To automatically add a user to groups based on self registration	You must 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 they enter upon registration. The criteria in the rules must match the user-entered criteria.
If you wish to prevent certain users from accessing particular pages in the Oracle Identity Manager Administrative and User Console.	
To designate the pages to which all users are to be allowed access	You must 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.	You must specify these pages on the **Menu Items** tab of the applicable administrative user groups (for example, System Administrators, AdminGroup1, and so on).
If you wish to allow administrators to create Oracle Identity Manager accounts for other users	
To allow administrators to create an Oracle Identity Manager account for other users	Ensure that the groups of which these administrators are members are added to the **Administrators** tab of the Organizations that contain the users they are to administer.

Administrative and User Console functionality	Configuration Items
To specify the fields for which values can be entered (for example, are visible) when creating the user account.	You must designate the fields for which you are allowing values to be entered when creating user accounts within the *FormMetaData.xml* file. Refer to the *Oracle Identity Manager Administrative and User Console Customization Guide* for the section of the file to be edited.
To specify the fields for which values will be required when creating the user account.	You must designate the fields for which you must specify values when creating user accounts within the *FormMetaData.xml* file. Refer to the *Oracle Identity Manager Administrative and User Console Customization Guide* for the section of the file to be edited.
To specify the groups of which a user is automatically made a member.	You must 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.
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.
If you want to allow users to edit their Oracle Identity Manager profile	
To require an approval for user-initiated Oracle Identity Manager profile updates	You must define an approval task in the *User Profile Edit* approval process
To allow separate workflow approvals for user-initiated profile updates	You must define additional approval processes for the *Request* resource definition. You must also create a rule (of type *process determination*) containing a rule element that (at least) requires that the request object action is *Modify Entity*. You must then associate the rule with the particular approval process on the *Request* resource definition to allow Oracle Identity Manager to determine which process to select.
To control which fields you want to allow users to be able to edit in their own profile	You must designate which fields you want to allow user to edit in their own profile in the *FormMetaData.xml* file. Refer to the *Oracle Identity Manager Administrative and User Console Customization Guide* for the section of the file to be edited.
If you want to allow administrators to edit the Oracle Identity Manager accounts of other users	
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.

Administrative and User Console functionality	Configuration Items
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. Refer to the *Oracle Identity Manager Administrative and User Console Customization Guide* for the section of the file to be edited.
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. Refer to the *Oracle Identity Manager Administrative and User Console Customization Guide* for a list of the pages that will require this and the section of the file to be edited.

Index

A

C

D

G

H

J

M

O

P

R

S

T

U

V

W