Oracle® Fusion Middleware

User's Guide for Oracle Identity Manager

11*g* Release 1 (11.1.1)

E14316-04

November 2010

ORACLE®

Oracle Fusion Middleware User's Guide for Oracle Identity Manager, 11*g* Release 1 (11.1.1)

E14316-04

Contents

3 Interfaces

4 Deployment Configurations

5   Integration Solutions

6   Auditing

Part II   Oracle Identity Manager Self Service

7   Configuring and Using Self-Service Registration

8   Managing Profile

9   Managing Tasks

10   Managing Requests

Part III   Identity Administration

11   Managing Users

12 Managing Roles

13 Managing Organizations

18 Managing Approval Policies

19 Managing Attestation Processes

Part V Reporting

20 Using Reporting Features

Index

List of Examples

List of Figures

List of Tables

Preface

The Oracle Fusion Middleware User's Guide for Oracle Identity Manager introduces you to Oracle Identity Manager Self Service tasks, and delegated administration functionalities.

Audience

This guide is intended for users who can log in to Oracle Identity Manager and perform Oracle Identity Manager Self Service operations, request for roles and resources, and manage various approval, provisioning, and attestation tasks. This guide is also intended for delegated administrators who can perform identity administration tasks and define authorization policies to delegate administration privileges. In addition, a user with any role can refer to this guide for an introduction and conceptual information about Oracle Identity Manager.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit

http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

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

- *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Suite Integration Overview*
- *Oracle Fusion Middleware User Reference for Oracle Identity Management*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*
- *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Developer's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Administrator's Guide for Authorization Policy Manager*

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.

Part I

Concepts

This part introduces Oracle Identity Manager and describes the concepts related to Oracle Identity Manager.

It contains the following chapters:

- Chapter 1, "Feature Overview"
- Chapter 2, "Architecture"
- Chapter 3, "Interfaces"
- Chapter 4, "Deployment Configurations"
- Chapter 5, "Integration Solutions"
- Chapter 6, "Auditing"

1

Feature Overview

Oracle Identity Manager is a user provisioning and administration solution, which automates the process of adding, updating, and deleting user accounts from applications and directories. It also improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a stand-alone product or as part of Oracle Identity and Access Management Suite.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility.

1.1 Features of Oracle Identity Manager

The features of Oracle Identity Manager can be divided into the following categories:

- User Administration
- Workflow and Policy
- Password Management
- Audit and Compliance Management
- Integration Solutions
- User Provisioning
- Organization and Role Management

1.1.1 User Administration

By deploying self-service features and delegating administrative functions, an organization can increase user productivity, user satisfaction, and operational efficiency.

Oracle Identity Manager Self Service Profile Management

Users can view and edit their own profiles by using the self-service interface of Oracle Identity Manager. This reduces administrative overhead and provides users with control over their identity profiles.

Administrative Profile Management

You can view and manage the profiles of other users subject to access permissions by using the user interface for Oracle Identity Manager administration. This allows you to

create and edit user profiles, change passwords of users, and perform other delegated administration tasks.

Request Management

The self-service interface also enables users to create provisioning requests for resources with fine-grained entitlements, profile management requests, and role membership requests. Business approvers, such as team leaders, line managers, and department heads, can use the same Web-based interface to examine and approve incoming requests. This helps organizations in reducing effort and cost.

Delegated Administration

Oracle Identity Manager features a highly flexible security framework that supports delegation of most administrative functions to any group or user. By moving administration points as close to the user as possible, an organization can achieve tighter control and better security, increasing productivity at the same time.

1.1.2 Workflow and Policy

The use of workflow and policy to automate business and IT processes can lead to improved operational efficiency, enhanced security, and more cost-effective compliance tracking. Oracle Identity Manager provides the following features in this category:

- Policy Management

- Workflow Management

- Dynamic Error Handling

- Transaction Integrity

- Real-Time Request Tracking

Policy Management

Oracle Identity Manager enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators can specify access levels for each resource to be provisioned, granting each user only the exact level of access required to complete the job. These policies can be driven by user roles or attributes, enabling implementation of role-based access control as well as attribute-based access control. Effective blending of role-based and attribute-based policies is key to a scalable and manageable organization provisioning solution.

A request goes through multiple approvals before it is executed. When the request is submitted, it must acquire approvals at different levels. An approval in the system is represented as an approval policy. An approval policy defines the approval process to be invoked and the approval rules associated with the policy. These approval rules help the request engine to select the approval process. Business analysts can define approval policies and approval rules.

Workflow Management

Oracle Identity Manager supports the separation of approval and provisioning workflows. An *approval workflow* enables an organization to model its preferred approval processes for managing resource access requests. A *provisioning workflow* enables an organization to automate IT tasks for provisioning resources with the most complex of provisioning procedures.

The separation of these two workflows empowers business and IT process owners to manage work efficiently with minimum cross-process interferences. It also enables an organization to leverage existing workflows already deployed in systems such as a help desk and HRMS. Oracle Identity Manager provides the Workflow Visualizer that allows business users, administrators, and auditors to visualize task sequences and dependencies to understand process flow and the Workflow Designer to edit and manage the process flow.

Dynamic Error Handling

The error-handling capability of Oracle Identity Manager enables you to handle exceptions that occur during provisioning. Frequent problems, for example, absence of resources, do not stop the entire provisioning transaction or cause it to fail. Business logic defined within the provisioning workflow offers customized fail-safe capabilities within an Oracle Identity Manager implementation.

Transaction Integrity

Based on embedded state management capabilities, Oracle Identity Manager provides the high level of transaction integrity required by other mission-critical organization systems. Oracle Identity Manager features a state engine with rollback and recovery capabilities. When a provisioning transaction fails or is stopped, the system is able to recover and roll back to the last successful state or reroute to a different path, in accordance with predefined rules.

Real-Time Request Tracking

To maintain better control and provide improved visibility into all provisioning processes, Oracle Identity Manager enables users and administrators to track request status in real time, at any point during a provisioning transaction.

1.1.3 Password Management

Password management is one of the foremost issues in organizations nowadays. Implementing a password management solution reduces cost and overhead related to raising tickets or calling help desks. The password management features of Oracle Identity Manager discussed in this section aim to help organizations in this area.

Self-Service Password Management

Users can manage their own enterprise passwords, which might then be synchronized with their managed accounts depending on how the managed accounts are individually configured. The enterprise passwords are managed by using the self-service capabilities of Oracle Identity Manager. If a user forgets the password, Oracle Identity Manager can present customizable challenge questions to enable self-service identity verification and password reset. Research shows that the bulk of help desk calls are related to password reset and account lockout. By reducing the need for help desk calls, this self-service capability lowers costs.

Advanced Password Policy Management

Most best practices are supported out of the box and are configurable through an intuitive user interface. Supported password complexity requirements include: password length, alphanumeric and special characters usage, uppercase and lowercase usage, full or partial exclusion of user name, minimum password age, and historical passwords. Oracle Identity Manager lets you define complex password policies that control the passwords set by users. In addition, Oracle Identity Manager allows the application of multiple policies for each resource. For instance, users with

fewer privileges can be subjected to a more relaxed password policy, whereas privileged administrators can be subjected to a more stringent policy.

Password Synchronization

Oracle Identity Manager can synchronize or map passwords across managed resources and enforce differences in password policies among these resources. In addition, if an organization is using the desktop-based password reset feature of Microsoft Windows, the Active Directory (AD) connector of Oracle Identity Manager can intercept password changes at the AD server and subsequently propagate these changes to other managed resources in accordance with policies. Similar bidirectional password synchronization capability is offered in most Oracle Identity Manager connectors for directory servers and mainframes.

1.1.4 Audit and Compliance Management

Identity management forms a key component in any audit compliance solution of an organization. Oracle Identity Manager helps an organization to minimize risk and reduces the cost of meeting internal and external governance and security audits. This section discusses the features of Oracle Identity Manager that are listed in the audit and compliance management category.

Identity Reconciliation

Reconciliation is one of the significant capabilities of Oracle Identity Manager that enables it to monitor and track the creation, updation, and deletion of account across all managed resources. The process of reconciliation is performed by the reconciliation engine. If Oracle Identity Manager detects any accounts or changes to user access privileges are affected beyond its control, then the reconciliation engine can immediately take corrective action, such as undo the change or notify you. Oracle Identity Manager also helps you to detect and map existing accounts in target resources. This helps in the creation of an organization-wide identity and access profile for each employee, partner, or customer user.

Rogue and Orphan Account Management

A *rogue account* is an account created "out of process" or beyond the control of the provisioning system. An *orphan account* is an operational account without a valid owner. These accounts represent serious security risks to an organization. Oracle Identity Manager can monitor rogue and orphan accounts continuously. By combining denial access policies, workflows, and reconciliation, an organization can perform the required corrective actions when such accounts are discovered, in accordance with security and governance policies.

Service Accounts

Oracle Identity Manager can also manage the life cycle of special *service accounts*, also known as administrator accounts. These accounts have special life cycle requirements that extend beyond the life cycle of an assigned user and across the life cycles of multiple assigned users. Proper management of service accounts can help to eliminate another source of potential orphan accounts.

Comprehensive Reporting and Auditing

Oracle Identity Manager reports on both the history and the current state of the provisioning environment. Some of the identity data captured by Oracle Identity Manager includes user identity profile history, role membership history, user resource access, and fine-grained entitlement history. Oracle Identity Manager also captures data generated by its workflow, policy, and reconciliation engines. By combining this

data along with identity data, an organization has all the required data to address any identity and access-related audit inquiry.

Attestation

Attestation, also referred to as recertification, is a key part of Sarbanes-Oxley compliance and a highly recommended security best practice. Organizations meet these attestation requirements mostly through manual processes based on spreadsheet reports and e-mails. These manual processes tend to be fragmented, are difficult and expensive to manage, and have little data integrity and auditability.

Oracle Identity Manager offers an attestation feature that can be deployed quickly to enable an organization-wide attestation process that provides automated report generation, delivery, and notification. Attestation reviewers can review fine-grained access reports within an interactive user interface that supports fine-grained *certify*, *reject*, *decline*, and *delegate* actions. All report data and reviewer actions are captured for future auditing needs. Reviewer actions can optionally trigger corrective action by configuring the workflow engine of Oracle Identity Manager.

1.1.5 Integration Solutions

A scalable and flexible integration architecture is critical for the successful deployment of organization provisioning solutions. Oracle Identity Manager offers a proven integration architecture and predefined connectors for fast and low-cost deployments.

Adapter Factory

Integrating most provisioning systems with managed resources is not easy. Connecting to proprietary systems might be difficult. The Adapter Factory eliminates the complexity associated with creating and maintaining these connections. The Adapter Factory provided by Oracle Identity Manager is a code-generation tool that enables you to create Java classes.

The Adapter Factory provides rapid integration with commercial or custom systems. Users can create or modify integrations by using the graphical user interface of the Adapter Factory, without programming or scripting. When connectors are created, Oracle Identity Manager repository maintains their definitions, creating self-documenting views. You use these views to extend, maintain, and upgrade connectors.

Predefined Connectors

Oracle Identity Manager offers an extensive library of predefined connectors for commercial applications and other identity-aware systems that are used widely. By using these connectors, an organization can get a head start on application integration. Each connector supports a wide range of identity management functions. These connectors use the most appropriate integration technology recommended for the target resource, whether it is proprietary or based on open standards. These connectors enable out-of-the-box integration between a set of heterogeneous target systems and Oracle Identity Manager. Because the connectors provide a set of components that were originally developed by using the Adapter Factory, you can further modify them with the Adapter Factory to enable the unique integration requirements of each organization.

Generic Technology Connectors

If you do not need the customization features of the Adapter Factory to create your custom connector, you can use the Generic Technology Connector (GTC) feature of

Oracle Identity Manager to create the connector. For detailed information about GTC, see "Generic Technology Connectors" on page 5-2.

> **See Also:** Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for more information about generic technology connectors

1.1.6 User Provisioning

Provisioning provides outward flow of user information from Oracle Identity Manager to a target system. Provisioning is the process by which an action to create, modify, or delete user information in a resource is started from Oracle Identity Manager and passed into the resource. The provisioning system communicates with the resource and specifies changes to be made to the account.

Provisioning includes the following:

- Automated user identity and account provisioning: This manages user identities and accounts in multiple systems and applications. For example, when an employee working in the payroll department is created in the human resources system, accounts are also automatically created for this user in the e-mail, telephone, accounting, and payroll reports systems.

- Workflow and policy management: This enables identity provisioning. Administrators can use interfaces provided by provisioning tools to create provisioning processes based on security policies.

- Reporting and auditing: This enables creating documentation of provisioning processes and their enforcement. This documentation is essential for audit, regulatory, and compliance purposes.

- Attestation: This enables administrators to confirm users' access rights on a periodic basis.

- Access deprovisioning: When the access for a user is no longer required or valid in an organization, Oracle Identity Manager revokes access on demand or automatically, as dictated by role or attribute-based access policies. This ensures that a user's access is promptly terminated where is it no longer required. This is done to minimize security risks and prevent paying for access to costly resources, such as data services.

1.1.7 Organization and Role Management

An organization entity represents a logical container of other entities such as users, roles, and policies in Oracle Identity Manager. In other words, organizations are containers that can be used for delegated administrative model. In addition, organizations define the scope of other Oracle Identity Manager entities, such as users. Oracle Identity Manager supports a flat organization structure or a hierarchical structure, which means that an organization can contain other organizations. The hierarchy can represent departments, geographical areas, or other logical divisions for easier management of entities.

Roles are logical groupings of users to whom you can assign access rights within Oracle Identity Manager, provision resources automatically, or use in common tasks such as approval and attestation. Roles can be independent of organizations, span multiple organizations, or can contain users from a single organization.

2

Architecture

The architecture of Oracle Identity Manager provides a number of compelling technical benefits for deploying a provisioning solution as part of the identity and access management architecture.

Oracle Identity Manager platform automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connects users to resources and revokes and restricts unauthorized access to protect sensitive corporate information.

This chapter consists of the following sections:

- Key Features and Benefits
- How Oracle Identity Manager Works: The Tiers of Oracle Identity Manager
- System Components

2.1 Key Features and Benefits

Oracle Identity Manager architecture is flexible and scalable, and provides the following features:

- Ease of Deployment
- Flexibility and Resilience
- Maximum Reuse of Existing Infrastructure
- Extensive User Management
- Web-Based User Self-Service
- Modular and Scalable Architecture
- Built-in Audit and Compliance
- Based on Leading Software Development Standards
- Powerful and Flexible Process Engine
- Integration By Using the Adapter Factory
- Built-In Change Management

2.1.1 Ease of Deployment

Oracle Identity Manager provides a flexible Deployment Manager utility to assist in the migration of integration and configuration information between environments. The utility exports integration and configuration information as XML files. These files are then imported into the destination environment, which can be staging or

production. You can use the XML files to archive configurations and maintain versions, as well as replicate integrations.

The Deployment Manager provides you with the flexibility to select what to import and export. It also helps you to identify data object dependencies during both import and export steps. This flexibility enables you to merge integration work done by multiple people and to ensure the integrity of any migration.

2.1.2 Flexibility and Resilience

You can deploy Oracle Identity Manager in single or multiple server instances. Multiple server instances provide optimal configuration options, supporting geographically dispersed users and resources for increased flexibility, performance, and control. The Java 2 Enterprise Edition (J2EE) application server model of Oracle Identity Manager also provides scalability, fault tolerance, redundancy, failover, and system load balancing. As deployments grow, moving from a single server to a multiserver implementation is a seamless operation.

2.1.3 Maximum Reuse of Existing Infrastructure

To lower cost, minimize complexity, and leverage existing investments, Oracle Identity Manager is built on an open architecture. This allows Oracle Identity Manager to integrate with and leverage existing software and middleware already implemented within the IT infrastructure of an organization. For example, if an implementation requires integrating with an existing customer portal, then the advanced APIs of Oracle Identity Manager offer programmatic access to a comprehensive set of system functions. This allows IT staff to customize any part of its Oracle Identity Manager provisioning implementation to meet the specific needs of the organization.

2.1.4 Extensive User Management

Oracle Identity Manager enables you to define unlimited user organizational hierarchies and roles. It supports inheritance, customizable user ID policy management, password policy management, and user access policies that reflect customers' changing business needs. It also helps you to manage application parameters and entitlements, and to view a history of resource allocations. In addition, it provides delegated administration with comprehensive permission settings for user management.

Oracle Identity Manager contains a Web-based customizable Oracle Identity Manager Self Service that helps you extensively in user management.

2.1.5 Web-Based User Self-Service

Oracle Identity Manager contains a customizable Web-based, user self-service portal. This portal enables management of user information, changing and synchronizing passwords, resetting forgotten passwords, requesting available applications, reviewing and editing available entitlements, and initiating or reacting to workflow tasks.

2.1.6 Modular and Scalable Architecture

Oracle Identity Manager simplifies the change management required in a dynamic organization. Oracle Identity Manager supports abstraction, which separates the execution logic separate from the application of that logic. For example, if you define

the logic for a task, then the abstraction layer does not combine the logic with the actual execution of that task.

The abstraction layer allows the execution logic to be changed and refined without affecting logic or definitions that still apply. This also provides an iterative provisioning approach that allows IT to implement a provisioning system to fit existing requirements and to ensure that this system can evolve to meet future business needs. As user needs and business policies evolve, outdated execution logic can be "unplugged" from the provisioning instance for replacement with new execution logic. This provides the most cost-effective mechanism for handling change management and supporting the ongoing evolution of processes and systems for the organization.

The J2EE application server model of Oracle Identity Manager provides scalability, fail over, load-balancing, and Web deployment. It is based on an open, standards-based technology and has a three-tier architecture (the client application, an Oracle Identity Manager supported J2EE-compliant Application Server, and an ANSI SQL-compliant database). Oracle Identity Manager can provision LDAP-enabled and non-LDAP-enabled applications.

2.1.7 Built-in Audit and Compliance

Identity management is a key part of any audit and compliance solution. Therefore, auditing and compliance capabilities must be integrated into the core identity management architecture; they should not be add-on utilities for the identity provisioning platform or separate products. Oracle Identity Manager is a fully integrated platform for identity provisioning and identity audit and compliance. An integrated application means that when a resource is brought under its management, the connection can be leveraged for both provisioning and compliance use, avoiding duplication of integration cost.

Oracle Identity Manager provides real-time reporting and up-to-the-minute status reports for all processes with full state information. The complete online analytical processing (OLAP) capability of Oracle Identity Manager supports the most complex reports, analysis, and dynamic queries.

The audit and compliance features need not be restricted to reporting. With these features, no additional product integration effort is required to enable corrective actions as part of an audit and compliance process. For example, when using the attestation feature of Oracle Identity Manager, a reviewer's reject action can directly trigger the workflow to send notification or deprovision a user. An integrated platform provides easy access to identity and transaction data, enabling an organization to control its auditors without lengthy reporting lag time.

2.1.8 Based on Leading Software Development Standards

Oracle Identity Manager incorporates leading industry standards. For example, Oracle Identity Manager components are fully based on a J2EE architecture, so customers can run them from within their standard application server environments. Complete J2EE support results in performance and scalability benefits while aligning with existing customer environments to leverage in-house expertise.

Oracle develops its identity management products on a foundation of current and emerging standards. For example, Oracle is a Management Board member of Liberty Alliance, and incorporates Liberty Alliance developments in its solutions. Oracle participates in the Provisioning Services Technical Committee (PSTC), which operates under the auspices of the Organization for the Advancement of Structured Information Standards (OASIS).

2.1.9 Powerful and Flexible Process Engine

With Oracle Identity Manager, you can create business and provisioning process models in easy-to-use applications. Process models include support for approval workflows and escalations. You can track the progress of each provisioning event, including the current status of the event and error code support. Oracle Identity Manager supports complex, branching and self-healing processes, and nested processes with data interchange and dependencies. The process flow is fully customizable and does not require programming.

2.1.10 Integration By Using the Adapter Factory

Attempting to support all systems with hand-coded adapters is impractical. Oracle developed an automated tool for adapter generation. This tool, the Adapter Factory, supports a wide range of interfaces and virtually any application or device. These adapters run on Oracle Identity Manager server, and do not require agents to be installed or updated on target platforms. In situations where the target application resource does not have a network-enabled interface, you can create remote integration by using UDDI/SOAP-based support. With the Adapter Factory, integrations that take months to implement can now be accomplished in a few days. Numerous adapters can be generated instantly. With the Adapter Factory, you can keep existing integrations updated, and you can support new integration needs quickly. Oracle Identity Manager has the ability to run programs on external third-party systems by using the remote managers.

2.1.11 Built-In Change Management

Oracle Identity Manager enables you to package new processes, import and export existing ones, and move packages from one system to another.

2.2 How Oracle Identity Manager Works: The Tiers of Oracle Identity Manager

Oracle Identity Manager is based on the n-tier J2EE application architecture. Oracle Identity Manager architecture contains the following tiers:

- Presentation Tier

- Business Services Tier

- The Data Tier

Figure 2–1 illustrates Oracle Identity Manager architecture.

Figure 2–1   Oracle Identity Manager Architecture
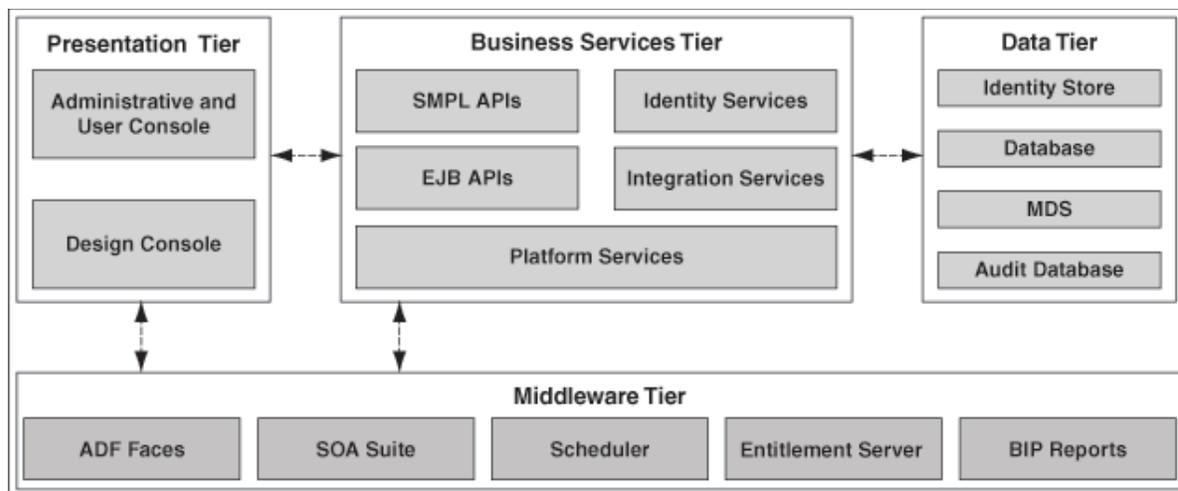
2.2.1 Presentation Tier

The Presentation tier consists of two clients, Oracle Identity Manager Administrative and User Console and Oracle Identity Manager Design Console.

Oracle Identity Manager Administrative and User Console is a Web-based thin client that can be accessed from any Web browser. This client provides user self-service and delegated administration features that serve most of the users of Oracle Identity Manager.

Oracle Identity Manager Design Console provides the full range of Oracle Identity Manager system configuration and development capabilities, including Form Designer, Workflow Designer, and the Adapter Factory. You can access Oracle Identity Manager Design Console by using a desktop Java client.

Oracle Identity Manager Design Console is implemented as a Java Swing client that communicates directly with the Business Services layer in the application. It also supports a highly sophisticated delegated administration model, guaranteeing that users can only work on those parts of the application configuration that they have been given privileges to.

> **See Also:** *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* and *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for details about using Oracle Identity Manager Administrative and User Console and Oracle Identity Manager Design Console

In many enterprises, there is a requirement for the provisioning system to support a custom developed client. Some of the requirements that drive this are:

- Integration of the client into an existing enterprise portal and adherence to enterprise portal standards

- Creation of custom flows for user interaction

- Creation of custom pages built around unique requirements from the provisioning system

To support customization, Oracle Identity Manager exposes the bulk of the necessary functionality via its published public APIs. The client environment for Oracle Identity Manager is customizable via Java APIs.

2.2.2 Business Services Tier

The Business Services Tier is implemented as an Enterprise JavaBeans (EJB) application. The core functionality for Oracle Identity Manager platform is implemented in Java using a highly modular, object-oriented methodology. This makes Oracle Identity Manager flexible and extensible. The Business Services Tier for Oracle Identity Manager includes the following services and capabilities:

- The Core Services that comprise the core of the business features offered by Oracle Identity Manager, such as the User Management Service, the Policy Management Services, and the Provisioning and Reconciliation Services.

- The API Services that describe the APIs supported by Oracle Identity Manager that allow custom clients to integrate with Oracle Identity Manager. This includes a rich set of APIs that expose the business functionality of Oracle Identity Manager for use by custom clients, in product customization, and in plug-in and adapter development.

- The Integration Services based on the Adapter Factory and Connector Framework, which dynamically generates integration code based on the metadata definition of the adapters.

- The Platform Services that are crucial to the business features offered by Oracle Identity Manager, such as the Request Management Service, the Entity Manager Service, and the Scheduler Service.

2.2.2.1 The API Services

The API Services describe the APIs supported by Oracle Identity Manager that allow custom clients to integrate with Oracle Identity Manager. This includes a rich set of APIs that expose the business functionality of Oracle Identity Manager for use by custom clients, in product customization, and in plug-in and adapter development.

The API Services consist of:

- **SPML APIs:** Service Provisioning Markup Language (SPML) is a standard for managing the provisioning and allocation of identity information and system resources within and between organizations. Oracle Identity Manager supports a set of SPML-based Web services that expose identity administration functionality to the clients. The APIs provide support for:

  - Adding, modifying, and deleting identities

  - Adding, modifying, and deleting roles

  - Adding and deleting role memberships

  These APIs support requests coming into Oracle Identity Manager for administration purposes, which is distinct and separate from SPML as the protocol used to integrate with provisioning targets.

- **EJB APIs:** Highly granular access to the functionality of the platform is via a set of EJB. These session beans are the basis for functionality implemented in Oracle Identity Manager Web application clients. It is also the interface that custom clients can use to access Oracle Identity Manager capabilities.

2.2.2.2 Integration Services

A scalable and flexible integration architecture is critical for the successful deployment of provisioning solutions. Oracle Identity Manager offers an integration architecture for fast and low-cost deployments.

Oracle Identity Manager integration services provide all the components required to support the development, deployment, and maintenance of connectors. This includes entity management services, metadata management, code generation tools, and deployment tools. The integration services includes:

- Connector Framework
- Adapter Factory
- Generic Technology Connector
- Remote Manager

> **See Also:** "Integration Solutions" on page 5-1 for details about how to define adapters by using the Adapter Factory.

2.2.2.2.1 Connector Framework

Oracle Identity Manager connectors are packaged solutions that are used to integrate with target applications for the purposes of managing identities in those applications. Examples of such target applications are Microsoft Active Directory or Oracle E-Business Suite. A connector can be predefined by Oracle for particular target systems or can be custom developed.

Because a predefined connector is designed specifically for the target application, it offers the quickest integration method. These connectors support popular business applications such as Oracle eBusiness Suite, PeopleSoft, Siebel, JD Edward and SAP, as well as technology applications such as Active Directory, Java Directory Server, UNIX, databases, and RSA ClearTrust. Predefined connectors offer the quickest integration alternative because they are designed specifically for the target application. They use integration technologies recommended by target and are preconfigured with application specific attributes.

If predefined connectors does not use integration technologies recommended by target, then a custom connector can be developed. The Adapter Factory tool in Oracle Identity Manager Design Console provides a definitional user interface that facilitates such custom development efforts without coding or scripting.

A connector contains:

- Multiple connector-specific Oracle Identity Manager entities such as resource objects, data forms, provisioning workflows, and adapters
- Target-specific Java libraries that provide the underlying functions such as connectivity, authentication and user account management
- Event triggers that wire provisioning operations to both identity profile changes and policy operations

The connector framework combines all of these components together into a functional connector that is run at appropriate times, either manually based on user interaction or based on system triggering. It defines the various operational triggers, policy triggers, and hooks that allow the connector operation to be tailored to specific requirements.

2.2.2.2.2 Adapter Factory

The Adapter Factory is a code-generation tool provided by Oracle Identity Manager. It enables an Oracle Identity Manager application developer to create Java classes, known as adapters. An adapter provides the following benefits:

- It extends the internal logic and functionality of Oracle Identity Manager.

- It interfaces with any software resource by connecting to that resource with the help of the API of the resource.

- It enables the integration between Oracle Identity Manager and an external system.

- It can be generated without manually writing code.

- It can be maintained easily because all the definitions for the adapter are stored in a repository. This repository can be edited through a GUI.

- A user in Oracle Identity Manager can retain the domain knowledge about the integration, while another user can maintain the adapter.

- It can be modified and upgraded.

The Adapter Factory provides rapid integration with commercial or custom systems. Users can create or modify integrations by using the graphical user interface of the Adapter Factory, without programming or scripting. When connectors are created, Oracle Identity Manager repository maintains the definitions and creates self-documenting views. You use these views to extend, maintain, and upgrade connectors.

> **See Also:** *"Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager"* for details about how to define adapters by using the Adapter Factory

2.2.2.2.3 Generic Technology Connector

To integrate Oracle Identity Manager with a target system that has no corresponding predefined connector, you can create a custom connector to link the target system and Oracle Identity Manager. If you do not need the customization features of the Adapter Factory, then you can create the connector by using the Generic Technology Connector (GTC) feature of Oracle Identity Manager.

You can quickly and easily build a basic connector without advanced features and customized behavior by using generic connectivity technologies such as SPML and JDBC. GTC is a wizard that provides an alternative environment for connector development to rapidly create all the necessary functional components that make up a target system connector in Oracle Identity Manager.

The reconciliation and provisioning modules of a generic technology connector are composed of reusable components that you select. Each component performs a specific function during provisioning or reconciliation.

The components that constitute a generic technology connector are called providers. Each provider performs a transport, format change, validation, or transformation function on the data that it receives as input. In other words, data items processed by a provider are moved to a new location, validated against specified criteria, or undergo modification in structure or value. Data sets describe data structures arranged in the form of layers, with data flowing from one layer to another during provisioning and reconciliation.

The GTC employs a Web-based graphical wizard that displays the data flows being defined within the connector. It stores in metadata all the configuration information about the connector so that it can reload the GTC view of the connector and enable

ongoing maintenance of the connector in the same graphical environment. Because the GTC builds the connector by using the standard connector framework, the application developer can access the standard Oracle Identity Manager development environment and make further modifications to the generated connector. However, after the GTC-based connector has been customized in this manner, it can no longer be managed or maintained using the GTC.

> **See Also:** "Generic Technology Connectors" on page 5-2 for detailed information about the functional architecture and features of GTC

2.2.2.2.4 Remote Manager

The Remote Manager is an Oracle Identity Manager server component that runs on a target system computer. It provides the network and security layer required to integrate with applications that do not have network-aware APIs or do not provide security. It is built as a lightweight Remote Method Invocation (RMI) server. The communication protocol is RMI tunneled through Hypertext Transfer Protocol/Secure (HTTP/S).

The J2EE RMI framework enables the creation of virtually transparent, distributed services and applications. RMI-based applications consist of Java objects making method calls to one another, regardless of their location. This enables one Java object to call methods on another Java object residing on another virtual computer in the same manner in which methods are called on a Java object residing on the same virtual computer.

Figure 2–2 shows an overview of the Remote Manager architecture.

Figure 2–2   Remote Manager Architecture
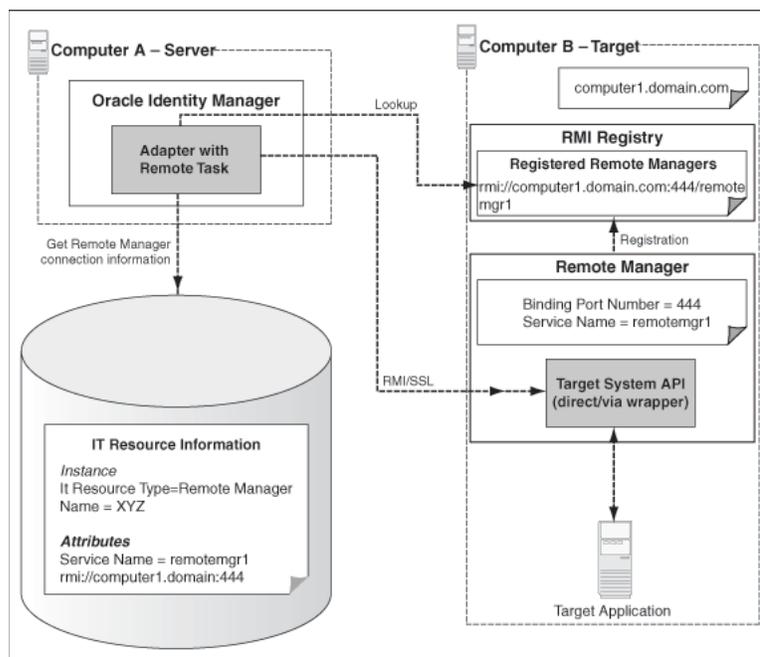
> **See Also:** "Creating and Testing a Remote Manager IT Resource" and "Remote Manager" for information about the Remote Manager and its configuration in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

2.2.2.3 Platform Services

The Platform Services include:

- Request Service
- Authorization Service
- Plug-In Framework
- SoD Engine Framework
- Scheduler Service

2.2.2.3.1 Request Service

Oracle Identity Manager architecture includes a request service that allows you to configure approval workflows. To deliver this functionality, Oracle Identity Manager uses Oracle Service Oriented Architecture (SOA) Suite.

Oracle SOA Suite enables you to build service-oriented applications and deploy them to your choice of middleware platform. It consists of a number of components, but for the purposes of delivering comprehensive workflow capabilities, Oracle Identity Manager relies on the following components:

- **BPEL Process Manager:** Oracle BPEL Process Manager provides a comprehensive solution for creating, deploying, and managing cross-application business processes with both automated and human workflow steps. It also provides audit trails for both completed and running processes, and process history that enables process improvement.

- **Human Request Service:** Although the BPEL standard does not cover manual tasks, it supports asynchronous services. Therefore, the Oracle SOA Suite supports the Human Request Service, which is a manual task service, so that manual steps can be included in standard BPEL processes. Oracle Identity Manager Administration and User Console includes a task list that allows users to view and interact with assigned tasks being managed within the Human Request Service.

- **BPEL Designer:** The Oracle BPEL Designer is available as a plug-in for JDeveloper and offers a visual design paradigm for creating and deploying BPEL-based processes.

Oracle Identity Manager provides an abstraction service on top of the SOA suite that optimizes and simplifies the interaction of users with the SOA suite. This service includes capabilities to register BPEL composites for use in Oracle Identity Manager, define parameterized variables for use in the BPEL and Human Workflow modules, and APIs that are used by the task list and custom development.

> **See Also:** "Approval Workflows" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about workflows and BPEL composites.

The Request Service also provides the services used to raise and track requests in Oracle Identity Manager. A request allows a user to ask that an action be taken after obtaining the necessary approvals, and that a tracking record of the entire process and its status be maintained. The request can be for various types of actions that are defined as request types. The request types can be:

- Creating, modifying, or deleting an entity
- Enabling or disabling an entity
- Provisioning a resource to a user or a set of users

- Adding or removing an identity as a member of a role

The request service supports various types of requests and has the ability to accommodate multiple request types. Oracle Identity Manager provides a number of predefined request model that cover the most common use cases. The request service also provides support for request templates, that allow you to customize the request types for a specific requirement. In addition, request templates allow you to customize the request types for a specific requirement.

The request service defines the flow models by which data provided in a request flows through the various services in Oracle Identity Manager. This includes invoking approval workflows at the correct time, monitoring the status of the workflows, and running the request if approval is received.

Both transaction data and history data for requests is maintained, which supports audit and compliance requirements.

> **See Also:** "Managing Requests" on page 10-1" for information about creating requests and perform request-related operations in the task list of Oracle Identity Manager Self Service

2.2.2.3.2 Authorization Service

Oracle Identity Manager is a security product and requires a strong level of access control over what users can view and change in the application. To meet this requirement, customers must be able to define authorization policies that determine at runtime whether or not a particular action is allowed. This is controlled by the authorization service embedded within Oracle Identity Manager. The authorization service is built on Oracle Entitlements Server (OES), which is a sophisticated authorization product. OES enables centralized management of entitlements and authorization policies to granularly determine access to both application components and application business objects.

The OES architecture is made up of two major components. The administration application acts as the policy administration point (PAP) and is used to manage policy, configuration, roles, and entitlements. The second major component is the use of one or more Security Modules (SMs) that are stored in the application container. The SMs evaluate fine-grain access control polices at the policy decision point (PDP) and enforce it at the policy enforcement point (PEP). The SMs are also the integration point for access to external attributes that can be incorporated into the policy.

Figure 2–3 shows the architecture of OES-based authorization service:

Figure 2–3 OES-Based Authorization Service
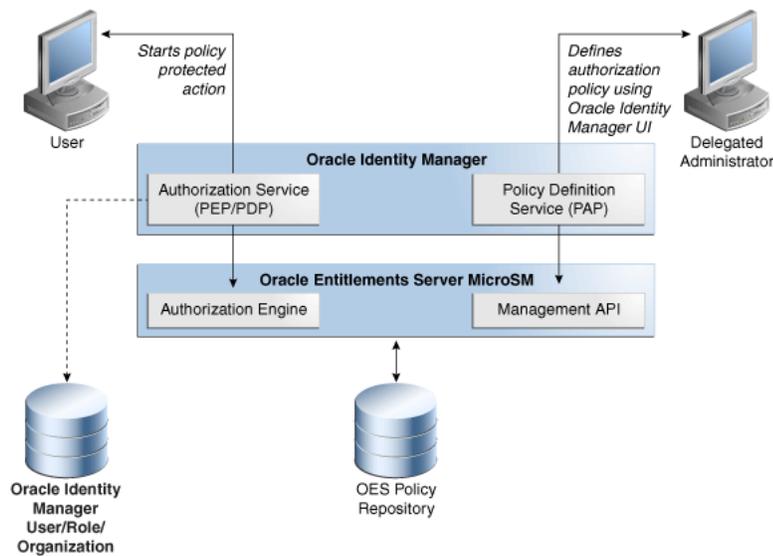
Each time a privilege check is requested, the following takes place:

- Oracle Identity Manager connects to the authorization service to prepare access decision for the operations performed on protected entities.

- The service then finds and evaluates the policy or policies that apply to the resource.

- All information required to evaluate a policy is collected by the Security Modules at run time.

- If the policy references subject by role, all roles are evaluated and the access decision is made.

Oracle Identity Manager provides an abstraction service on top of OES that optimizes and simplifies the definition of policies in Oracle Identity Manager. This service includes a policy definition UI that allows the definition of authorization policies that are feature specific and support fine-grained controls for attributes and functions on entities such as users and roles. For information about the structural components of authorization policies and how to create and manage authorization policies, refer "Creating and Managing Authorization Policies" on page 15-2.

2.2.2.3.3 Plug-In Framework

The Plug-in Framework allows customers to easily extend and customize the capabilities of the out-of-the-box Oracle Identity Manager features. The features expose specific plug-in points in the business logic where extensibility can be provided. An interface definition accompanies each such point and is called the plug-in interface. Customers can create code that extends these plug-in interfaces and defines customizations based on their business needs. These plug-ins are deployed and registered with Oracle Identity Manager by using the Plug-in Manager. Oracle Identity Manager then incorporates the plug-ins into the feature processing from that point onward.

Feature developers do not have to keep a track of where the custom implementations are stored and how they are loaded. The plug-in framework supports loading plug-ins from the classpath, from the file system, and from the database.

> **See Also:** "Developing Plug-ins" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about the plug-in framework

2.2.2.3.4 SoD Engine Framework

An attempt to enforce good compliance practices is through the definition of Segregation of Duties (SoD) policies. SoD is broadly defined as a way of preventing a user from acquiring a conflicting set of entitlements. This conflicting set is also referred to as a toxic combination. An example of a toxic combination is that a person should not have the ability to create and approve the same purchase order. Enterprises often have business application-specific SoD engines that define and enforce SoD policies on the entitlements users have within those business applications. Examples of such SoD engines are OAACG and SAP GRC.

The SoD Engine Framework allows customers to integrate Oracle Identity Manager with their choice of SoD Engine to enable SoD checks at appropriate points in the request and provisioning process. Oracle Identity Manager can send a request for an SoD check to the SoD Engine through the SoD Invocation Library (SIL). SIL provides a common service interface to all supported SoD engines. The common service interface provides an abstraction on the business components within Oracle Identity Manager. As a result, SoD checks do not have to take care of the correct data formats required by the SoD Engine and also the interpretation of the results returned.

SoD checks can be run at various times in the provisioning lifecycle, such as during an access request, during the approval workflow execution, or during the provisioning execution. If a violation is detected, then the request or resource is marked as being in violation, and the approver or administrator is responsible for deciding whether to proceed or not. If violations are detected during request processing, then various approval workflows can be invoked that allow for higher levels of approval.

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about SoD

2.2.2.3.5 Scheduler Service

Business systems frequently make use of scheduling systems, which are configured to run other programs at specified times. Scheduling systems run applications that generate reports, reformat data, or perform audits at regular intervals of time. Scheduling systems often run batch jobs or scheduled jobs that perform routine work automatically at a prescribed time.

Scheduling systems are an integral part of any enterprise provisioning solution. Provisioning often involves tasks to be performed in a time-based manner. Some examples are:

- Running a nightly job to reconcile all changes made directly on a managed application

- Do escalations of assigned tasks that have not been handled within a specified time period

- Execute requests at a specific time

Oracle Identity Manager platform includes the Scheduler to provide the scheduling capabilities necessary for enterprise provisioning requirements. This Service is managed as part of Oracle Identity Manager platform and not as an independent product. Figure 2–4 provides an overview of Oracle Identity Manager Scheduler architecture.

Figure 2–4   Oracle Identity Manager Scheduler Architecture
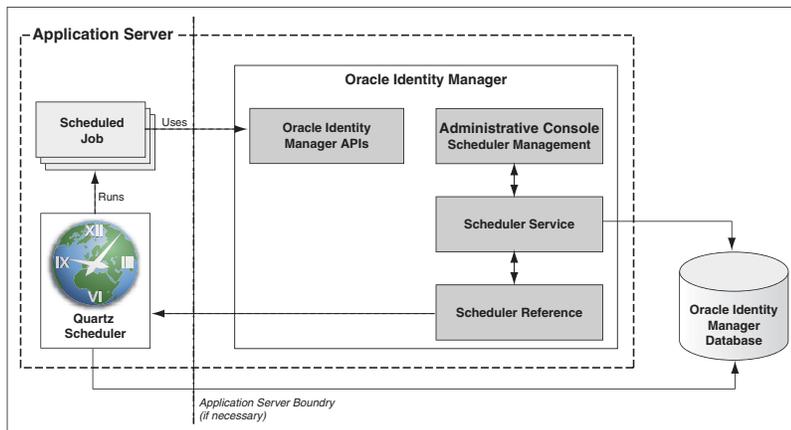
Key capabilities provided by the Scheduler service are:

- The ability to create simple or complex schedules for running thousands of jobs

- The ability to run the scheduling service as a clustered service to provide the necessary high availability capabilities including fail-over and load balancing

- The ability to persist the job definitions for management and fail-over support

- The ability to create, modify, enable, disable, and delete jobs and manage individual job runs by using an administrative UI

- The ability to run a job in an ad-hoc fashion outside of regularly scheduled runs

- The ability to manage errors and failures

- The ability to maintain history of job runs, including statistics and results of these runs

- The ability to manage the Scheduler service itself

> **See Also:**
>
> - "Managing Scheduled Tasks" chapter detailed information about the Scheduler service and creating and implementing custom scheduled tasks in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*

2.2.3 The Data Tier

Oracle Identity Manager is driven by data and metadata, which provides flexibility and adaptability to Oracle Identity Manager functionalities. Oracle Identity Manager data tier consists of Oracle Identity Manager repository or database, which manages and stores Oracle Identity Manager data and metadata in an ANSI SQL 92-compliant relational database, and an optional LDAP Identity Store.

This section describes the data tier in the following topics:

- Oracle Identity Manager Database

- The Metadata Store

- The Identity Store

2.2.3.1 Oracle Identity Manager Database

Oracle Identity Manager repository is the authoritative store for the *Who Has What, When, How, and Why* data that is the core value of the identity administration and provisioning system. The data stored in Oracle Identity Manager database falls into the following broad categories:

- Entity Data: Users, organizations, roles, role memberships, resources, provisioned resources

- Transactional Data: Requests, approval and provisioning workflow instances, human tasks

- Audit Data: Request history, user profile history

High Availability

The database provides a scalable and redundant data layer to avoid downtime and performance issues. Reliability, recoverability, timely error detection, and continuous operations are primary characteristics of a highly available solution.

Oracle Identity Manager architecture relies on the corresponding capabilities provided by the Database Management System that is used with the product. These capabilities must:

- Encompass redundancy across all components

- Provide protection and tolerance from computer failures, storage failures, human errors, data corruption, lost writes, system hangs or slowdown, and site disasters

- Recover from outages as quickly and transparently as possible

- Provide solutions to eliminate or reduce planned downtime

- Provide consistent high performance

- Be easy to deploy, manage, and scale

- Achieve Service Level Agreements (SLAs) at the lowest possible total cost of ownership

A broad range of high availability and business continuity solutions are available. You can find out more about maximizing database availability by using technologies such as Oracle Real Application Clusters (Oracle RAC) and Oracle Data Guard at the following Web site:

http://www.oracle.com/technology/deploy/availability/htdocs/maa.htm

Reporting

The rich set of data stored in Oracle Identity Manager repository can be viewed through detailed reports that support management and compliance requirements. Oracle Identity Manager provides support for data reporting through the use of Oracle BI Publisher, which is an enterprise reporting solution and provides a single reporting environment to author, manage, and deliver all of your reports and business documents. Utilizing a set of familiar desktop tools, such as Microsoft Word, Microsoft Excel, or Adobe Acrobat, you can create and maintain report layouts based on data from diverse sources, including Oracle Identity Management products.

Oracle Identity Manager provides a set of standard Oracle BI Publisher report templates. However, you can customize each template to change its look and feel. in addition, you can create your own custom reports by leveraging Oracle Identity Manager database schema.

2.2.3.2 The Metadata Store

The logic underlying Oracle Identity Manager is metadata driven. The structural and behavioral aspects are described by using metadata. Oracle Identity Manager architecture relies on Oracle Metadata Services (MDS) to provide a unified store for metadata. This ensures consistent and reliable access to the metadata for Oracle Identity Manager and for the other Fusion Middleware components that it is built on. The same metadata that is used during the design phase of an application is used at application runtime through the metadata services layer. This ensures consistency through the lifecycle of Oracle Identity Manager, as shown in Figure 2–5. MDS also provides common administrative tooling for the metadata that can be used across various types of metadata stored in the common repository.

Figure 2–5   Metadata Services
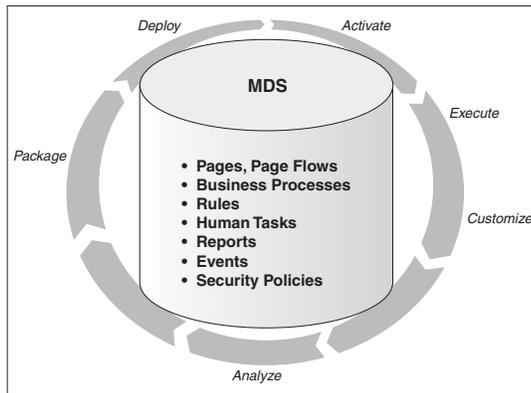
Key features and architectural principles of the MDS include:

- Simplified resource management through a single, unified repository for all artifacts used by various Fusion Middleware components

- Management of the metadata lifecycle for each artifact as it moves through the various stages of development, testing, staging, and production

- Sharing and reuse of metadata across components

- Categorization and reuse of artifacts, encouraging reuse, and promoting consistency

- Versioning capabilities, which form the basis for various features

- An upgrade-safe and layered customization mechanism through which metadata and application logic can be tailored per usage of the metadata

- Advanced caching and assembling techniques coupled with configurable tuning options to optimize performance

Metadata accessed and managed via MDS can be in a file-based repository or a database-based repository. In Oracle Identity Manager architecture, the metadata is in Oracle Identity Manager database to take advantage of some of the advanced performance and availability features that this mode provides.

2.2.3.3 The Identity Store

Oracle Identity Manager 11*g* Release 1 (11.1.1) provides the ability to integrate an LDAP-based identity store into Oracle Identity Manager architecture. In 9.x releases, Oracle Identity Manager identity store is in Oracle Identity Manager database. Therefore, Oracle Identity Manager integrates with LDAP as a provisioning target, or

you can build custom integration between Oracle Identity Manager users and LDAP users. However, in 11*g* Release 1 (11.1.1), you can connect and manage an LDAP-based identity store directly from Oracle Identity Manager. Using this feature, you can use advanced user management capabilities of Oracle Identity Manager, including request-based creation and management of identities, to manage the identities within the corporate identity store.

In this deployment architecture, user identity information is stored in Oracle Identity Manager database to support the relational functionality necessary for Oracle Identity Manager to function, as well as in the LDAP store. All data is kept in sync transparently without the need for provisioning actions and setting up policies and rules. Identity operations started within Oracle Identity Manager, such as user creation or modification, are run on both the stores in a manner that maintains transactional integrity. In addition, any changes in the LDAP store made outside of Oracle Identity Manager is pulled into Oracle Identity Manager and made available as a part of the identity context.

> **See Also:** ""Integration Between LDAP Identity Store and Oracle Identity Manager" on page 4-20" for more information about LDAP store integration and configuration

2.3 System Components

Oracle Identity Manager is built on an enterprise-class, modular architecture that is both open and scalable. Each module plays a critical role in the overall functionality of the system. Figure 2–6 illustrates the system components of Oracle Identity Manager.

Figure 2–6   System Components of Oracle Identity Manager

Oracle Identity Manager user interfaces define and administer the provisioning environment. Oracle Identity Manager offers two user interfaces to satisfy both administrator and user requirements:

- Powerful Java-based Oracle Identity Manager Design Console for developers and system administrators

- Web-based Administration and Oracle Identity Manager Self Service interfaces for identity administrators and users respectively

This section describes the following Oracle Identity Manager components:

- Identity Administration
- Provisioning
- Audit and Reports
- Reconciliation and Bulk Load
- Common Services
- Workflow and Request Management
- Infrastructure and Middleware Integration
- Connector Framework

Identity Administration

Identity administration includes creation and management of identities in Oracle Identity Manager. Identities include users, organizations, and roles. Identity administration also enables password management and user Oracle Identity Manager Self Service operations. Identity administration is performed by using Oracle Identity Manager Administration and Oracle Identity Manager Self Service Web clients, and the SPML Web service.

> **Note:** The identity administration tasks include, managing users, managing roles, managing organizations and managing authorization policies, which are explained in detail in this guide.

Provisioning

The provisioning transactions are assembled and modified in the provisioning module. This module maintains the "who" and "what" of provisioning. User profiles, access policies, and resources are defined in the provisioning module, as are business process workflows and business rules.

The Provisioning Server is the run-time engine for Oracle Identity Manager. It runs the provisioning process transactions as defined through Oracle Identity Manager Administration and Oracle Identity Manager Design Console and maintained within the provisioning module.

Audit and Reports

The audit and compliance functions include evaluating a person, organization, system, process, project, or product. This occurs by capturing data generated by the suite's workflow, policy, and reconciliation engines. By combining this data with identity data, an enterprise has all the information it requires to address any identity and to access a related audit inquiry. Audits are performed to ascertain the validity and reliability of information, and also provide an assessment of a system's internal control.

Reporting is the process of generating a formal document, which is created as a result of an audit. The report is subsequently provided to a user, such as an individual, a group of persons, a company, a government, or even the general public, as an assurance service so that the user can make decisions, based on the results of the audit. An enterprise can create reports on both the history and the current state of its provisioning environment. Some captured identity data includes user identity profile history, role membership history, user resource access, and fine-grained entitlement history.

Reconciliation and Bulk Load

The reconciliation engine ensures consistency between the provisioning environment of Oracle Identity Manager and Oracle Identity Manager managed resources within the organization. The reconciliation engine discovers illegal accounts created outside Oracle Identity Manager. The reconciliation engine also synchronizes business roles located inside and outside the provisioning system to ensure consistency.

> **See Also:**
>
> - "Reconciliation Configuration" on page 4-2 for detailed information about reconciliation
>
> - "Managing Reconciliation Events" for information about managing reconciliation events in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*

If you want to load a large amount of data from other repositories in your organization into Oracle Identity Manager, then you can use the Bulk Load utility. The Bulk Load utility reduces the downtime in loading the data. In addition, Bulk Load utility import Oracle Identity Manager users, roles, role memberships, and accounts provisioned to users.

> **See Also:** "Bulk Load Utility" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about Bulk Load utility

Common Services

Various services are grouped together that are shared and used by other Oracle Identity Manager components. These services are:

- **Form Designer:** A form that allows you to create process and resource object forms that do not come packaged with Oracle Identity Manager. See "Form Designer Form" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about the Form Designer.

- **Scheduler:** A service that provides the capability to run specific jobs at specific schedules. This service can be used by users, application developers, connector developer, and administrators to create and configure a Job to be run at specified intervals. In addition, this service provides administrative capabilities to manage the functionality of jobs and their schedules. See the "Managing Scheduled Tasks" chapter in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information.

- **Notification Templates:** A common notification service is used by other functional components to send notifications to interested parties about events occurring in Oracle Identity Manager. In addition, this service provides the administrative capabilities for notification template management. A notification template is used for sending the outgoing notifications. These templates typically contain the variables that refer to the available data to provide more contextual content. See the "Creating and Managing Notification Templates" chapter for more information.

- **System Properties:** A system property is an entity that controls the configuration aspect of an application. In addition, to the default system properties, you can create and manage system properties in Oracle Identity Manager. See the "Administering System Properties" chapter in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information.

- **Deployment Manager:** The Deployment Manager is a tool for exporting and importing Oracle Identity Manager configurations. The Deployment Manager enables you to export the objects that make up your Oracle Identity Manager configuration. See "Importing and Exporting Data Using the Deployment Manager" chapter in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information.

Workflow and Request Management

Various operations in Oracle Identity Manager cannot be performed directly. Instead, the operations must be requested. The request management service provides a mechanism to create, approve, and manage requests. A request is an entity created by the users or administrators who want to perform a specific action, which requires a discretionary permission to be obtained from someone or some process before the action can be performed. For example, a user can create a request to gain access to a laptop computer, a manager can approve the request and create an open requisition, and an IT resource administrator can approve the request.

The primary goal of a provisioning solution is to manage requests and provision resources. Request service provides an abstraction layer on the Business Process Execution Language (BPEL) 11*g* workflow engine. Functional components such as request, provisioning, and attestation interacts with the workflow engine for human approvals. Request service caters to the various functional components in Oracle Identity Manager by managing workflow instances and categories, and provides an abstraction layer on BPEL. For information about registering workflows with Oracle Identity Manager, see, *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Infrastructure and Middleware Integration

The Adapter Factory, Kernel Orchestration mechanism, Context Manager, and Plug-in Framework are designed to eliminate the need for hard-coding integrations with these systems.

For more information about the integration of Oracle Identity Manager with middleware applications, see "Integration Solutions" on page 1-5.

Connector Framework

A description of the Connector Framework is provided in the "Integration Services" on page 2-7.

3

Interfaces

Oracle Identity Manager provides user interfaces that you can use to perform various tasks. These are Oracle Identity Manager Administrative and User Console and Oracle Identity Manager Design Console. These interfaces are located in the Presentation or Client tier of Oracle Identity Manager. Oracle Identity Manager also provides the SPML Web Service interface that supports inbound provisioning requests.

This chapter introduces Oracle Identity Manager interfaces and briefly describes the functionality of each. This chapter also provides a brief introduction to the SPML Web Service. The chapter contains the following topics:

- Overview of Oracle Identity Manager Administrative and User Console
- Overview of Oracle Identity Manager Design Console
- SPML Web Service

3.1 Overview of Oracle Identity Manager Administrative and User Console

Oracle Identity Manager is an advanced, flexible provisioning system for automatically granting and revoking access to organization applications and managed systems. Oracle Identity Manager Administrative and User Console can provide the staff and partners of an organization with access to the organization's resources, and enforce access policies that are associated with these resources.

Oracle Identity Manager Administrative and User Console enables you to perform various functions, such as viewing user accounts, modifying profiles, viewing request status, and changing passwords. You can also customize Oracle Identity Manager Administrative and User Console, as explained at the end of this section.

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

Oracle Identity Manager Administrative and User Console consists of the following main areas:

- Unauthenticated User Self Service
- Authenticated User Self Service
- Oracle Identity Administration
- Oracle Identity Manager Advanced Administration

■ Localizing Interfaces

3.1.1 Unauthenticated User Self Service

Unauthenticated user self service or Oracle Identity Manager login page allows the unauthenticated user to perform self service operations. In other words, a user who is not logged in to Oracle Identity Manager can use the login page to perform Oracle Identity Manager Self Service operations such as self registering to Oracle Identity Manager, tracking the self registration request, logging in to Oracle Identity Manager, and retrieve a forgotten password.

3.1.1.1 Features of the Unauthenticated User Self Service

Use the unauthenticated user self service to perform the following functions:

■ **Self Registering to Oracle Identity Manager**

If you do not have an account in Oracle Identity Manager, you must create one by self registering to Oracle Identity Manager from the unauthenticated user self service. Depending on how your system is configured, you might need your manager to create an account for you.

■ **Tracking Self Registration Request**

You can track the self registration request with the help of the registration tracking ID that is generated when you submit the self registration request.

■ **Logging in to Oracle Identity Manager**

Log in to Oracle Identity Manager by using the login ID and password provided during registration. When you login to Oracle Identity Manager for the first time, you must provide answers to challenge questions that will be used to authenticate your account if you forget your password.

■ **Retrieving Forgotten Password**

If you forget your password, you can retrieve the forgotten password by correctly answering the challenge questions.

> **See Also:** Chapter 7, "Configuring and Using Self-Service Registration" for detailed information about the unauthenticated user self service interface

3.1.2 Authenticated User Self Service

When you login to Oracle Identity Manager Administrative and User Console, Oracle Identity Manager Self Service is displayed. Oracle Identity Manager Self Service allows the authenticated or logged in user to perform various self service operations. This section describes the features of Oracle Identity Manager Self Service.

3.1.2.1 Features of the Authenticated User Self Service

Use Oracle Identity Manager Self Service to perform the following:

■ **Managing Self Profile**

Using authenticated user self service, you can modify basic information associated with your Oracle Identity Manager user profile. Managing self profile includes updating user attributes for self, and requesting and removing roles and resources.

■ **Managing Proxies**

Authenticated user self service lets you delegate your task approval responsibilities to another user if you are unavailable because of illness or vacation.

■ **Password Management**

You can also change passwords at will, or from time to time depending on system requirements.

■ **Viewing and Resource Profile and Request Profile**

Authenticated user self service lets you view resources that have been provisioned to you. This Web client also lets you view all resource requests that you have submitted for yourself and those made by other users for you. You can also request provisioning of a new resource.

■ **Managing Tasks in the Tasklist**

The process for approving requests and their associated resources consists of multiple tasks, so as the process for making a request and resources available for provisioning. For a request, before resources can be provisioned to the target users, they must be approved. On the other hand, the tasks associated with the requests also require approval. Using the Oracle Identity Manager Self Service, you can complete tasks on which your approvals are pending, retry a task if it has a Rejected status, and manage open attestation tasks that are assigned to you.

> **See Also:** Part II, "Oracle Identity Manager Self Service" for detailed information about completing tasks using Oracle Identity Manager Self Service.

3.1.3 Oracle Identity Administration

Oracle Identity Administration enables you to perform identity management tasks such as creating and managing users, roles, and organizations. It also lets you define authorization policies to control the access of various components and features in Oracle Identity Manager.

3.1.3.1 Features of Oracle Identity Administration

Use Oracle Identity Administration to perform the following functions:

■ **Searching Records**

Many fields in Oracle Identity Manager have lookup capabilities. You use them when you want to locate a record. You can locate a record by constructing a search or query and then by running it. To do so, you must enter data in one or more fields to limit the records retrieved by your search. You can also use wildcard characters in addition to the data that you enter in the fields.

> **Note:** The manner in which the search is constructed and run depends on the type of search you perform. The results retrieved are based on the context in which you are conducting the search.

Oracle Identity Manager supports simple and advanced search. Simple search operation lets you search records based on the search strings that you specify as search attributes. This operation is also referred to as simple search or quick search. Advanced search operation presents a form, which allows you to specify more complex search criteria than the simple search operation.

- **Creating and Managing User Records**

  Using Oracle Identity Administration, you can create and manage user records.

- **Creating and Managing Organizations**

  Using Oracle Identity Administration, you can create and manage organization records. You can also enable, disable, revoke, and provision resources, organizations, and suborganizations.

- **Creating and Managing Roles**

  Using Oracle Identity Administration, you can define roles that represent logical groupings of users to whom you can assign access rights within Oracle Identity Manager, provision resources automatically, or use in common tasks such as approval and attestation. Roles can be independent of organizations, span multiple organizations, or can contain users from a single organization.

- **Creating and Managing Authorization Policies**

  Authorization policy management is centralized as an administrative feature. This is achieved by integrating Oracle Identity Manager with Oracle Entitlements Server (OES) as the authorization system, which secures the access control to the application. In addition, you can create context-sensitive authorization policies for various features in Oracle Identity Manager. Authorization policies control access to the application by the users to allow or prevent the users to perform various operations in the application.

3.1.4 Oracle Identity Manager Advanced Administration

Oracle Identity Manager Advanced Administration enables you to perform various administrative functions, such as creating and managing requests, reconciliation events, and policies.

3.1.4.1 Features of Oracle Identity Manager Advanced Administration

Use Oracle Identity Manager Advanced Administration to perform the following functions:

- **Administration features:**

  - **Creating and Managing Accounts**

    Using Advanced Administration, you can create, update, and delete managed accounts via requests or administrative direct management. This capability also allows you to assign and revoke roles, add and remove resources, add and remove proxies, and view the details of direct reports and the requests assigned to the user.

  - **Creating and Tracking Requests**

    Oracle Identity Manager enables you to create and manage requests for various tasks, such as provisioning resources and creating and managing users and roles, for yourself, other users, and organizations. Based on the privileges granted to you by Oracle Identity Manager, you might be able to use Advanced Administration to view requests for resources. In addition, you might be able to edit details or approve tasks within those requests. This is known as tracking requests.

  - **Generating Reports**

    Based on your requirement, you can use Advanced Administration to generate reports in BI Publisher, which is the reporting solution in Oracle

Identity Manager 11*g* Release 1 (11.1.1). The reports are classified based on functional areas, such as Access Policy Reports, Attestation Reports, Request and Approval Reports, and Password Policy Reports.

- **Event management features:**

  - **Managing Reconciliation Events**

    The reconciliation process involves generation of events to be applied to Oracle Identity Manager. These events reflect atomic changes in the target system, and contain the data that has changed, the type of change, along with other information. Advanced Administration allows you to manage the reconciliation events by querying the events stored, displaying event details, and performing the actions required to resolve event issues.

  - **Viewing Attestation Tasks and Processes**

    You can use Advanced Administration to view attestation reports assigned to you, and provide your attestation response to each individual item within the report.

    In Oracle Identity Manager, attestation is supported through the definition of scheduled attestation processes. It is implemented as a configurable business process in Oracle Identity Manager, and it creates an attestation task for a user. The user acts as a reviewer, and must complete this process to provide correct audit information.

- **Policy features:**

  - **Creating and Managing Access Policies**

    You can create and manage access policies that define how resources are to be automatically provisioned or deprovisioned for users based on business rules. The Access Policy Wizard in Advanced Administration helps you define an access policy for provisioning resources to users that are members of the roles to which the access policy is attached. The access policy can also specify the entitlements to be provisioned to the account created during provisioning. Advanced Administration also enables you to modify information in existing access policies.

  - **Creating and Managing Approval Policies**

    Approval policy is a configurable entity of request management that helps associate various request types with approval processes defined in the request service only for request and operation level approvals. It associates approval workflows to be loaded at request or operation levels for a request type. You can use Advanced Administration to create, modify, and delete approval policies.

  - **Creating and Managing Attestation Processes**

    Advanced Administration allows you to define new attestation processes, manage existing attestation processes, and start ad-hoc attestation processes. The Attestation Dashboard feature in Advanced Administration allows you to create, modify, disable, enable, run, and delete attestation processes.

- **Configuration features:**

  - **Configuring User Management**

    Oracle Identity Manager user management feature is configured and customized by using the configuration management feature. Configuration management helps customize the way in which the user records are displayed

in Oracle Identity Manager Administrative and User Console and configure the user entity operations and attributes. Based on the operations performed on an entity, a set of attributes is displayed to the user in Oracle Identity Manager Administration. You can use Advanced Administration to define user entity data structure and configure user management operations and operational attributes.

– **Managing Resources**

You can use the Resource Management feature of Advanced Administration to manage resource objects for an organization or an individual user. Managing resources includes the following activities:

– Search for a resource and view its details

– Manage Resource Administrator and Authorizer groups

– View and edit the workflow

– Define Resource audit objectives

– Define and manage IT Resources

– Define and manage scheduled tasks

– **Creating and Managing Request Templates**

Request templates allow you to control the attributes of the request by controlling the various capabilities in the UI. Every request type has a default template, which cannot be deleted or renamed. Name of the default template is same as the model name. Advanced Administration allows you to create and manage custom request templates to customize the request types based on requirement.

– **Creating and Managing Generic Connectors**

You can quickly and easily build a basic connector without advanced features and customized behavior by using generic connectivity technologies such as SPML and JDBC. You can use Advanced Administration to create and modify generic technology connectors, and to import and export connector XML files that contain definitions for all the objects that are part of the connector.

See Also: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about how to create and manage generic technology connectors

■ **System management features:**

– **Creating and Managing Scheduler Jobs**

In Oracle Identity Manager, it is often required to run jobs at specified times on a regular basis to manage various activities. A job is a task that can be scheduled to run at the specified interval. The scheduler feature enables you to schedule jobs that automatically run predefined scheduled tasks at the specified time. Advanced Administration allows you to create, modify, disable, enable, and delete jobs.

– **Creating and Managing Notification Templates**

A notification template is used to send notification e-mail messages to requesters, beneficiaries, or administrators about events occurring in Oracle Identity Manager. These templates contain variables that refer to available data to provide more context to the notifications. Using Advanced

Administration, you can create, modify, delete notification templates, and add or remove locales from notification templates.

– **Creating and Managing System Properties**

The system configuration service enables you to manage system properties used by Oracle Identity Manager. System properties define the characteristics that control the behavior of Oracle Identity Manager. You can define the administration and self-service functionalities of Oracle Identity Manager by using system properties. The system configuration service in Advanced Administration allows you to create, modify, delete, and search existing system properties depending on their roles.

– **Using the Deployment Manager**

The Deployment Manager tool, accessed through Advanced Administration, helps you to export and import Oracle Identity Manager configurations. The Deployment Manager enables you to export the objects that form your Oracle Identity Manager configuration. Usually, you use the Deployment Manager to migrate a configuration from one deployment to another.

3.1.5 Customizing Oracle Identity Manager Administrative and User Console

You can customize the various aspects of Oracle Identity Manager Administrative and User Console. Oracle Identity Manager allows you to customize UI elements, such as branding information, menu options, and columns in search result tables, to be customized to meet the requirement of the organization.

You can customize the following components of Oracle Identity Manager Administrative and User Console:

- Branding information, such as branding text, logo image, and logo mouseover text
- Button labels
- Menus and Tabs
- Columns in search result tables
- Form templates
- Custom URLs
- Popup properties
- Colors, font, and alignment

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about how to customize the different components of Oracle Identity Manager Administrative and User Console

3.1.6 Localizing Interfaces

Localization is the process of rendering User Interface (UI) to the end user based on the locale setting. Oracle Identity Manager uses the locale setting in the following order:

1. Oracle Access Manager (OAM) protected environments - If OAM login screen provides a language selection option and the user selects a language, then it is provided the highest preference.

2. Oracle Identity Manager Self Service user profile provides selection of a language preference. If a locale is set in the user's profile, it is used to render Oracle Identity Manager UI. If the user does not make a preference to select the language, the next option is evaluated.

3. Browser locale, if there is an issue in retrieving this locale, then the next option is evaluated.

4. Server locale, the locale with which the server is installed.

3.2 Overview of Oracle Identity Manager Design Console

Oracle Identity Manager Design Console is mainly used to configure the system settings. These settings control the systemwide behavior of Oracle Identity Manager and affect its users. This section describes the basic features of Oracle Identity Manager Design Console.

3.2.1 Features of Oracle Identity Manager Design Console

The following features of Oracle Identity Manager Design Console let you perform different tasks:

- **Field Types**

  The behavior of the basic features of Oracle Identity Manager Design Console is standard for all forms to enable ease of use. You can view records that are displayed in the data fields. You can also search for values by using the lookup fields. For example, the Date & Time window enables you to select a date, month, year, and time.

  In addition, you can enter supplemental information about a record in the notes window. Oracle Identity Manager Design Console also lets you select and assign available entities to a record.

- **Search Functions**

  Using Oracle Identity Manager Design Console, you can perform searches for records in a database, also known as queries. Every form in Oracle Identity Manager Design Console provides a search function. You can filter the search criteria in a form field. This limits the results that are returned to only the records that match the criteria you entered.

  You can also use a wildcard in a search. The asterisk (*) wildcard character represents unspecified portions of the search criteria. For example, if you enter B* in the Location field of a Oracle Identity Manager Design Console form and execute a search, you retrieve all records with locations that begin with the letter B, for example, Burbank, Boston, Bristol, and so on.

  > **Note:** If multiple records in the database match your search criteria, then you can view details of each record.

- **User Management**

  Oracle Identity Manager Design Console lets you perform the following user management functions:

  – Define default values for certain process form parameters at the organizational level

- Display resources that are allowed or disallowed by policies for each user

- Define what forms and folders on Oracle Identity Manager Design Console are allowed for which roles

It also enables you to view, analyze, correct, link, and manage information in reconciliation events received from target resources and the trusted source.

- **Resource Management**

    You can manage resources in Oracle Identity Manager by using Oracle Identity Manager Design Console. The different tasks that you can perform in resource management are:

    - Create resource types that appear as lookup values on IT resources from.

    - Create rules that can be applied to password policy selection, auto-group membership, provisioning process selection, task assignment, and pre-populating adapters.

    - Create and manage resource objects.

- **Process Management**

    Process management includes creating and managing Oracle Identity Manager processes and templates for e-mail notifications.

    An Oracle Identity Manager process is the mechanism for representing a logical workflow for approvals or provisioning. Process definitions consist of tasks that you must perform to complete a process. Using Oracle Identity Manager Design Console, you can create and manage the provisioning processes that are associated with the resource objects.

    You can also create templates for e-mail notifications by using Oracle Identity Manager Design Console. These notifications can be set to be sent to the user:

    - When a task is assigned to the user

    - When the task achieves a particular status

    - On various attestation activities

    - During self-registration and self profile modification

- **Oracle Identity Manager Administration**

    Oracle Identity Manager Design Console provides you with tools to manage Oracle Identity Manager administrative features. You can perform various administrative tasks for Oracle Identity Manager by using these tools. Oracle Identity Manager Design Console also lets you create and manage lookup fields and their values, and user-defined fields.

    Using this console, you can specify the value of properties that control the behavior of the client and server. You can also display information about servers that Oracle Identity Manager uses to communicate with third-party programs. In addition, you can set up schedules for when tasks should be run.

- **Development Tools**

    Oracle Identity Manager Design Console contains a suite of development tools that enable you or developers to customize Oracle Identity Manager.

    You can create and manage the code that enables Oracle Identity Manager to communicate with any IT Resource by connecting to that resource's API. This code is known as an adapter. You can also compile multiple adapters simultaneously.

Oracle Identity Manager Design Console lets you create error messages that are displayed when certain problems occur. In addition, you can create and manage event handlers, data objects, and reconciliation rules that are used in Oracle Identity Manager.

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about the features and functions of Oracle Identity Manager Design Console

3.3 SPML Web Service

The SPML Web Service is an interface for inbound SPML-based provisioning requests. It supports the creation, modification, deletion, and lookup of Oracle Identity Manager users, organizations, and roles. It also provides features for managing references (such as assignment and revocation of role memberships), resetting user passwords, and disabling and re-enabling user accounts.

> **See Also:** "SPML Services" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for details about the SPML Web Service

4

Deployment Configurations

This chapter discusses the following deployment configurations of Oracle Identity Manager:

- Provisioning Configuration
- Reconciliation Configuration
- Integration Between LDAP Identity Store and Oracle Identity Manager

4.1 Provisioning Configuration

Provisioning is the process by which any action to create, modify, or delete a target system identity initiated in the provisioning system (Oracle Identity Manager) is communicated to the target system. Changes made to the identity triggers a set of provisioning actions. For deployments on which Oracle Identity Manager has the identities in its own repository, changes made to the identity attributes are detected and the provisioning actions are triggered accordingly.

You can use Oracle Identity Manager to create, maintain, and delete users on target systems. In this configuration, Oracle Identity Manager acts as the front-end entry point for managing all the user data on the target systems. After accounts are provisioned, the users for whom the accounts have been provisioned can access the target systems without any interaction with Oracle Identity Manager. This is the provisioning configuration of Oracle Identity Manager.

The purpose of provisioning is to automate the creation and maintenance of users on target systems. Provisioning is also used to accommodate any requirement for workflow approvals and auditing that can be a component of that provisioning life cycle. Figure 4–1 illustrates the working of the provisioning module.

Figure 4–1   Provisioning Configuration
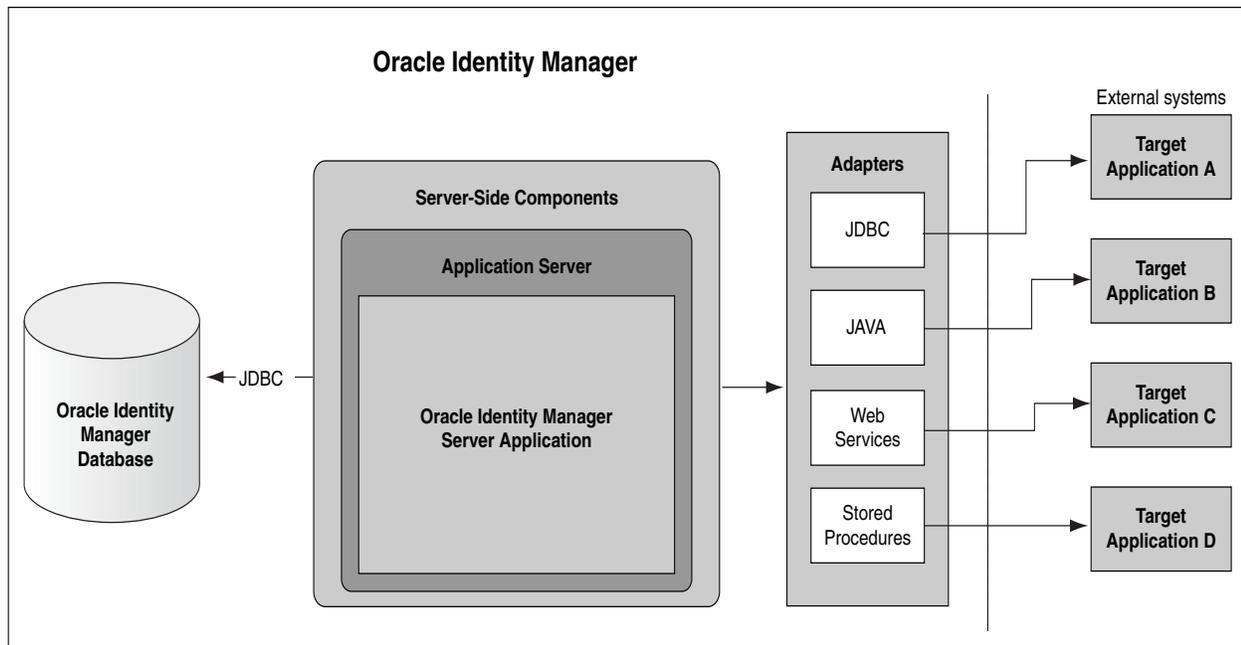
Provisioning events can be started through any of the following ways:

- **Request-based provisioning**

  A request can be manually created by an administrator or, in certain instances, by users themselves. Approval workflows are started after a request is submitted and provisioning of the approved account profile is started after the approval is completed.

- **Policy-based provisioning**

  This type of provisioning refers to the automation of target resources being granted to users through access policies. Access policies are used to define the association between roles and target resources. By default, each member of these roles gets a predefined account in the target resource.

- **Direct provisioning**

  This type of provisioning is a special administrator-only function. An authorized administrator can create an account. An account for a particular user can be created on a target system without having to wait for any approval processes.

4.2 Reconciliation Configuration

Reconciliation is the process by which operations, such as user creation, modification, or deletion, started on the target system are communicated to Oracle Identity Manager. The reconciliation process compares the entries in Oracle Identity Manager repository and the target system repository, determines the difference between the two repositories, and applies the latest changes to Oracle Identity Manager repository.

Reconciliation of roles, role memberships, and role hierarchy changes are handled as separate reconciliation events. Ideally role events must be submitted first and then only the membership events in order to avoid race conditions. For race conditions, the automatic retry logic allows the reconciliation engine to handle it. More details in race

condition section. For information about roles, role memberships, and role hierarchies, see "Managing Roles" on page 12-1.

> **See Also:** "Handling of Race Conditions" for information about race conditions in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*

Figure 4–2 shows that provisioning and reconciliation involve synchronization from Oracle Identity Manager to the target system or from the target system to Oracle Identity Manager. Provisioning and reconciliation enable the provisioning system to build the managed identities in the target system as well as replicate the managed identities as they already exist in the target system.

Figure 4–2   Provisioning and Reconciliation
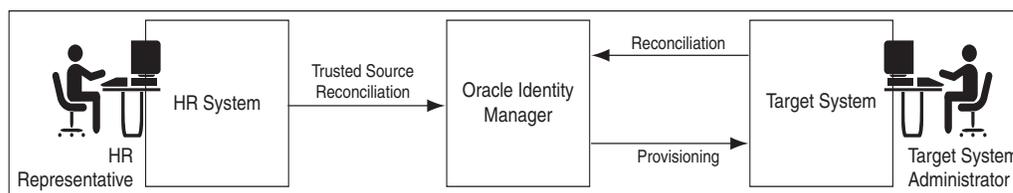
In Figure 4–2, a user is created by the HR representative when a new employee joins. The user is reconciled to Oracle Identity Manager by trusted source reconciliation. When the user is created in Oracle Identity Manager, the account for the user is provisioned in the target system. In the target system, the target system administrator can make changes in the account, which must be reconciled to Oracle Identity Manager.

In terms of data flow, provisioning provides the outward flow from the provisioning system by using a push model, in which the provisioning system indicates the changes to be made to the target system. Reconciliation provides the inward flow into the provisioning system by using either a push or a pull model, by which the provisioning system finds out about any activity on the target system.

The reconciliation process involves generation of events to be applied to Oracle Identity Manager. These events reflect atomic changes in the target system, and contain the data that has changed, the type of change, along with other information. The reconciliation events that are generated consequently because of changes occurring in the target system are managed by using the Reconciliation Event Manager in Oracle Identity Manager Administration console, which addresses these event management needs.

> **See Also:** "Managing Reconciliation" for information about managing reconciliation events by using Oracle Identity Manager Administration console in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*

This section consists of the following topics:

- Types of Reconciliation
- Reconciliation Architecture
- Integration Between LDAP Identity Store and Oracle Identity Manager

4.2.1 Types of Reconciliation

Reconciliation can be of different types, as shown in Table 4–1:

Table 4–1   Types of Reconciliation

Classification Criteria	Reconciliation Type
Object being reconciled	Based on identity being reconciled, such as user, account, role, or relationship that includes role hierarchy and role membership
	Note: Oracle Identity Manager does not support reconciliation of organizations.
Mode of reconciliation	Changelog
	Regular
Approach used for reconciliation	Incremental reconciliation
	Full reconciliation

This section describes the following topics:

- Reconciliation Based on the Object Being Reconciled
- Mode of Reconciliation
- Approach Used for Reconciliation

4.2.1.1 Reconciliation Based on the Object Being Reconciled

Reconciliation depends on the entity object that is being reconciled. The following entities in Oracle Identity Manager are reconciled:

- **User:** A user is an identity that exists within and is managed through Oracle Identity Manager.

- **Account:** An account is granted to a user to give the user the ability to log in to Oracle Identity Manager and access Oracle Identity Manager features. At the minimum, these features involve self-service and request. An account can be granted additional privileges including the ability to define workflows and the delegated administration of various entities, such as users, organizations, and roles.

- **Role:** A Role is a logical grouping of users to whom you can assign access rights within Oracle Identity Manager, provision resources automatically, or use in common tasks such as approval and attestation.

- **Role hierarchy:**

- **Role membership:**

This section discusses the following topics:

- Trusted Source Reconciliation
- Account Reconciliation
- Reconciliation Process Flow

4.2.1.1.1   Trusted Source Reconciliation

If data is reconciled from a system that drives the *creation* of users, roles, role memberships, or role hierarchies in Oracle Identity Manager repository, then that reconciliation mode is called identity reconciliation, or authoritative source

reconciliation, or trusted source reconciliation. The system that is being reconciled from is referred to as the authoritative source for the enterprise identities, and may be an HR system or a corporate directory.

> **Note:**
>
> ■ By default, users reconciled into Oracle Identity Manager are created with the same passwords as the user login. Make sure to create your own event handler to generate reconciliation passwords that conform to Oracle Identity Manager password policy. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about event handlers. In addition, you can refer to the sample event handler in Oracle Technology Network (OTN) Web site by using the following URL:
>
> `http://www.oracle.com/technetwork/index.html`

As shown in Figure 4–3, the authoritative sources of identity may be more than one. The different authoritative sources may be the source of reconciliation for different categories of user identities or may be the source of reconciliation for different sets of attributes. The various events generated by the reconciliation engine are add, modify, and delete.

Figure 4–3 Trusted Source Reconciliation from Single and Multiple Authoritative Sources
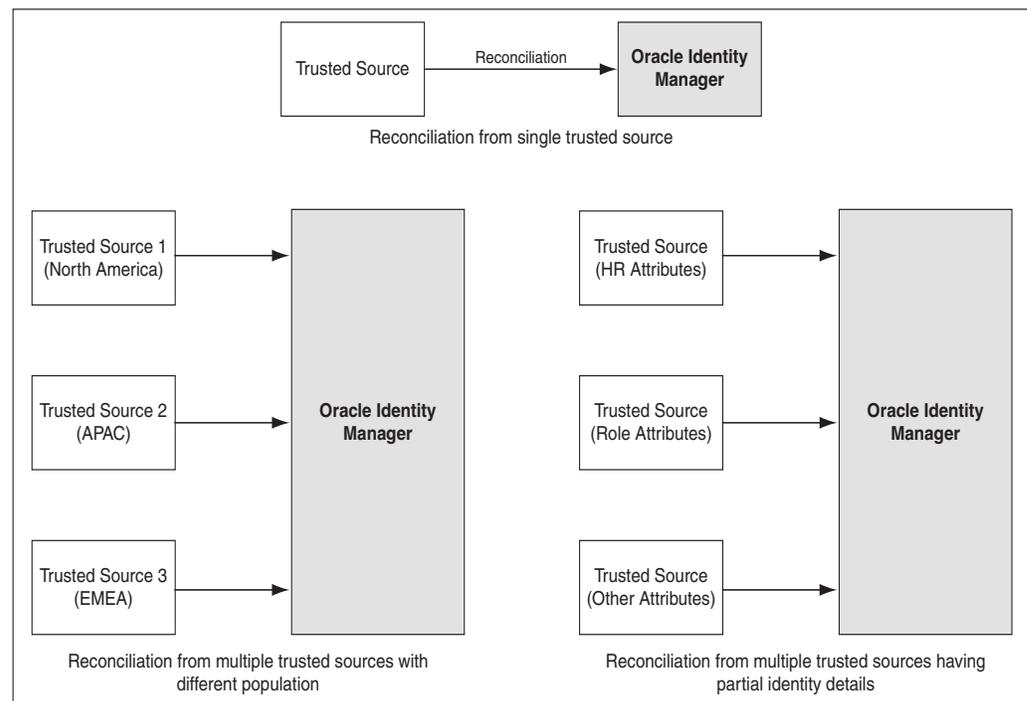
In Figure 4–3, trusted source reconciliation from a single authoritative source and multiple authoritative sources are shown. Creation of user entities can be reconciled from multiple authoritative sources. In addition, different attributes can be reconciled from different multiple authoritative sources. For example, the user ID and e-mail ID can be provided by an authoritative source and role attributes can be provided by another authoritative source.

Trusted source reconciliation must be followed by account reconciliation when the target system is the source for identities as well as accounts. For instance, if Active Directory is the corporate LDAP repository in which user information is stored, then the user information is reconciled from the Active Directory target system. Subsequently, the Active Directory accounts are reconciled into Oracle Identity Manager by using a different connector. Identity reconciliation occurs only from trusted sources, by using connectors specific to those trusted sources.

> **Note:** A reconciliation connector is a component developed to reconcile identities or accounts from a specific target system. Typically, a reconciliation connector is configured to be run as a scheduled task. However, there are push-based connectors, such as the PeopleSoft HR connector, for which there is no scheduled task to trigger the reconciliation.

4.2.1.1.2 Account Reconciliation If the target system identities are accounts that get reconciled to Oracle Identity Manager, then that is target resource reconciliation or account reconciliation. This type of reconciliation is to reconcile a specific resource object that represents the target system being managed. There is always a corresponding provisioning flow for it. The identity retrieved from the target system maps to a resource object instance that has been provisioned to a user or organization.

Account reconciliation takes place in the following scenarios:

Scenario I

Identity gets created in Oracle Identity Manager from an authoritative source. The identities are provisioned with resources on the target system. Any change on the target system is reconciled with Oracle Identity Manager. Figure 4–4 shows account reconciliation from a target system:

Figure 4–4   Account Reconciliation From a Target System
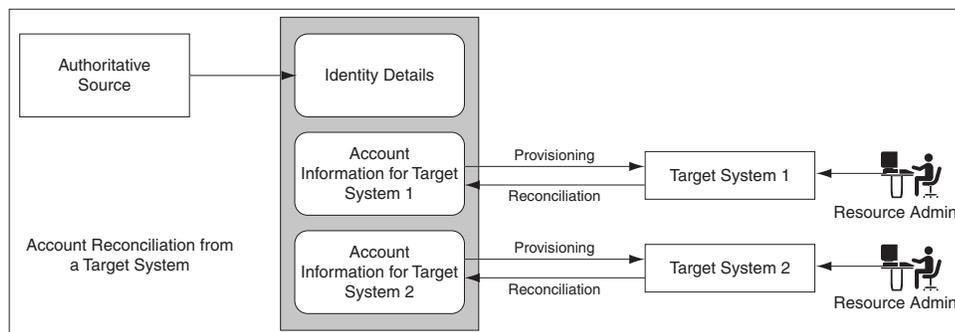
Scenario II

In this scenario, the target system initially plays the role of an authoritative source. Later it plays the role of a regular provisioning target. Following are the sequence of steps:

1. Identities are created in Oracle Identity Manager based on the target system entity details. Corresponding accounts are also created for these entities.

2. The entities are updated as provisioned entities in the target system.

3. The resource administrator at the target system makes changes to the accounts.

4. The changes made on the target system are reconciled with Oracle Identity Manager.

Figure 4–5 shows identity reconciliation followed by account reconciliation:

Figure 4–5   Identity and Account Reconciliation
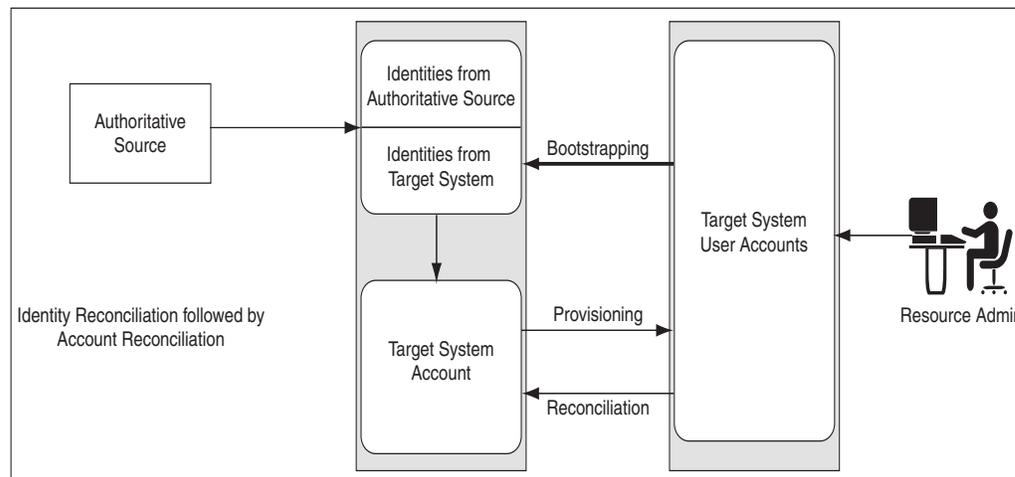
> **Note:**   When the value of the XL.UserProfileAuditDataCollection property is set to an audit data collection level, then the account reconciliation performs the matching in the database layer at a batch-level and performs the event action by using the provisioning APIs. This in turn triggers the audit event handlers for account reconciliation. By default, the value of this property is set to Resource Form. See "Administering System Properties" for information about system properties in Oracle Identity Manager in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

4.2.1.1.3   Reconciliation Process Flow   The reconciliation process flow is shown in Figure 4–6:

Figure 4–6   Reconciliation Process Flow
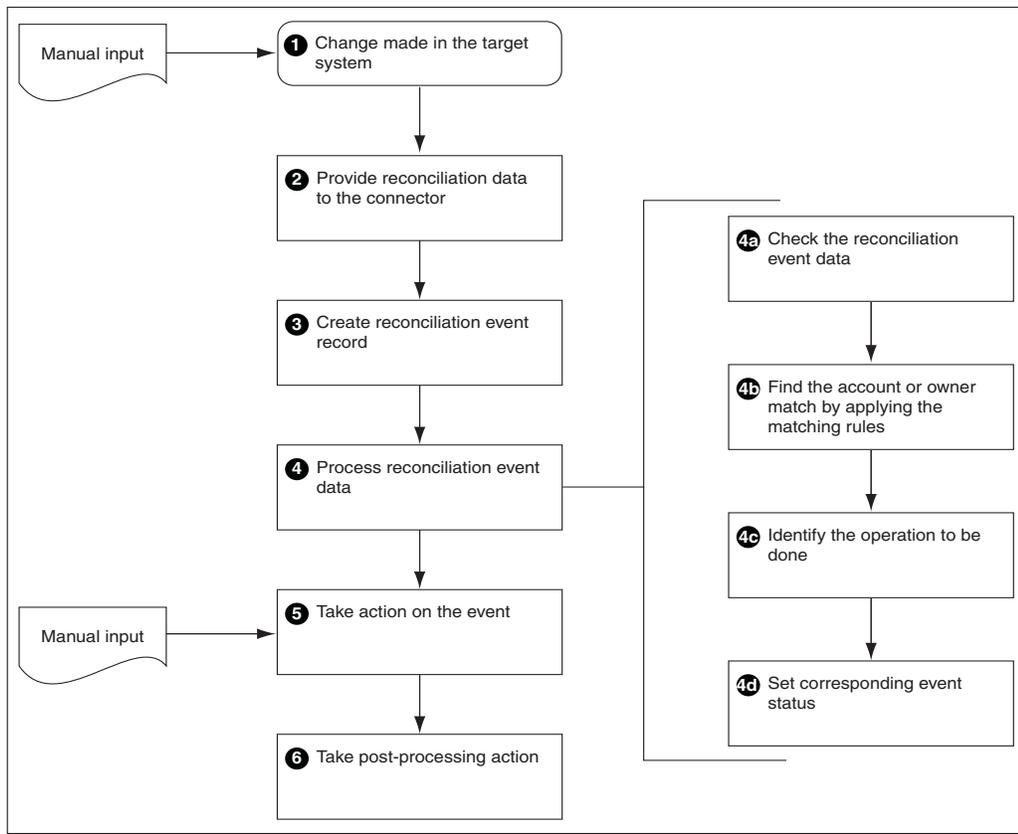
Reconciliation process involves the following steps:

1. **Changes in the target system:** The various activities that can happen in the target system are creation, modification, or deletion of user, account, role, role membership, or role hierarchy.

> **Note:** If you create an entity on an external system and then modify it a short time later, reconciliation processes the create entity step, but the modify entity step fails with the Creation Failed event status. This is because reconciliation cannot process a create and a modify action for the same entity in the same batch process.
>
> However, the entity modification action can be resubmitted for reconciliation at a later time by one of the following built-in mechanisms:
>
> - The "Automated Retry of Failed Async Task" scheduled task will run to re-process the failed events without any manual intervention. See "Automated Retry Error Handling Mechanism" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for details.
>
> - The failed event will be re-processed if the "Manual Retry Error Handling Mechanism" is triggered. See "Manual Retry Error Handling Mechanism" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for details.
>
> Reconciliation failure messages that are caused by processing conflicts within the same batch process should be regarded as transitory failures only.

2. **Providing reconciliation data:** When the creation, modification, or deletion event occurs, data about that event is sent to the reconciliation service by using reconciliation APIs.

> **Note:** Reconciliation service refers to the collection of reconciliation engine, reconciliation APIs, and the associated metadata and schema.

3. **Creation of reconciliation event record:** When the data for a reconciliation event is provided to reconciliation service, a record of that event is stored in Oracle Identity Manager repository.

4. **Processing of the reconciliation event data:** The data received is then evaluated to determine the actual operation to be performed in Oracle Identity Manager based on the changes in the target system. The evaluation involves application of a specific set of rules that help in:

   a. Identifying whether the data is for an account or for an identity that Oracle Identity Manager already has a record of

   b. Identifying the owner of the account or identity that the data represents

   c. Defining the context-sensitive action to be taken

   d. Setting the status of the event at the end of evaluation and the action that the reconciliation engine must take

5. **Taking action on the event:** Based on the evaluation result of processing the reconciliation event data, the intended action is taken. The various actions can be:

   - Creating a new account and associating with proper owner identity

   - Updating the matched account

   - Deleting the matched account

- Creating a new user in Oracle Identity Manager

- Modifying an existing user in Oracle Identity Manager

- Deleting an existing user

- Enabling and disabling account status by updating the status attribute

- Enable or disable user

- Create, update, or delete role

- Create or delete role membership

- Create or delete role hierarchy

   See Also: "Reconciliation Engine" on page 4-15 for information about role membership and role hierarchy

6. **Follow up actions triggered by the reconciliation event:** After the action is taken, follow up tasks can be started based on the reconciliation event. An example of follow up tasks or post-processing task is creating a request to provision a resource, such as a laptop computer, after a user creation event.

4.2.1.2 Mode of Reconciliation

The mode of reconciliation is either pull or push that depends on the connector used. Most connectors, such as Active Directory, uses the pull model. For the pull model, a pull reconciliation task is scheduled in the IAM Scheduler. The task runs at recurring intervals.

   See Also: "Managing Scheduled Tasks" for information about the IAM Scheduler in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*

Typically, the pull-based reconciliation connectors submit the reconciliation events within a scheduled task. Every time the scheduled task runs, a new reconciliation run is triggered and the reconciliation events are created in batches. When the batch size is met, the batch is submitted for processing. At the end of the scheduled task, an end of job listener is triggered, which submits all the batches whose size is not met.

Other reconciliation connectors, such as the PeopleSoft connector, uses a push model. The connector comprises of an HTTP listener that detects any asynchronous messages issued by PeopleSoft. On receiving a message, the listener submits reconciliation events by calling the reconciliation API. The events are processed by the reconciliation engine in batches when the batch size is met. For batches where batch size is not met, a scheduled task runs periodically and submits the batches for reconciliation processing.

Pull or push model is used based on the nature of the target system and how the changes can be detected in the target system. But irrespective of the push or pull model being used, reconciliation is performed by using a scheduled task that runs in the IAM Scheduler.

   Note: You can also create the reconciliation events directly by using the reconciliation APIs.

Changelog reconciliation is the default reconciliation mode. In this mode, only changed attributes are reconciled. Unspecified fields are ignored. You typically use the Changelog reconciliation mode when a connector is aware of the list of changed

attributes. Along with the changed attributes, Oracle Identity Manager needs a list of required fields for matching. The Changelog reconciliation mode was supported in previous Oracle Identity Manager releases, so all connectors work in this mode.

Regular reconciliation is a new reconciliation mode, introduced in this release, where the reconciliation engine completely replaces the existing snapshot of the entity. You typically use this reconciliation mode when the connector cannot determine which attributes have changed, and therefore, sends an entire snapshot of the entity. For new connectors, you can specify this mode when performing a full reconciliation. Using regular reconciliation mode results in better performance because the events are processed faster.

> **Note:** The mode of reconciliation depends on the connector implementation. For information about connector implementation, see "Connector for Reconciliation" on page 4-19.

Table 4–2 lists the differences between regular and changelog reconciliation modes:

Table 4–2   Regular and Changelog Reconciliation Modes

Regular	Changelog
Must pass a full set of mapped attributes	Must pass a subset of mapped attributes that are required by the specific profile and used by matching a rule
Performs better in batch processing mode (no difference in performance while in single event processing mode)	
Creates and updates all fields	Creates and updates only specified fields, and all other fields remain unchanged

> **See Also:** "Changing the Profile Mode" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for information about changing the reconciliation mode

4.2.1.3 Approach Used for Reconciliation

When you run reconciliation for the first time on a target system, all users and accounts on the target system are reconciled into Oracle Identity Manager by default. This is called full reconciliation. To perform full reconciliation, the connector sends the reconciliation events for each entity in the target system. The reconciliation engine processes the events as create or update events depending on whether or not the entity already exists in Oracle Identity Manager. The connector also identifies all the deleted entries and sends the deletion events to Oracle Identity Manager.

At the end of full reconciliation, the connector typically sets the last execution time parameter to the time when the reconciliation run ends. For the next reconciliation run, only the entity records that have been added, modified, or deleted after the first reconciliation run ended are fetched for reconciliation. This is called incremental reconciliation.

You can manually switch from incremental reconciliation to full reconciliation by setting the value of the timestamp IT resource parameter to 0.

4.2.2 Reconciliation Architecture

Reconciliation is the process of pulling entity data from the target system into Oracle Identity Manager to keep the entity data in a consistent state between the two systems. The various components of Oracle Identity Manager involved in reconciliation and the interaction between these components are shown in the Figure 4–7:

Figure 4–7   Reconciliation Architecture
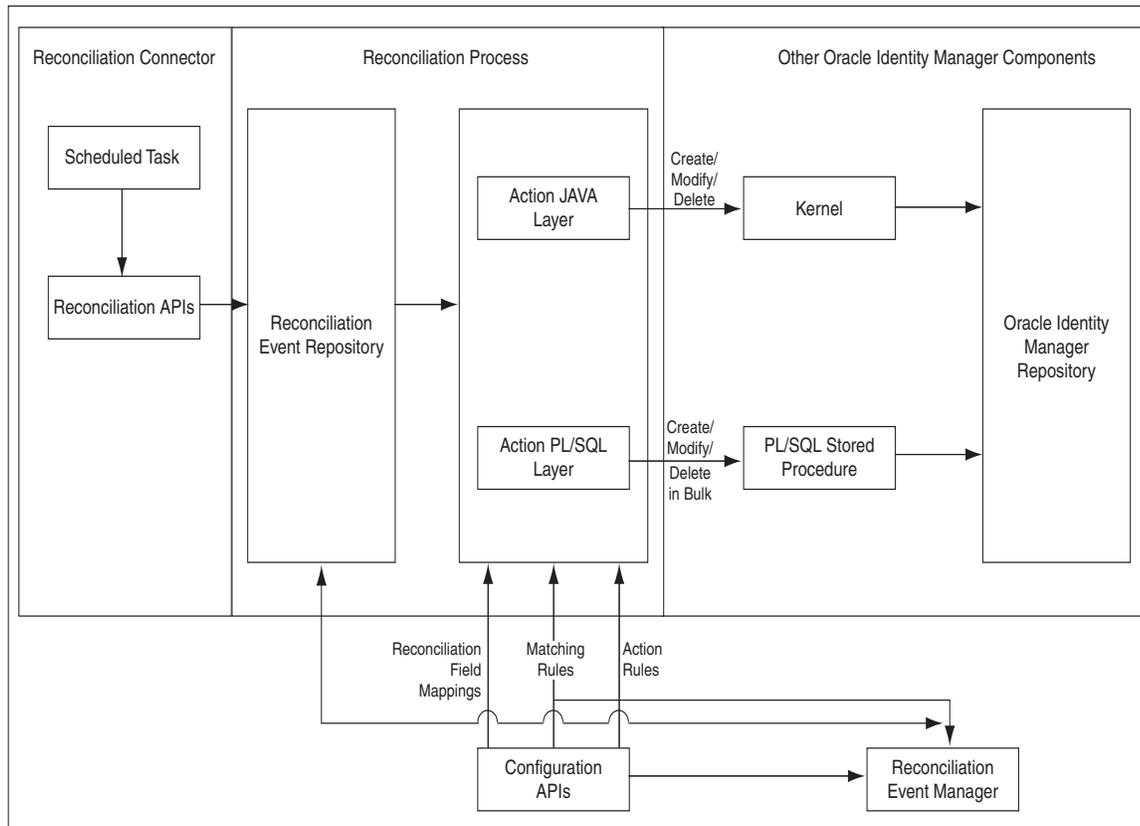
The reconciliation architecture is described in the following steps:

1. Each connector has scheduled tasks associated with it. The scheduler triggers the connector scheduled task, which invokes reconciliation APIs to generate events. The event can be of type Regular, Changelog, or Delete. For more information about the scheduler, see "Managing Scheduled Tasks" for information about the Scheduler in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*. For more information about scheduled tasks, see "Connector for Reconciliation" on page 4-19.

2. The reconciliation events are stored in the reconciliation event repository, which is Oracle Identity Manager database.

3. When batch size is met, an asynchronous message is submitted which processes the batch of events in bulk. At the end of the schedule task another asynchronous message is submitted for processing the events of the last batch. For information about the matching module, see "Matching Module" on page 4-16.

> **Note:**
>
> - In Figure 4–7, the reconciliation engine encapsulates the Action JAVA Layer as well as parts of the Reconciliation Event Repository, and orchestrates all the arrows in that diagram.
>
> - In 11*g* Release 1 (11.1.1) architecture, audit is a postprocessing task. For bulk reconciliation processing, audit is triggered for trusted reconciliation but not for account reconciliation. If you want audit to be enabled for account reconciliation, then you must enable the accountPostProcessingRequiredFlag property in the reconciliation profile. If this property is enabled, then the matching takes place in batches but the event processing occurs one event at a time by using the 9.1 account processing functionality, which also triggers the audit. See "Reconciliation Profile" on page 4-14 for information about reconciliation profiles.
>
> - In this release, trusted source reconciliation is supported for users only. It is not supported for roles, role membership, and role hierarchy reconciliation.

4. The processing involves data validation, matching of the entities and action (create, update, delete and so on). This is followed by post processing via kernel orchestrations. For information about the action module, see "Action Module" on page 4-17. For information about the reconciliation profile, see "New Metadata Model-Profile" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.*

5. By default the reconciliation event processing happens in bulk, and therefore all the steps till post processing are performed by PL/SQL stored procedures. Event can be processed one at a time in the following scenarios (in this case all the steps till matching are done in PL/SQL and the action is performed in java layer):

   - When events are processed from the Reconciliation Management console

   - When failed events are retried by the retry scheduled task that runs periodically

   For reconciliation single event processing, actions and post processing take place through the kernel.

6. Reconciliation events are made available to the Reconciliation Management console by another API call in the reconciliation management service.

The functionality of various components of the reconciliation service are explained in the following sections:

- Reconciliation Profile
- Reconciliation Metadata
- Reconciliation Target
- Reconciliation Run
- Reconciliation APIs
- Reconciliation Schema
- Reconciliation Engine
- Connector for Reconciliation

- [Archival](#)
- [Backward Compatibility](#)
- [Reconciliation Manager](#)

4.2.2.1 Reconciliation Profile

A reconciliation profile is the configuration defined to govern how reconciliation is run for a particular resource. A particular resource can have multiple reconciliation profiles, each of which defines matching rules, action rules, and field mappings, which can differ in each profile corresponding to the resource. For example, while one reconciliation run can perform reconciliation of new and modified accounts, another reconciliation run can reconcile deletion of accounts because you might want to run the deletions only once a day. In this example, you define two reconciliation runs and two profiles. Each profile is associated with respective reconciliation run and each profile having its own rules of reconciliation.

The profile is an XML-based configuration file stored in Oracle Identity Manager MetaData Store (MDS).

There is always a default profile associated with reconciliation configurations for any resource object. The default profile can be explicitly generated from Oracle Identity Manager Design Console in the developer's environment or implicitly generated during import from the Deployment Manager. For details on how to create and update profiles, see "Managing Reconciliation Events" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.*

4.2.2.2 Reconciliation Metadata

The reconciliation metadata consists of various configurations used in creating and processing the reconciliation events. The reconciliation metadata is stored in a logical container called a profile. For information about reconciliation profile, see "Reconciliation Profile" on page 4-14.

Examples of the reconciliation metadata are:

- **Mapping rules:** Used to map the data received from the target system to the data managed about that target system in Oracle Identity Manager.

- **Matching rules:** Used during the processing of each reconciliation event to correlate the event data to a particular account, user, or role in Oracle Identity Manager.

- **Action Rules:** Used to specify the actions taken by Oracle Identity Manager based on the result of the processing of a reconciliation event.

- **List of target attributes:** Used to define the data attributes received from the target system via reconciliation. It is used in the mapping rules, and is configured by using Oracle Identity Manager Design Console.

The various configurations used in creating and processing the reconciliation events are managed by using Oracle Identity Manager Design Console, and for backward compatibility, is stored in the same Oracle Identity Manager tables as in Oracle Identity Manager release 9.1.0. In addition, the configurations are also stored in the reconciliation profile.

> **Note:** For reconciliation in Oracle Identity Manager, a metadata
> model is being used. See "Managing Reconciliation Events" in the
> *Oracle Fusion Middleware System Administrator's Guide for Oracle
> Identity Manager*.

4.2.2.3 Reconciliation Target

Reconciliation target refers to an instance of an application that acts as a source of
changes for Oracle Identity Manager. An example of reconciliation target is an HR
system, which acts as a source of identities for Oracle Identity Manager. A
reconciliation target can be a source of users or accounts.

4.2.2.4 Reconciliation Run

Reconciliation run refers to the combination of a reconciliation connector and
associated configurations which when run by the scheduled task, performs the
reconciliation based on the rules defined in the associated configurations. The
scheduler runs reconciliation periodically at fixed intervals. Reconciliation runs are
scheduled within Oracle Identity Manager scheduler to run at a specified frequency.
All events created during a reconciliation run are grouped together by a unique
reconciliation run ID.

4.2.2.5 Reconciliation APIs

These are a set of published APIs to provide reconciliation data to Oracle Identity
Manager in the form of reconciliation events. Connectors can use the APIs to push
data to the reconciliation event repository. Scheduled tasks can be setup to run the
APIs when reconciliation is to be run on a scheduled basis. The existing connectors do
not need to be changed because the existing APIs are supported.

4.2.2.6 Reconciliation Schema

The data that comes from the target system for reconciliation is stored in the
reconciliation schema. The data contains the changes to be reconciled with Oracle
Identity Manager.

Reconciliation schema refers to the set of schema tables to store the reconciliation data.
The reconciliation schema is redesigned for performance reasons and future
extensibility. See "Reconciliation Schema" on page 4-15 for more details.

4.2.2.7 Reconciliation Engine

The reconciliation engine uses all configurable components and includes the data
processor and rule evaluator that use these components to convert input data into a
list of action items. It also includes the components that determine whether or not the
actions can be automated based on the rule context. When an action is performed,
either automatically or manually, the engine performs the appropriate updates and
provisioning actions.

The main task of the reconciliation engine is to perform the comparison, determine the
action to be taken, and apply the action in Oracle Identity Manager. It contains two
modules, which are described in the following sections:

- Matching Module
- Action Module

4.2.2.7.1 Matching Module The matching rule specified in the profile is used to identify whether the record being searched, exists in Oracle Identity Manager or not. Matching rules are rules to identify whether the data is for an identity that Oracle Identity Manager already has a record of, or to identify the owner of the account in Oracle Identity Manager. When no record is found for the data of an account, an owner match is then performed to identify the owner of the account by using the matching rules.

For user and role entities owner matching is performed. For account entities, when no record is found, an owner match is then performed to identify the owner of the account.

For role membership events, matching is performed to identify role and user.

For role hierarchy events, matching is performed to identity the parent and child role.

At the end of the evaluation, the match table contains all the possible matches found within Oracle Identity Manager that meet the criteria for the event, and the state of the event is updated to one of the statuses listed in Table 4–3:

Table 4–3   Reconciliation Status Events

Status Events	Description
Data Received	Event data has been created in the database and is ready for further processing.
Event Received	A reconciliation event has been created and is ready for further processing. The finishReconciliationEvent API has not yet been called.
Data Validation Failed	The reconciliation event record is invalid. For example, a role event with an invalid role category will fail to validate. (This situation could indicate a race condition.) The RE_NOTE field should contain the details of the failure, which is also displayed in the user interface.
Data Validation Succeeded	The event data was successfully validated and the event can now safely be processed by the Engine.
Multiple Accounts Match Found	Given the current matching rules, multiple matching account records were found for the data.
No Account Match Found	Given the current matching rules, no matching account records were found for the data.
Single Account Match Found	Given the current matching rules, one matching account record was found for the data.
Multiple Org Matches Found	Given the current matching rules, multiple matching organization records were found for the data.
No Org Match Found	Given the current matching rules, no matching organization records were found for the data.
Single Org Match Found	Given the current matching rules, one matching organization record was found for the data.
Multiple Role Grants Match Found	Multiple matching records for user membership within a role were found.
No Role Grant Match Found	No matching records for user membership within a role were found.
Single Role Grant Match Found	One matching record for user membership within a role was found.
Multiple Roles Match Found	Given the current matching rules, multiple matching role records were found for the data.

Table 4–3   (Cont.) Reconciliation Status Events

Status Events	Description
No Role Match Found	Given the current matching rules, no matching role records were found for the data.
Single Role Match Found	Given the current matching rules, one matching role record was found for the data.
No Role Members Found	The Reconciliation Engine did not find role members matching the data, given the current matching rules.
No Role Parent Found	The Reconciliation Engine did not find a role matching the data, given the current matching rules.
Multiple Role Relationships Match Found	Given the current matching rules, reconciliation has found multiple role-to-role relationships that match data in the event.
No Role Relationship Match Found	Given the current matching rules, reconciliation did not find any role-to-role relationships that match data in the event.
Single Role Relationship Match Found	Given the current matching rules, reconciliation has found one role-to-role relationship that matches data in the event.
Multiple Users Match Found	Given the current matching rules, multiple matching user records were found for the data.
No User Match Found	Given the current matching rules, no matching user records were found for the data.
Single User Match Found	Given the current matching rules, one matching user record was found for the data.
Invalid Event Data Passed	The event contains invalid data. This status pertains to the e-mail attribute.
Being Re-evaluated	The reconciliation event is being reevaluated from the reconciliation management console.
Being Re-tried	The reconciliation event is being retried automatically. This status event has been deprecated.
Creation Failed	The user/account/role entity was not created successfully.
Creation Succeeded	The user/account/role entity was created successfully.
Delete Failed	The user/account/role entity was not successfully deleted.
Delete Succeeded	The user/account/role entity was deleted successfully.
Event Closed	The reconciliation event was closed from the reconciliation management console. The change is complete.
Update Failed	The user/account/role entity was not updated successfully.
Update Succeeded	The user/account/role entity was updated successfully.

4.2.2.7.2   Action Module This module applies the action based on the event state, entity type, and the action rules, as listed in Table 4–4:

Table 4–4   Action Rules

Event State	Entity Type	Action	Description
No User Match Found	User	No Action	Does not perform any action
		Create User	Creates a user in Oracle Identity Manager
No Account Match Found	Account	No Action	Does not perform any action

Table 4–4   (Cont.) Action Rules

Event State	Entity Type	Action	Description
User Matched	User or Account	No Action	Does not perform any action
	User	Establish Link	Modifies or deletes the matched user based on the change type
	Account	Establish Link	Owner identified - creates an account
Users Matched	User or Account	No Action	Does not perform any action
Account Matched	Account	No Action	Does not perform an action
		Establish Link	Modifies or revokes the account based on the change type
Accounts Matched		No Action	Does not perform any action
No Role Match Found	Role	No Action	Does not perform any action
Single Role Match Found	Role	No Action	Does not perform an action
		Establish Link	Modify or delete a role
	Role Membership	Create role membership	Grant a role member to Oracle Identity Manager
		Delete role membership	Delete a role member from Oracle Identity Manager
		No action	Does not perform an action
	Role Hierarchy	Create role hierarchy	Creates a role hierarchy in Oracle Identity Manager
		Delete role hierarchy	Delete a role hierarchy in Oracle Identity Manager
		No action	Does not perform an action
Multiple Roles Matched	Role, Role membership and Role Hierarchy	No action	Does not perform an action
No Role Grant Match Found	Role Membership	No Action	Does not perform an action
		Create Role Member	Creates a role member in Oracle Identity Manager
Single Role Grant Match Found	Role Membership	No action	Does not perform an action
		Establish Link	Delete role member
Multiple Role Grant Match Found	Role Membership	No action	Does not perform an action
			Note: This state does not occur because the role grant match is done by looking for the primary key, which is a combination of the usr key and the group key.
No Role Parent Match Found	Role Hierarchy	No Action	Does not perform an action
		Create role parent	Create a role parent in Oracle Identity Manager

Table 4–4   (Cont.) Action Rules

Event State	Entity Type	Action	Description
Single Role Parent Match Found	Role Hierarchy	No Action	Does not perform an action
		Establish Link	Delete role parent
Multiple Role Parent Match Found	Role Hierarchy	No Action	Does not perform an action
Data Validation Failed	Role, Role Hierarchy, Role Member	Race condition	Does not perform an action. The event needs to be re-evaluated.
Parent role not found	Role Hierarchy	Race condition	Does not perform an action. The event needs to be re-evaluated.
Role member not found	Role membership	Race condition	Does not perform an action. The event needs to be re-evaluated.

4.2.2.8 Connector for Reconciliation

The connector refers to the software that extracts the changes from the target system and creates events in the reconciliation schema by calling the reconciliation APIs. If the connector that you want to use is shipped with a predefined reconciliation module, then a scheduled task definition is available. You use this component to control the frequency at which the target system is polled for changes to track data and other connector-specific parameters.

The connector for reconciliation is deployed by using the Deployment Manager. When the connector is deployed, the corresponding reconciliation profile for that connector is created in the metadata store (MDS), and horizontal tables that store the event data are also created.

> **Note:**   Do not manually update reconciliation profile or update any reconciliation configurations from the Deployment Manager or Oracle Identity Manager Design Console when a reconciliation run is still in progress. This is because, if a reconciliation field is deleted or updated when a reconciliation run is in progress, then the event data might not be valid any more.

For information about configuring connectors, see Oracle Identity Manager Connector documentation.

> **See Also:**
>
> - "Reconciliation Metadata" on page 4-14 for information about MDS
>
> - "Horizontal Tables" for information about the horizontal tables in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.*

4.2.2.9 Archival

The Reconciliation Archival utility allows you to move processed events from the active reconciliation tables to archive tables. The events to move can be selected based on a time range. Only linked and closed events, which means successfully processed or closed by an administrator, can be archived.

> **See Also:** "Using the Reconciliation Archival Utility" for information about how to use the Reconciliation Archival utility in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.*

4.2.2.10 Backward Compatibility

You do not need to change the existing reconciliation configurations or scheduled tasks to leverage the new reconciliation service.

The existing configurations for reconciliation setup in earlier Oracle Identity Manager releases continues to function after upgrading to 11*g* Release 1 (11.1.1). As part of the upgrade, corresponding reconciliation event tables are created for each of the existing object types being reconciled.

4.2.2.11 Reconciliation Manager

The Reconciliation Manager is a Web-based UI, which is a part of Oracle Identity Manager Administrative and User Console. The Reconciliation Manager lets you view and manage reconciliation events generated by Oracle Identity Manager reconciliation engine. These events are generated through scheduled reconciliation runs. The Reconciliation Manager provides search capabilities on reconciliation runs as well as events. Users can use the Reconciliation Manager to perform reconciliation manually on generated events.

> **See Also:** "Managing Reconciliation Events" for more information about the Reconciliation Manager in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

4.3 Integration Between LDAP Identity Store and Oracle Identity Manager

Oracle Identity Manager users and roles are stored in Oracle Identity Manager database. However, when a user, role, or role membership change takes place in Oracle Identity Manager, this information is propagated to LDAP identity store. If user, role, or role membership change takes place in LDAP directly, then these changes are synchronized into Oracle Identity Manager. The synchronization involves:

- User creation, modification, deletion, change in enable or disable states, and password change are made in LDAP in addition to the internal Oracle Identity Manager tables.

- Role creation, modification, and deletion actions update the LDAP groups, including membership changes.

- Initial load of users, roles, and role memberships are synchronized.

- Direct changes to user profile in LDAP are reconciled to Oracle Identity Manager.

- Direct changes to roles and role memberships in LDAP are reconciled to Oracle Identity Manager.

When changes are made in the user and role data, the actual operation is performed with the help of the kernel handlers. These handlers go through an orchestration lifecycle of various stages, such as validation, preprocessing, action, and postprocessing. For more information about the various stages of kernel orchestration, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Oracle Identity Manager kernel orchestration connects to the Entity Manager, which in turn connects to the LDAP provider. The LDAP provider connects to Oracle Virtual Directory (OVD). The OVD is an interface to various directory systems, such as Oracle

Internet Directory, iPlanet, and Active Directory. The LDAP provider reaches the LDAP data by using OVD. Figure 4–8 shows the communication between Oracle Identity Manager and LDAP:

Figure 4–8   Oracle Identity Manager and LDAP
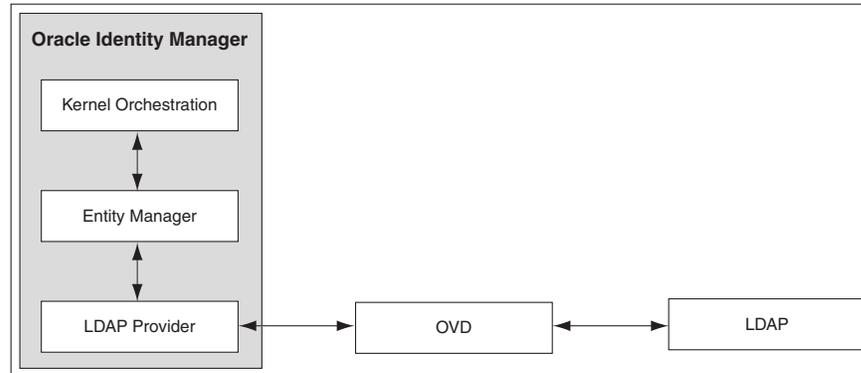
The integration configuration and synchronization of data between Oracle Identity Manager and the LDAP identity store are described in the following sections:

- Configuring the Integration with LDAP

- Provisioning Data From Oracle Identity Manager to LDAP Identity Store

- Reconciliation From LDAP Identity Store to Oracle Identity Manager

4.3.1 Configuring the Integration with LDAP

Configuring the integration between Oracle Identity Manager and LDAP is performed while installing Oracle Identity Manager. You can choose to install Oracle Identity Manager with or without LDAP. If you install Oracle Identity Manager with LDAP, then you must install OVD and Oracle Internet Directory, create a container to store reserved users, create a new user in Oracle Identity Manager to perform Oracle Identity Manager operations, and configure OVD and Oracle Internet Directory for Oracle Identity Manager. For information about how to perform these configuration steps, see "Setting Up LDAP Synchronization" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

After installing Oracle Identity Manager with LDAP enabled, you must open the following scheduled jobs and update their Last Change Number parameter with the last changelog number value of Oracle Internet Directory:

- LDAP User Create and Update Reconciliation

- LDAP User Delete Reconciliation

- LDAP Role Membership Reconciliation

- LDAP Role Hierarchy Reconciliation

- LDAP Role Create and Update Reconciliation

- LDAP Role Delete Reconciliation

In addition, you must enable these scheduled jobs after updating the Last Change Number parameter. To do so, see "Disabling and Enabling Jobs" in the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager..

> **See Also:** "Managing Scheduled Tasks" for detailed information about scheduled jobs in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

4.3.2 Provisioning Data From Oracle Identity Manager to LDAP Identity Store

Oracle Identity Manager database stores the user and role information. When the user and role information is updated in Oracle Identity Manager, then the external repositories, such as the LDAP directory, must also be updated.

The LDAP changes are performed before Oracle Identity Manager changes. If Oracle Identity Manager changes fail, then the LDAP changes must be reverted to the original state. This is achieved by correcting an enable operation with a disable operation, a create operation with a delete operation, and a modification operation with another modification operation with the original values.

For instance, when a user is created, the validation processes are performed in the validation stage, such as password or any other policy validation. In the preprocessing stage, the user is created in LDAP first. Then, in the action stage, the user is to be created in Oracle Identity Manager. If there is an error in creating the user in Oracle Identity Manager, then the user must be deleted from LDAP because the corresponding user could not be created in Oracle Identity Manager. The operation to revert the change made is provided by the kernel handlers through the compensation method, which is predefined in Oracle Identity Manager.

> **Note:** Each handler has predefined execute and compensate methods. The execute method runs any operation, such as creating a user. The compensate method is called when an error occurs to revert the operation performed by the execute method.

To synchronize date from Oracle Identity Manager to LDAP, the location of the LDAP must be known to Oracle Identity Manager. The information about the LDAP location is stored in Oracle Identity Manager as the DirectoryServer IT resource. This is a default IT resource provided by Oracle Identity Manager. The various parameters of this IT resource, which you can specify while installing Oracle Identity Manager, allows the connection between Oracle Identity Manager and LDAP.

In order to identify the same entry in Oracle Identity Manager and LDAP, the Distinguished Name (DN) and GUID attributes are used. Each entry has the DN attribute in LDAP, which indicates the unique location of an entry in LDAP. The GUID attribute is an unique ID to identify the entry. The DN and GUID for users and roles are stored in columns in the users and role tables in Oracle Identity Manager database. For information about how to synchronize user-defined fields between Oracle Identity Manager and LDAP, refer "Synchronizing User-Defined Fields Between Oracle Identity Manager and LDAP" in the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.

This section describes the following topics:

- Managing Users
- Managing Roles

4.3.2.1 Managing Users

The following user operations can be performed to synchronize data from Oracle Identity Manager to LDAP:

- Create user

- Update user

- Delete user

- Enable user

- Disable user

- Lock user

- Unlock user

- Add role member

- Delete role member

- Change password

4.3.2.2 Managing Roles

The following role operations can be performed to synchronize data from Oracle Identity Manager to LDAP:

- Create role

- Update role

- Delete role

- Add role to a member

- Add and Update role

- Remove role from a member

- Add role hierarchy

- Remove role hierarchy

4.3.3 Reconciliation From LDAP Identity Store to Oracle Identity Manager

When changes in the identities are made directly in the LDAP identity store, the changes must be replicated to Oracle Identity Manager through authoritative source reconciliation. The identities include users and roles.

Reconciling users from LDAP to Oracle Identity Manager works with the general configuration of reconciliation, which includes the scheduled tasks for reconciliation.

See Also:

- "Reconciliation Configuration" on page 4-2 for detailed information about reconciliation

- "Managing Scheduled Tasks" for information about scheduler and scheduled tasks in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

> **Note:** Instead of using LDAP synchronization reconciliation jobs to reconcile users from LDAP to Oracle Identity Manager, if the Bulk Load utility is used, then subsequent operation on these users might fail if LDAP synchronization is enabled. To avoid this, all the users that are loaded in Oracle Identity Manager must be updated with correct GUID and DN values, and all these users in LDAP must be updated with an object class called orclIDXPerson.
>
> For detailed information about the Bulk Load utility, see "Bulk Load Utility" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

The role reconciliation works only with the LDAP groups. Role reconciliation supports creation, updation, and deletion of roles. Role membership reconciliation supports creation and deletion of role memberships being driven from changes in an external LDAP directory.

> **See Also:** "Creating and Managing Roles" for information about roles, role memberships, and role hierarchies in the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.

Without roles and users being present in Oracle Identity Manager, role membership reconciliation will fail. Therefore, configure the LDAP synchronization scheduled jobs to run in the following order:

1. Fusion Applications Role Category Seeding

> **Note:** Fusion Applications Role Category Seeding is a predefined scheduled task that is generated only when LDAP synchronization is enabled, along with other LDAP synchronization scheduled jobs. This job gets all distinct business categories in LDAP and creates them as OIM role categories.
>
> For a list of the predefined scheduled jobs, see "Predefined Scheduled Tasks" in the Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager.

2. LDAP Role Create and Update Reconciliation

3. LDAP Role Hierarchy Reconciliation

4. LDAP User Create and Update Reconciliation

5. LDAP Role Membership Reconciliation

For each of these jobs, except Fusion Applications Role Category Seeding, there is a parallel job to do the full reconciliation. All these jobs, except Fusion Applications Role Category Seeding, perform the reconciliation based on change logs, whereas full reconciliation jobs use the search base to do the reconciliation.

5

Integration Solutions

Oracle Identity Manager has a three-tier integration solutions strategy to provide connectors to various heterogeneous identity-aware IT systems. This three-tier strategy is designed to minimize custom development, maximize the reuse of code, and reduce deployment time. The three tiers are:

- Out-of-the box integration using predefined connectors and predefined generic technology connector providers

- Connectors based on custom generic technology connector providers

- Custom connectors using the Adapter Factory

Figure 5–1 illustrates the three-tier integration solutions strategy of Oracle Identity Manager.

Figure 5–1 Three-Tier Integration Solutions Strategy of Oracle Identity Manager
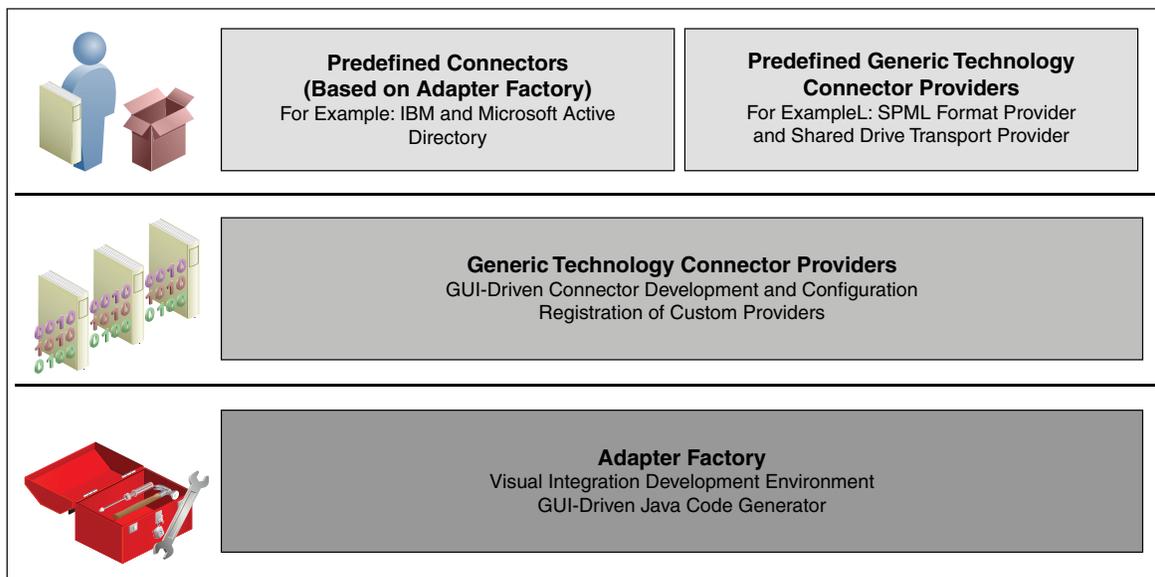
This chapter discusses the following topics:

- Predefined Connectors

- Generic Technology Connectors

- Custom Connectors

- Components Common to All Connectors

■   [Connector Installation](#)

5.1 Predefined Connectors

When a predefined connector is available for the target resource, this is the preferred integration method. Because a predefined connector is designed specifically for the target application, it offers the quickest integration method. These connectors support popular business applications such as Oracle eBusiness Suite, PeopleSoft, Siebel, JD Edward and SAP, as well as technology applications such as Active Directory, Java Directory Server, UNIX, databases, and RSA ClearTrust. Predefined connectors offer the quickest integration alternative because they are designed specifically for the target application. They use target recommended integration technologies and are preconfigured with application specific attributes.

> **See Also:**   ""Predefined Scheduled Tasks" for information about predefined connector installation in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

5.2 Generic Technology Connectors

Similar to a predefined connector, a generic technology connector acts as the bridge for reconciliation and provisioning operations between Oracle Identity Manager and a target system. In terms of functionality, a generic technology connector can be divided into a reconciliation module and provisioning module. When you create a generic technology connector, you can specify whether you want to include both modules or only the reconciliation or provisioning module.

The GTC framework provides basic components that are used to rapidly assemble a custom connector. The reconciliation and provisioning modules of a generic technology connector are composed of these reusable components that you select. Each component performs a specific function during provisioning or reconciliation. The components are:

■   Reconciliation:

–   Reconciliation Transport Provider: This provider is responsible for moving the reconciled data from the target system to Oracle Identity Manager.

–   Reconciliation Format Provider: This provider parses the message received from the target system, which contains the reconciled data, into a data structure that can be interpreted by the reconciliation engine in Oracle identity Manager.

–   Validation Provider: This provider validates any data received before passing it on to the reconciliation engine.

■   Provisioning:

–   Provisioning Format Provider: This provider converts Oracle identity Manager provisioning data into a format that is supported by the target system.

–   Provisioning Transport Provider: This provider carries the provisioning message received from the Provisioning Format Provider to the target system.

[Figure 5–2](#) shows the functional architecture of a generic technology connector.

Figure 5–2 Functional Architecture of a Generic Technology Connector
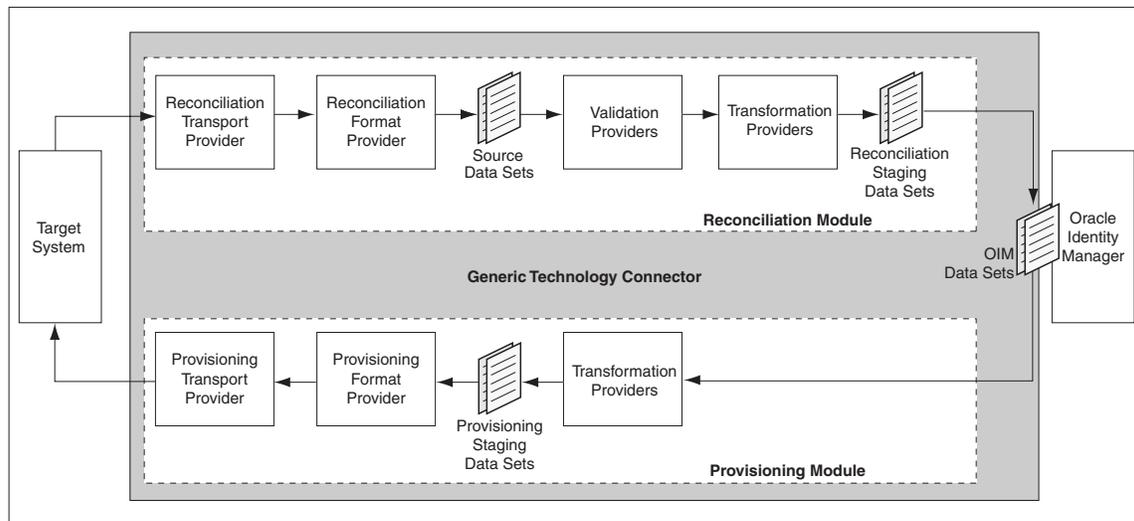
> **See Also:** "*Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*" for detailed information about the functional architecture, configuration, and functionalities of the generic technology connector

Generic technology connectors have the following features:

- Features specific to the reconciliation module are:

  - **Generic technology connector in trusted source reconciliation:** A generic technology connector can be used for trusted source reconciliation. During reconciliation in trusted mode, if the reconciliation engine detects new target system accounts, then it creates corresponding OIM Users. If the reconciliation engine detects changes to existing target system accounts, then the same changes are made in the corresponding OIM Users.

  - **Generic technology connector in account status reconciliation:** User account status information is used to track whether or not the owner of a target system account is to be allowed to access and use the account. If the target system does not store account status information in the format in which it is stored in Oracle Identity Manager, then you can use the predefined Translation Transformation Provider to implement account status reconciliation.

  - **Generic technology connector in full or incremental reconciliation:** While creating a generic technology connector, you can specify that you want to use the connector for full or incremental reconciliation. In incremental reconciliation, only target system records that have changed after the last reconciliation run are reconciled (stored) into Oracle Identity Manager. In full reconciliation, all the reconciliation records are extracted from the target system.

  - **Generic technology connector for batched reconciliation:** To exercise more control over the reconciliation process, you can use the generic technology connector to specify a batch size for reconciliation. By doing this, you can break into batches the total number of records that the reconciliation engine fetches from the target system during each reconciliation run.

  - **Generic technology connector in reconciliation of multivalued attribute data (child data) deletion:** You can specify whether or not you want to reconcile

into Oracle Identity Manager the deletion of multivalued attribute data on the target system.

– **Generic technology connector in failure threshold for stopping reconciliation:** During reconciliation, Validation Providers can be used to run checks on target system data before it is stored in Oracle Identity Manager. You can set a failure threshold to automatically stop a reconciliation run if the percentage of records that fail the validation checks to the total number of records processed exceeds the specified threshold percentage.

■ Other features of generic technology connectors are:

– **Custom Providers:** If the predefined providers shipped with Oracle Identity Manager do not address the transport, format change, validation, or transformation requirements of your operating environment, then you can create custom providers.

– **Multilanguage Support:** Generic technology connectors can handle both ASCII and non-ASCII user data.

– **Custom Date Formats:** While creating a generic technology connector, you can specify the format of date values in target system records that are extracted during reconciliation and the format in which date values must be sent to the target system during provisioning.

– **Propagation of Changes in OIM User Attributes to Target Systems:** While creating a generic technology connector, you can enable the automatic propagation of changes in OIM User attributes to the target system.

5.3 Custom Connectors

If the target resource has no technology interface or accessible user repository, then the customer can develop a custom connector. The Adapter Factory tool in Oracle Identity Manager Design Console provides a definitional user interface that facilitates such custom development efforts without coding or scripting.

> **See Also:** "Adapters" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for details about how to define adapters by using the Adapter Factory

5.4 Components Common to All Connectors

Table 5–1 lists the definitions of connector components contained in the connector XML file. These components are common to all connectors.

Table 5–1 Connector Components

Components	Description
Resource Object	This is a virtual representation of the target application on which you want to provision accounts. It is the parent record with which the provisioning process and process form are associated.
Provisioning Process	This process definition is used to create, maintain, and delete accounts on the target system. It consists of definitions of the individual tasks that are used to perform automated functions on the target system. Each connector is packaged with a single provisioning process. You can manually create additional provisioning processes. Note: For more information about provisioning process, see Table 5–2 and Table 5–3.

Table 5–1 (Cont.) Connector Components

Components	Description
Process Form	This form is used to provide information about user accounts to be created, updated, or deleted on the target system. This form is also used to capture data that can be used by provisioning process tasks or to provide a mechanism for users to provide real-time data.
	This form is used extensively when conducting reconciliation. The table structure associated with this form supports the archiving and auditing of user accounts on the target system.
	Each process form consists of field definitions required by a standard connector. If you require additional fields, then you can create another version of the form and add the required fields.
	Each connector is shipped with certain default process forms. You can manually create additional process forms.
IT Resource Type	This component is a template for all IT resource definitions associated with the connector. An IT resource type specifies the parameters that are common to all IT resource instances, such as host servers and computers, of that particular IT resource type.
	The parameters specified in this definition are inherited by all IT resource definitions of that type. For example, the Solaris 8 IT resource type can have a parameter called IP Address. The value of that parameter for the Target_Solaris IT resource instance can be set to 192.168.50.25.
Adapters	This includes all adapters that are required to perform common functions on the target application. Each adapter is predefined with certain mappings and functionality. These adapters are capable of interacting with the tasks in the provisioning process and the fields of the process form.
	Note: For more information about adapters, see *Oracle Identity Manager Tools Reference*.
Scheduled Task (where applicable)	If the connector that you want to use is shipped with a predefined reconciliation module, then you are provided with a scheduled task definition. You use this component to control the frequency at which the target system is polled for changes to tracked data.

5.4.1 Provisioning Process Tasks

Table 5–2 lists the predefined tasks (or their equivalents) that the Provisioning Process component contains.

Table 5–2   Provisioning Process Tasks

Provisioning Process Task	Purpose
Create User	Creates a new user account in the target application (provisions the user with an account)
Disable User	Temporarily disables a user account in the target application
Enable User	Re-enables a disabled user account in the target application
Delete User	Deletes a user account in the target application (revokes the user's account)
Update User	Modifies the privileges or profile of a user account in the target application

5.4.2 Reconciliation-Related Provisioning Process Tasks

In addition to the tasks listed in the previous section, the Provisioning Process component also contains the reconciliation-related tasks. Table 5–3 lists these tasks.

> **Note:** When Oracle Identity Manager receives a reconciliation event, all provisioning-related tasks within the provisioning process are suppressed and the relevant reconciliation-related task is inserted.

Table 5–3 Reconciliation-Related Provisioning Process Tasks

Provisioning Process Task (Reconciliation-Related)	Purpose
Reconciliation Insert Received	This task is inserted into the Provisioning Process instance associated with the user or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the creation of a user or organization account.
	In addition, the information in the reconciliation event record is stored in the process form according to the mappings set on the provisioning process.
Reconciliation Update Received	This task is inserted into the Provisioning Process instance associated with the user or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the update of an existing user or organization account.
	In addition, the information in the reconciliation event record is stored in the process form according to the mappings set on the provisioning process.
Reconciliation Delete Received	This task is inserted into the Provisioning Process instance associated with the user or organization when Oracle Identity Manager determines that the reconciliation event received from the target system represents the deletion of an existing user or organization account.

5.5 Connector Installation

Oracle Identity Manager provides features to install connectors. The following are general considerations that you must address before installing connectors:

- Some connectors require external libraries in the form of JAR files for normal functioning. You can purchase these JAR files from the respective vendors. After you obtain these JAR files, you must configure Oracle Identity Manager as required. For example, you can update the CLASSPATH environment variable.

- Some connectors require external software to be installed on the target system. For example, if you are using the Bourne (sh) shell on Solaris, then you must install and start WBEM Services on the target Solaris computer. Otherwise, you cannot use Oracle Identity Manager to provision users on Solaris.

- For optimal performance of the prepackaged connectors, you must configure the target systems separately. Where required, this step is explained in the connector deployment guides.

- While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, all the JAR files that you copy to Oracle Identity Manager server during the connector

deployment process must be copied to the corresponding directories on each node of the cluster.

6

Auditing

Oracle Identity Manager provides a powerful audit engine to collect extensive data for audit and compliance purposes. You can use the audit functionality together to capture, archive, and view entity and transactional data for compliance monitoring and IT-centric processes and forensic auditing. Therefore, with the audit and compliance modules, Oracle Identity Manager provides profile auditing, reporting, and attestation features. You can capture, transport, store, retrieve, and remove historical data over its life cycle. Security is maintained at every stage of the data life cycle. For information about attestation processes, see "Managing Attestation Processes" on page 19-1.

This chapter consists of the following topics:

- Overview
- Audit Engine
- User Profile Auditing
- Role Profile Auditing

6.1 Overview

This section provides an overview of auditing in the following sections:

- Auditing Design Components
- Profile Auditing
- Standard and Customized Reports

6.1.1 Auditing Design Components

Figure 6–1 shows the design components for Oracle Identity Manager auditing process.

Figure 6–1   Design Components of the Auditing Process
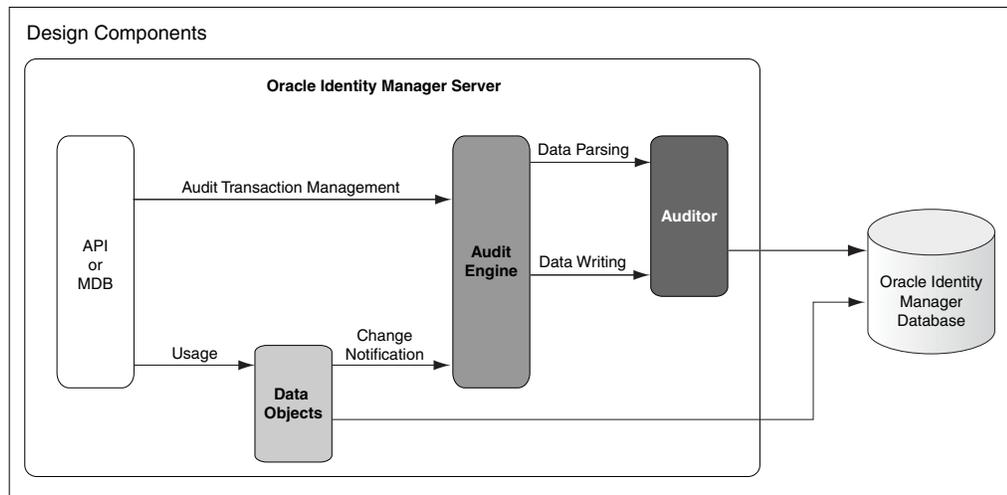
Any action that a user performs in Oracle Identity Manager translates into an Application Programming Interface (API) call or into a Message Driven Bean (MDB) picking up a message to process an action.

One action can cause multiple changes. All changes are combined into an audit transaction. Each API method that can modify data objects calls the startTransaction method in the audit engine at the beginning of the API call and the endTransaction method at the end of the API call. This defines boundaries for the audit transaction. The audit engine generates a transaction ID to identify the changes made in the transaction.

6.1.2 Profile Auditing

Oracle Identity Manager provides auditing and historical archiving of profile information. It takes a snapshot of a profile, stores the snapshot in an audit table in the database, and updates the snapshot each time the profile data changes. In the context of profile auditing, the term snapshot means a copy taken of the entire profile data at any instant when the data is modified.

6.1.3 Standard and Customized Reports

The BI Publisher provides standard reports for viewing archived data. You can also create customized reports.

For information about reporting, refer to the following:

- ""Using Reporting Features" on page 20-1"

- "Reporting" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about reporting

6.2 Audit Engine

User profile audits cover changes to user profile attributes, user membership, resource provisioning, access policies, and resource forms.

The audit engine collects auditing information in Oracle Identity Manager. Whenever a profile is modified, the audit engine captures the changes (the delta) and updates (or generates, if missing) the snapshots of the user and role profiles and stores these

snapshots and deltas in XML format. The audit engine also contains post-processors, which, based on the generated XML, populate the reporting tables with relevant data. To maintain high performance, by default the audit engine performs these tasks in an asynchronous and offline manner by using the underlying Java Messaging Service (JMS) provided by the application server.

This section discusses the following topics:

- Audit Levels
- Tables Used for Storing Information About Auditors
- Issuing Audit Messages

6.2.1 Audit Levels

As mentioned earlier in this chapter, When you install Oracle Identity Manager user profile auditing is enabled by default and the auditing level is set to Resource Form. If you change the auditing level, then you must run the GenerateSnapshot.sh script (on UNIX) or the GenerateSnapshot.bat script (on Microsoft Windows). This script is in the *IDM_HOME*/server/bin directory. The script examines all users in Oracle Identity Manager database and generates new snapshots based on the new auditing level.

> **Note:** If you change the auditing level, then you must run the GenerateSnapshot script before allowing users to access the system.

You can configure the "level of detail for auditing" aspect of the auditing engine and specify the audit level as the value of the XL.UserProfileAuditDataCollection system property in the Advanced Administration.

> **See Also:** "System Properties in Oracle Identity Manager" in the *Oracle Fusion Middleware System Administrators Guide for Oracle Identity Manager* for information about this system property

The supported audit levels are:

- **Process Task:** Audits the entire user profile snapshot together with the resource lifecycle process.
- **Resource Form:** Audits user record, role membership, resource provisioned, and any form data associated to the resource.
- **Resource:** Audits the user record, role membership, and resource provisioning.
- **Membership:** Only audits the user record and role membership.
- **Core:** Only audits the user record.
- **None:** No audit is stored.

> **Note:** When you specify a particular audit level, all audit levels that are at a lower priority level are automatically enabled. For example, if you specify the Membership audit level, then the Core audit level is automatically enabled.
>
> Audit level specifications are case-sensitive. When you specify an audit level, ensure that you do not change the case (uppercase and lowercase) of the audit level.

6.2.2 Tables Used for Storing Information About Auditors

Information about auditors is stored in the following tables of the database:

- AUD: This table stores information about all the auditors defined in Oracle Identity Manager.

- aud_jms: This table stores information about the changes made for an auditor.

  The key in this table is sent to the JMS. Oracle Identity Manager uses this table to control the order of the changes when multiple changes are made to the same user. You can use the Issue Audit Messages Task scheduled task to automate the reissue of messages that are not processed. This scheduled task is discussed in the "Issuing Audit Messages" on page 6-4.

6.2.3 Issuing Audit Messages

Oracle Identity Manager provides a scheduled task named Issue Audit Messages Task. This scheduled task retrieves audit message details from the aud_jms table and sends a single JMS message for a particular identifier and auditor entry in the aud_jms table. An MDB processes the corresponding audit message.

The following is the attribute of this task:

Max Records

Use the Max Records attribute to specify the maximum number of audit messages to be processed for a specified scheduled task run. The default value of this attribute is 400.

If there is a backlog of audit messages in the aud_jms table, then you can increase the value of the Max Records attribute. The value that you set depends on how many messages the JMS engine can process during the default scheduled task execution interval. This, in turn, depends on the performance of the application server and database. Before increasing the Max Records value, you must determine how much time is taken to process the number of audit messages in the JMS destination (oimAuditQueue) by, for example, using the administrative console of the application server. If the time taken is less than the scheduled task interval, then you can make a corresponding increase in the value of the Max Records attribute.

6.3 User Profile Auditing

User profile audits cover changes to user profile attributes, user membership, resource provisioning, access policies, and resource forms.

This section discusses the following topics:

- Data Collected for Audits
- Post-Processor Used for User Profile Auditing
- Tables Used for User Profile Auditing

6.3.1 Data Collected for Audits

By default, user profile auditing is enabled and the auditing level is set to Resource Form when you install Oracle Identity Manager. This auditing level specifies the minimum level required for attestation of form data.

You configure the audit level in the System Configuration part of the Advanced Administration by using the XL.UserProfileAuditDataCollection system property.

> **See Also:**
>
> "Audit Levels" on page 6-3 for more information about audit levels
>
> "System Properties in Oracle Identity Manager" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for information about the XL.UserProfileAuditDataCollection system property

This section discusses the following topics:

- Capture and Archiving of User Profile Audit Data
- Storage of Snapshots
- Trigger for Taking Snapshots

6.3.1.1 Capture and Archiving of User Profile Audit Data

Each time a user profile changes, Oracle Identity Manager takes a snapshot of the user profile and stores the snapshot in an audit table in the database.

A snapshot is also generated when there is a change in a user profile that must be audited, even if an initial snapshot is missing. The current snapshot is treated as the initial snapshot.

The following are the components of a user profile and the tables that store these components:

- User Record: USR table, including all User Defined Fields (UDFs)
- User Role Membership: USG, UGP, and RUL tables
- User Policy Profile: UPP and UPD tables

> **Note:** When you change a role name by using the Administrative and User Console, the User Profile Audit (UPA) tables in the database are not updated with the change until the next snapshot of the user.

- User Resource Profile: This component can be divided into the following subcomponents:
  - User Resource Instance: OIU, OBI , OST, and OBJ tables
  - Resource Lifecycle (Provisioning) Process: ORC, PKG, TOS, STA, OSI, SCH , MIL tables
  - Resource State (Process) Form: All tables that have names starting with UD_* (including child tables)

6.3.1.2 Storage of Snapshots

When Oracle Identity Manager takes a snapshot of a user profile, it stores the snapshot in the UPA table. The structure of the UPA table is described in Table 6–1.

Table 6–1   Definition of the UPA Table

Column	Data Type	Description
UPA_KEY	NUMBER (19,0)	Key for the audit record
USR_KEY	NUMBER (19,0)	Key for the user whose snapshot is recorded in this entry

Table 6–1   (Cont.) Definition of the UPA Table

Column	Data Type	Description
EFF_FROM_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry became effective
EFF_TO_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry was no longer effective In other words, this is the date and time at which the next snapshot entry was created. For the entry representing the latest user profile, the To Date column value is set to NULL.
SRC	VARCHAR2 (4000)	User ID of the user responsible for the change, and the API used to carry out the change
SNAPSHOT	CLOB	XML representation of the snapshot
DELTAS	CLOB	XML representation of old and new values corresponding to a change made to the snapshot
SIGNATURE	CLOB	Can be used to store a digital signature for the snapshot (for nonrepudiation purposes)

6.3.1.3 Trigger for Taking Snapshots

When any data element in a user profile changes, Oracle Identity Manager creates a snapshot.

The following events trigger the creation of a user profile snapshot:

- Modification of any kind to the user record (for example, through reconciliation and direct provisioning)

- Role membership change for the user

- Changes in the policies that apply to the user

- Provisioning a resource to the user

- Deprovisioning of a resource for the user

- Any provisioning-related event for a provisioned resource:

  - Resource status change

  - Addition of provisioning tasks to the provisioning process

  - Updates to provisioning tasks in the provisioning process, for example, status changes, escalations, and so on

  - Creation of or updates to Process Form data

6.3.2 Post-Processor Used for User Profile Auditing

The user profile auditor has an internal post-processor that normalizes the snapshot XML into the reporting tables: UPA_USR, UPA_FIELDS, UPA_GRP_MEMBERSHIP, UPA_RESOURCE, UPA_UD_FORMS, and UPA_UD_FORMFIELDS. These tables are used by the reporting module to generate the appropriate reports.

6.3.3 Tables Used for User Profile Auditing

User profile audits use the following tables in the database:

The UPA table is the main table and stores all the snapshots and changes made to the user profiles. The audit engine reads data from the UPA table and normalizes it across the following reporting tables:

- UPA_USR: This table stores user profile information.

■ UPA_FIELDS: This table stores user profile information in a vertical format.

   This table has more information than the UPA_USR table. For instance, UD fields are stored in this table as well as other fields that are not available in UPA_USR.

■ UPA_GRP_MEMBERSHIP: This table contains role membership for all the users in the system.

   The information includes when a user was added and removed from a role.

■ UPA_RESOURCE: The information in this table includes provisioned resources and changes in status for each of the resources.

   This table does not include any form table information.

■ UPA_UD_FORMS: Along with the UPA_UD_FORMFIELDS table, this table contains information about changes to the process form. It contains information about the corresponding tables that are being changed. The actual field changes are stored in the UPA_UD_FORMFIELDS table.

■ UPA_UD_FORMFIELDS: This table stores the names of form fields that are changed and the old and new values of the changed form fields. Whenever a form field is changed, a new row is inserted in this table to reflect the change.

> **Note:** The UPA_UD_FORMS and UPA_UD_FORMFIELDS tables will be populated only if the XL.EnableExceptionReports system property is set to TRUE. For more information about this property, see "System Properties in Oracle Identity Manager" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

6.4 Role Profile Auditing

Role profile audits cover changes to role profile attributes, role administrators, and direct subroles.

This section discusses the following topic:

■ Data Collected for Audits

6.4.1 Data Collected for Audits

Unlike user auditing, an independent audit level is not defined for role profile auditing. Instead, the audit levels defined for user profile auditing are used for role profile auditing. Role profile auditing takes place only if the audit level defined for user profile audit level is Membership or a level higher than that. By default, user profile auditing is enabled and the audit level is set to Resource Form when you install Oracle Identity Manager. As a result, role profile auditing is also enabled by default because the default audit level for user profile audit is Resource Form, which is higher than Membership.

This section discusses the following topics:

■ Capture and Archiving of Role Profile Audit Data

■ Storage of Snapshots

■ Trigger for Taking Snapshots

6.4.1.1 Capture and Archiving of Role Profile Audit Data

Each time a role profile changes, Oracle Identity Manager takes a snapshot of the role profile and stores the snapshot in an audit table in the database.

Oracle Identity Manager generates a snapshot when an audit is created for a role, even if an initial snapshot is missing. The current snapshot is treated as the initial snapshot.

The following are the components of a role profile and the tables that constitute these components:

- User role record: UGP table, including all UDFs for roles

- Subrole information: GPG table

6.4.1.2 Storage of Snapshots

When Oracle Identity Manager takes a snapshot of a role profile, it stores the snapshot in a GPA table. The structure of this table is as described in Table 6–2.

Table 6–2   Definition of the GPA Table

Column	Data Type	Description
GPA_KEY	NUMBER (19,0)	Key for the audit record
UGP_KEY	NUMBER (19,0)	Key for the role whose role snapshot is recorded
EFF_FROM_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry became effective
EFF_TO_DATE	TIMESTAMP (6)	Date and time at which the snapshot entry was no longer effective In other words, this is the date and time at which the next snapshot entry was created. For the entry representing the latest user profile, the To Date column value is set to NULL
SRC	VARCHAR2 (4000)	Source of the entry, User ID of the user responsible for the change, and the API used to carry out the change
SNAPSHOT	CLOB	XML representation of the snapshot
DELTAS	CLOB	XML representation of old and new values corresponding to a change made to the snapshot
SIGNATURE	CLOB	Can be used to store a digital signature for the snapshot (for nonrepudiation purposes)

6.4.1.3 Trigger for Taking Snapshots

When any data element in the role profile snapshot changes, Oracle Identity Manager creates a snapshot.

The creation of role profile snapshots is triggered by events that result in changes in any of the following:

- Role profile data

- Subrole information

Part II

Oracle Identity Manager Self Service

This part describes the various self service tasks that you can perform in Oracle Identity Manager.

It contains the following chapters:

7

Configuring and Using Self-Service Registration

This chapter describes the tasks that you can perform using self-service registration and how to configure auto-approval for self-registration in the following sections:

- Using Self-Service Registration
- Configuring Auto-Approval for Self-Registration

7.1 Using Self-Service Registration

The login page when accessed in an unauthenticated context provides the ability to log in, and provides a starting point for all unauthenticated operations. This page is displayed when you access Oracle Identity Manager Administrative and User Console without authenticating either natively to Oracle Identity Manager or by using SSO.

Typical tasks you can perform before logging in to Oracle Identity Manager Administrative and User Console include:

- Logging In to Oracle Identity Manager Administrative and User Console
- Submitting Registration Requests
- Tracking Registration Requests

7.1.1 Logging In to Oracle Identity Manager Administrative and User Console

To login to Oracle Identity Manager Administrative and User Console:

> **Note:**
>
> - If Oracle Identity Manager is configured to support native authentication, then the login link takes you to a form in which you can authenticate by using your Oracle Identity Manager username and password.
>
> - If Oracle Identity Manager is configured to support Single Sign-On (SSO), then the login link takes you to the SSO application login page.

1. Go to Oracle Identity Manager Administrative and User Console login page.

2. In the User ID field, enter your username.

3. In the Password field, enter your password.

4. Click **Sign In**. If you are successfully authenticated, then are logged in and directed to the main page in the authenticated context.

   The login attempt might generate an error because of the following reasons:

   - **Incorrect credentials:** If the user name and password entered are not correct, then an error message is displayed. This may be because of the following reasons:

     Username does not exist

     Password is incorrect

     Username exists but the user is deleted

     Note:

     - The system configuration property Maximum Number of Login Attempts provides the number of times authentication can fail before your OIM account is locked. By default this value is 10. The login backend must keep a counter of the number of times a failed login attempt occurs on an account. When login fails, the backend increments the count. For a successful authentication while the account is not locked, the counter is reset to 0. If the counter exceeds the value of the Login Failures Allowed before Lockout configuration property, then the account is locked. In addition, the value of the Account Locked On attribute is set to current timestamp, and the value of the Manually Locked attribute is set to No.

     - If the configuration property is set to 0 or a negative number, then the account is not locked irrespective of how many login attempts fail.

   - **Locked account:** If the account is locked, then you are not allowed to log in even if the credentials are correct. If an account is locked by the system and not manually locked, then the system configuration property "Direct Locked User to Forgotten Password" determines if the error message stating that the account is locked also directs you to the "Forgotten Password" feature. Going through that flow successfully will unlock a locked account if the system is configured to do so.

   - **Disabled user:** If your user account is disabled, then you are not allowed to log in.

5. If your password has expired, then the Change Password form is displayed. You are not allowed to proceed to the main page of the console without changing the password. Enter a new password and click **Sign In**.

6. If the system configuration property "Force to set questions at start up" is set to "Yes", then the login flow checks if you have set the required challenge responses on your profile. If not, then the form to set the challenge responses is displayed. If you have the challenge responses set, or if the configuration property is set to "No", then this step is skipped. In the form, set the challenge responses, and then click **Submit**.

   Alternatively, you can click **Remind Later** if you want to avoid setting challenge questions and logging on to Oracle Identity Manager Self Service.

> **Note:** The PCQ.FORCE_SET_QUES system property with <NAME>
> Force to set questions at startup indicates whether or not the challenge
> questions are required to be set on login. If not, then a Remind Later
> button is displayed. On clicking this button, you can log in to the
> console without setting the challenge questions.

If you attempt to access a deep linked UI in Oracle Identity Manager and you are
not already logged in, then you are redirected to the login page. Follow the login
instruction provided in this section to log on to Oracle Identity Manager.
However, you will be directed to the deep linked UI instead of the authenticated
User console.

7. If the system property "Force Password Change At First Login" is set to "Yes" then
   the login flow forces you to change the password the first time when you log in to
   Oracle Identity Manager Administrative and User Console.

7.1.2 Submitting Registration Requests

Oracle Identity Manager requires you to register yourself with identity to Oracle
Identity Manager to perform certain tasks on Oracle Identity Manager Self Service. To
register yourself in to Oracle Identity Manager:

1. In Oracle Identity Manager Administrative and User Console login page, click
   Register. The Basic information page of User Registration wizard is displayed.

2. Enter first name, middle name, last name, and email in the respective fields and
   click **Next**. The Login Information and Security Information page is displayed.

   The UI does not allow you to enter more than the allowed number of characters.
   The maximum length for the values entered during self-registration is specified as
   80 characters for First Name, Middle Name, Last Name, and Common Name and
   382 characters for the Display Name.

   If any other attributes are added on the self-service UI by modifying the dataset,
   the values will not be validated explicitly. The field on the UI will allow only as
   many characters to be entered as specified in the length field of the UI.

   There is no restriction on the characters that can be entered in each of these fields.
   The input for each of these fields can contain any special characters.

   Email should be provided as per the pattern mentioned against system property
   "XL.EmailValidationPattern". If the email is inappropriate, the UI gives an error
   "Invalid e-mail ID. Please enter a valid email ID." If the email Id specified is
   already used by any other user in the system, the UI gives an error "Email ID
   <email id> is already taken. Please enter a different Email ID."

3. In the **Select a User ID and Password** section, enter user login, password and
   confirm password. The password entered will be subjected to a password policy.
   On the next page, the password policy is shown adjacent to the password fields. If
   the password does not satisfy the criteria of the password policy, the UI gives an
   error defining the criteria required to be satisfied. Refer "Password Management"
   on page 1-3 for detailed information about password policy.

   If you do not enter the password, then the system generates the password
   automatically and emails it to the email address that you entered in the first page
   of the User Registration page.

> **Note:**
>
> - The registration form is internally populated based on templates provided for self-registration. The registration page contains attributes defined in the template and not hardcoded to these attributes.
>
> - The Administrator can create custom self-registration URLs by specifying the custom template name in the URL. The link that the end-user uses will then determine the template used during self-registration. So, multiple forms of self-registration can be supported via such register links. For registration, either the link will be configured on the UI or specified in the email for the end-user to register.

4. In the **Set your Challenge Questions and Answers** section, select the challenge questions and set an answer for each question. The challenge questions and answers are checked for:

   - distinct challenge questions not selected

   - distinct answers not specified for the challenge questions

   If these conditions are not satisfied, an error is displayed.

5. Click **Register**. You are provided a tracking ID for the registration request that can used for tracking the request.

   > **Note:**
   >
   > - Challenge questions and answers are asked if the attribute for this is defined in the template for self registration.
   >
   > - All Oracle Identity Manager deployments do not support self-registration. This is especially true of internal deployments that manage the identities of employees and contractors, where the identities are added through reconciliation and not self-registration.
   >
   > - The configuration property Provide is "Is Self-Registration Allowed". The Register link is always displayed on the unauthenticated self-service console. If the property is set to False, then clicking on the Register link gives an error, "Self registration is not allowed". If it is set to True, then self registration is allowed.

7.1.3 Tracking Registration Requests

You can track your request to register as an identity in Oracle Identity Manager. If the current status indicates success, then you can go to the Oracle Identity Manager Administrative and User Console, and then enter your username and password to log in to the Oracle Identity Manager Self Service.

To track your registration:

1. In Oracle Identity Manager Administrative and User Console login page, click **Track Registration**. The Request Status page is displayed.

2. In the Tracking ID field, enter the tracking ID that was assigned to your registration request. Then click **Submit**. The Self-Registration Status page is displayed with the following details:

- Request ID

- Request submission date

  This date is not shown explicitly. When the request is submitted and approval is not done, the Date shown equals the request submission date. As such, track registration shows only the last update date.

- Current status

  Every self-registration request that is submitted has to go through approvals for it to be processed completely. Refer "Approval Levels" for details about different approval levels in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

  If a user tracks the current status of the request, the status is shown with a description of the stage the request is in. The status would be one of the following:

  Pending: This state indicates that the request is submitted and the approval is pending. In case of default approval, the following status message is displayed:

  "Obtaining request-level approval for registration. The manager needs to approve this request."

  If the request level approval is pending. Once the request level approval is obtained, the following status message is displayed:

  "Obtaining operation-level approval for registration."

  Rejected: This state indicates that the request is rejected during approval. The description indicates the reason of rejection. In case of default approval levels, if the request got disapproved at the request approval level, the following status message is displayed:

  "Request approval rejected for registration."

  If the request gets disapproved at the operation approval level, the following status message is displayed:

  "Operation approval rejected for registration."

  Completed: This state indicates that the request is completed. If all the approvals have been provided and the request is successfully completed, the following status message is displayed:

  "The registration request is completed."

  Failed: This state indicates that the request is failed during submission. If the request submission is failed, the following status message is displayed:

  "The request registration failed."

- Date of last status update

Note: You can only track the status of Self Registration Requests from this page.

7.2 Configuring Auto-Approval for Self-Registration

End-user self-registration can be configured so that the system will automatically approve new registrations without human intervention.

In the default self-registration template, SelfCreateUserDataset.xml, the Organization field is designated as an approver-only field. This means that an approver must manually supply a value for the Organization field when approving the request. To configure the self-registration template so that registrations are approved automatically, make a copy of the default template, remove the approver-only flag for the Organization field, and provide a link to the new template. See the following task for more details.

To Configure Auto-Approval for Self-Registration:

Note: You must understand the concepts covered in Chapter 10, "Managing Requests", before undertaking this task.

---

1. Create a new request template for Self-Register user by making a copy of the default template. Include the Organization attribute but add a restriction by specifying the organization that should be used.

   For information about configuring the request template, refer to Chapter 17, "Managing Request Templates".

2. Modify the self-create user data set to remove the approver-only flag for the Organization attribute.

   For details about request datasets, refer to "Creating a Request Dataset for the Resources" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

   For information about uploading the data set into MDS, refer to "Uploading Request Datasets into MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

3. Create two new approval policies, one with the request level approval enabled for self-registration, and the other with the operational level approval enabled.

   For information about creating approval policy rules, see "Creating Approval Policies" on page 18-4.

4. Refer to the following to use the newly created template for self-registration:

   ■ The system takes a parameter T_ID=<template name> to use a custom template for self-registration. If the user clicks on the Register link, it takes the user to the following page:

     http://host:port/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=SELF_REGISTRATION

     This page uses the default template.

   ■ To use a custom template, use T_ID at the end of the request, for example:

     http://host:port/oim/faces/pages/USelf.jspx?E_TYPE=USELF&OP_TYPE=SELF_REGISTRATION&T_ID=<new_template>

     This will display the self-registration page as per "new_template" instead of the default one.

8

Managing Profile

The Profile page enables you to view and modify personal details. The actions that you perform while managing a user profile are determined by the authorization policies defined for "Self Service User Management". These authorization policies are defined for Oracle Identity Manager and stored in Oracle Entitlements Server (OES).

All authorization privileges are controlled by authorization policies. Every privilege that is granted is validated to check if you have the permission to use it. Table 8 1 lists the privileges for profile management operations:

Table 8 1   Profile Management Privileges

Privilege	Description
VIEW_USER_DETAILS	This privilege determines if you have the ability to view the user profile attributes in the Attributes tab of the My Profile page. This privilege supports fine-grained attribute level controls, which allows you to select the specific attributes that apply to that operation.
MODIFY_USER_DETAILS	This privilege determines if you have the ability to modify the user profile attributes in the Attributes tab of the My Profile page. This privilege supports fine-grained attribute level controls, which allows you to select the specific attributes that apply to that operation. If you have view and modify privileges for an attribute, it will be shown as an editable attribute on the My Profile page. If you have the view privilege only for an attribute, then it will be shown as a read-only attribute on the My Profile page.
MODIFY_SELF_USER_PRO XY_PROFILE	This privilege determines if you have the ability to add, modify, and remove a proxy in the Proxies tab of the My Profile page.

> **See Also:**
>
> - Chapter 15, "Managing Authorization Policies" for details on authorization policies and authorization for profile attributes
>
> - Chapter 17, "Managing Request Templates" for information about request templates
>
> - "Request Dataset" for information about request datasets in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

To view the Profile section:

1. Login to Oracle Identity Manager Self Service.

2. Click the **Profile** tab.

The Profile page has the following sections:

- Managing Profile Attributes
- Managing Role Assignments
- Managing Resource Profile
- Managing Proxies
- Managing Security
- Resetting Forgotten Password

8.1 Managing Profile Attributes

The first tab of the My Profile page is the Attributes tab. This tab displays the user's profile attributes. The attributes that are displayed are controlled by field-level authorization policies that determine which profile attributes are visible to "self".

By default, all the profile attributes are visible to the user. Any new attribute added for the user entity is by default set to be hidden from the user until explicitly made visible.

In addition, field-level authorizations determine if the attributes are editable or not by self. Editable attributes are displayed in editable text boxes or appropriate UI widgets, such as lookup fields. You can provide new values and click the Apply button to submit a change.

When the profile update is submitted, request is submitted for modification of all attributes:

- The attributes for which a request is raised are displayed and along with a tracking number for the request. Workflow rules determine the approval workflow to start and obtain approval before allowing the changes in attributes. The status of the request can be seen on the Requests tab of the self-service page. For more information about request tab and Modify User request, see Chapter 10, "Managing Requests".

- The Preferences section on the Attributes tab provides access to user preferences. Using this option, you can set your preferences on how you expect the product to behave.

    The user preferences in Oracle Identity Manager are attributes stored as part of the user's profile. By default, the following attributes are shown on the UI:

    - **Locale:** You can select the language preference based on the languages supported by Oracle Identity Manager. The administrator defines the languages supported by the installation as part of the deployment configuration. You can only select from the limited set of languages configured for the deployment.

    - **Time Zone:** You can specify the time zone in which all data is displayed.

> **Note:**
>
> - Other default attributes can be added by modifying the user profile in the self service user management administration policy in Oracle Identity Administration. A custom policy needs to be created to view and modify other attributes in my profile.
>
> - User-defined fields (UDFs) can be added by creating a policy and adding attributes in the self service user management administration policy in Oracle Identity Administration. To add the User defined attributes for view or modification under the Attributes tab, these UDFs need to be added to the modify user data set for self-service. Also, a custom policy needs to be created under self service user management to grant permission to view and/or modify these attributes.
>
> For details on authorization policies, refer "Creating and Managing Authorization Policies" on page 15-2.

8.2 Managing Role Assignments

The Roles tab displays the roles of which you are a member, directly or indirectly. It displays the following information:

- Role Display Name: Displays the role name.

- Description: Displays the description of the role.

- Membership Type: Displays the membership type, either direct role or indirect role.

- Assigned Date: Displays the date on which you are assigned to a role.

The tab also provides options to start the following role management operations based on authorization policy:

- Requesting Roles

- Removing Roles

Based on authorization policy, you can perform role management operations, such as requesting a role and removing a role.

> **Note:** Removing a role can also be performed through a request.

8.2.1 Requesting Roles

To request a role:

1. Go to **My Profile**, **Roles**.

2. From the Actions list, select **Request Role**. The Select Roles page of the Request Role wizard is displayed. The roles those are made available for the end user in the list of roles on Request Roles page are the result of intersection of the roles provided in the request template and roles for which the user has search permission.

> **Note:** If you have access to any other template other than out of the box templates (templates in Oracle Identity Manager), then, you will be prompted to select a template. This step is skipped if you have access only to pre-defined templates.

3. In the Role Name field, enter the name of the role that you want to request. You can also search for roles based on role name and/or role display name by using the icon next to the Role Name field to display a list of available roles.

4. From the Available Roles list, select one or more roles that you want to request, and then click the **Move** icon to include the roles in the Selected Roles list.

5. Click **Next**. The Justification page is displayed.

6. Enter values in the Effective Date and Justification fields to specify the date from which the role is to be active and a comment to justify the request respectively.

7. Click **Finish**. You can view the status of the request on the Requests tab of Oracle Identity Manager Self Service. See Chapter 10, "Managing Requests" for the detailed information about request statuses.

8.2.2 Removing Roles

To remove a role:

1. Go to **My Profile**, **Roles**. A list of roles is displayed in a table.

2. Select a role to be removed in the table and from the Actions list, select **Remove Role**. The Select Roles page of the Remove Role wizard is displayed.

> **Note:** If you have access to any other template other than out of the box templates (templates in Oracle Identity Manager), then, you will be prompted to select a template. This step is skipped if you have access only to out of the box templates.

3. In the Role Name box, enter the name of the role that you want to remove. You can also search for the role names by using the icon next to the Role Name field to display a list of available roles.

4. From the Available Roles list, select one or more roles that you want to remove, and then click the **Move** icon to include the roles in the Selected Roles list. This step is applicable only if a custom template is configured for "self remove roles" operation and the user selects one of the templates.

5. Click **Next**. The Justification page is displayed.

6. Enter values in the Effective Date and Justification fields to specify the date from which the role is to be removed and a comments to justify the removal respectively.

7. Click **Finish**. The status of the request can be seen on the Requests tab of the self-service page. For more information about request tab, see Chapter 10, "Managing Requests".

8.3 Managing Resource Profile

The Resources tab displays the resources that are currently provisioned to you. For each resource in the list, you are allowed to view the following information associated with that resource:

- Resource name

- Status

- Identifying information

- Summary information block with additional information

You can drill down to a page that displays details about the provisioned resource. On this page, you can modify the resource by clicking the Modify Resource button. This redirects you to the "Modify Resource" request wizard with the beneficiary preset to "self" and the resource instance also preset. You can go through the process of providing the updates that you want to request, and any associated information. A tracking number for the request is generated.

Self-service requests can only modify one resource instance at a time and cannot support bulk requests. If you want to modify another resource instance, then you must raise another request.

In the Resources tab, you can perform the following:

- Requesting a Resource

- Modifying a Resource

- Removing a Resource

- Displaying Resource Details

8.3.1 Requesting a Resource

To request a resource:

1. Go to **My Profile**, **Resources**.

2. From the Actions list, select **Request Resource**. The Select Request Template page is displayed.

> **Note:** This page is displayed only if you have access to any other template other than out of the box templates (templates in Oracle Identity Manager). You will be prompted to select a template. This page is skipped if you have access only to out of the box templates.

3. From the Request Template list, select the request template assigned to the resource and click **Next**. The Select Resources page of the Request Resources wizard is displayed.

4. In the Resource Name field, enter the name of the resource that you want to request. You can also search for the resource names by using the icon next to the Resource Name field to display a list of available resources.

> **Note:** The resources displayed in this screen is a conjunction of the list of resources available and the list of resources restricted in request template that is being used. For example, If available resources are Active Directory, Exchange, and UNIX and in the template, if the resources are restricted to Active Directory and Exchange, this screen displays only Active Directory and Exchange.
>
> If no resources are selected for restriction in the request template, then all the available resources are displayed.

5. From the Available Resources list, select a resource that you want to request, and then click the **Move** icon to include the resource in the Selected Resources list.

> **Note:** In case of bulk request, you must select two or more resources (two or more child requests will be created). The rest of the procedure is same for bulk request.

6. Click **Next**. The Enter Resource Data form is displayed.

7. Enter appropriate details related to the resource, and then click **Next**. The Justification page is displayed.

8. Enter values in the Effective Date and Justification fields to specify the date from which the resource is to be active and a comment to justify the request respectively.

9. Click **Finish**. The status of the request can be seen on the Requests tab of the self-service page. For more information about request tab, see Chapter 10, "Managing Requests"

8.3.2 Modifying a Resource

To modify a resource:

1. Go to **My Profile**, **Resources**.

2. From the Actions list, select **Modify Resource**. The Select Request Template page is displayed.

> **Note:** This page is displayed only if you have access to any other template other than out of the box templates (templates in Oracle Identity Manager). You will be prompted to select a template. This page is skipped if you have access only to out of the box templates.

3. From the Request Template list, select the request template assigned to the resource and click **Next**. The Select Resources page of the Request Resources wizard is displayed. The Select Resources page is displayed.

4. In the Resource Name field, enter the name of the resource that you want to modify. You can also search for the resource names by using the icon next to the Resource Name field to display a list of available resources.

5. From the Available Resources list, select one or more resources that you want to request, and then click the **Move** icon to include the resource in the Selected Resource list.

6. Click **Next**. The Resource related page is displayed in which you can modify the resource details. Enter the updates that you want to request and any associated information.

> **Note:** You can raise a request to modify one resource instance at a time, and this model does not support bulk requests. If you want to modify another resource instance, then you must raise another request.

7. Click **Next**. The Justification page is displayed.

8. Enter values in the Effective Date and Justification fields to specify the date from which the resource is to be active and a comment to justify the request respectively.

9. Click **Finish**. The status of the request can be seen on the Requests tab of the self-service page. For more information about request tab, see Chapter 10, "Managing Requests".

8.3.3 Removing a Resource

To remove a resource:

1. Go to **My Profile**, **Resources**.

2. From the Actions list, select **Remove Resources**. The Select Request Template page is displayed.

> **Note:** This page is displayed only if you have access to any other template other than out of the box templates (templates in Oracle Identity Manager). You will be prompted to select a template. This page is skipped if you have access only to out of the box templates.

3. From the Request Template list, select the request template assigned to the resource and click **Next**. The Select Resources page of the Request Resources wizard is displayed. The Select Resources page is displayed.

> **Note:** This page is also displayed only if you have access to any other template other than out of the box templates (templates in Oracle Identity Manager). You will be prompted to select a template. This page is skipped if you have access only to out of the box templates.

4. In the Resource Name box, enter the name of the resource that you want to remove. You can also search for the resource names by using the icon next to the Resource Name field to display a list of available resources.

5. From the Available Resources list, select one or more resources that you want to remove, and then click the **Move** icon to include the resources in the Selected Resources list.

6. Click **Next**. The Justification page is displayed.

7. Enter values in the Effective Date and Justification fields to specify the date from which the resource is to be removed and a comment to justify the removal respectively.

8. Click **Finish**. The status of the request can be seen on the Requests tab of the self-service page. For more information about request tab, see Chapter 10, "Managing Requests"

8.3.4 Displaying Resource Details

To display resource details:

1. Go to **My Profile**, **Resources**.

2. From the resource information table, select a resource.

3. From the Actions list, select **Open Resource Details**. The Resource Details form with the details such as resource name, description, type, status, service account, and date provisioned are displayed for the selected resource.

8.4 Managing Proxies

The Proxies tab allows you to view and manage the proxy information. It displays the proxies currently set up within Oracle Identity Manager for you, and also allows you to view previously set up proxies. The Past Proxies view is read-only and no modifications are allowed.

The existing proxy view allows you to cancel an upcoming proxy whose start date is in the future. You can also edit only the end date of an in-progress proxy whose start date is in the past and end date is in future or not specified.

In the Proxies tab, you can also add new proxies. When adding up new proxies, you must specify a start date, an end date, and the user.

This section contains the following topics:

- Adding a Proxy

- Editing a Proxy

- Removing a Proxy

8.4.1 Adding a Proxy

To add a proxy:

1. Go to **My Profile**, **Proxies**.

2. In the Current Proxies section, from the Actions list, select **Add Proxy**. The Add Proxy window is displayed.

3. In the Proxy Name field, select **My Manager** to specify your manager as proxy. Otherwise, select **Other User** to specify any other user as proxy. You can search for the user name.

4. In the Start Date field, specify a start date.

5. In the End Date field, specify an end date.

6. Click **Apply**. A message box is displayed asking for confirmation.

7. Click **Yes**.

8.4.2 Editing a Proxy

To edit a proxy:

1. Go to **My Profile**, **Proxies**.

2. In the Current Proxies section, from the Actions list, select **Open Proxy Detail**. The Proxy Detail window is displayed.

3. In the Proxy Name field, select **My Manager** to specify your manager as proxy. Otherwise, select **Other User** to specify any other user as proxy. You can search for the user name.

> **Note:** To change the proxy user, you can search only those users for which you have search permission.

4. Click **Edit**. In case of active proxy, you cannot edit the proxy name and the start date, but in case of the proxy that has not started, you can change the proxy user, start date, and end date.

5. Click **Apply**. A message box is displayed asking for confirmation.

6. Click **Yes**.

8.4.3 Removing a Proxy

To edit a proxy:

1. Go to **My Profile**, **Proxies**. A table with the list of proxies is displayed.

2. Select a proxy to be removed.

3. In the Current Proxies section, from the Actions list, select **Remove Proxy**. The Remove Proxy window is displayed.

4. Click **Remove**. A message box is displayed asking for confirmation.

5. Click **Yes**.

8.5 Managing Security

The Security tab allows you to change your profile attributes related to password security. Using this tab, you can perform the following tasks:

- Changing Password
- Setting Challenge Questions and Response

8.5.1 Changing Password

Using this feature, you can reset your enterprise password.

After the security operations are successfully negotiated, you are allowed to provide a new enterprise password. To specify a new password, enter and re-confirm the new passwords. The new password is evaluated for compliance against the applicable password policy, which is displayed on the Change Password page. If the new password does not comply with the password policies, then the password change will be rejected and you will be informed of the failing condition(s). If the password evaluates successfully against all policies, then the enterprise password is changed.

To change the password:

1. Go to My Profile page, click the **Security** tab.

2. In the Password section, click **Change Password**. The Change Password window is displayed with the applicable password policy.

3. In the Old Password field, enter the existing password.

4. In the New Password field, enter the new password that you want to set.

5. In the Re-Type New Password field, re-enter the new password.

6. Click **Apply**. If the old password is valid and the new password is in compliance with the password policy, then the password is changed. Otherwise, an error message is displayed.

8.5.2 Setting Challenge Questions and Response

The challenge-response service allows you to set up a series of challenge questions that are used to validate the user's identity. Only the user should know the correct answers to the challenge questions.

Questions and answers are stored as part of the user's profile as a name-value pair list, where the name is the question, and the value is the answer to that question. For example, for user John Doe, the challenge-response set could be as follows:

Challenge	Response
What is your favorite color?	Blue
What is the name of your pet?	Rex
What is the city of your birth?	New York

When a user's identity needs to be validated without relying on the authentication scheme, the challenge questions are asked, and the user must provide the necessary number of correct answers.

Oracle Identity Manager configuration properties for this feature are as follows:

- **PCQ.USE_DEF_QUES:** If Oracle Identity Manager has been customized to allow end-users to create their own challenge questions, this property specifies whether users must select their challenge questions from a predefined list, or if users should create their own challenge questions. The default value is TRUE (users must select their challenge questions from a predefined list). To require users to provide their own challenge questions, set the value to FALSE.

  > **Note:** Functionality that allows end-users to create their own challenge questions is not supported in the standard, out-of-the-box user interface.

- **PCQ.NO_OF_QUES:** Sets the number of challenge questions that must be completed by a user. The default value is 3.

- **PCQ.FORCE_SET_QUES:** Determines if new users must set up challenge questions upon logging into the application for the first time, or if new users can skip this step and do it later. New users are redirected to the Self.jspx page where the user can select challenge questions. This page includes a Skip button so that users can skip the challenge question set up process.

> **Note:** You can access the Admin.jspx page in another tab. This is the same page for setting challenge questions in the Oracle Identity Manager Administrative and User Console by performing the password validation.

To set the challenge questions and responses:

1. Go to the My Profile page and click the **Security** tab.

2. In the Challenge Questions section, select questions from the Question 1, Question 2, and Question 3 fields.

3. In the corresponding Answer 1, Answer 2, and Answer 3 fields, select the answers.

4. Click **Apply**.

8.5.2.1 Localizing Challenge Questions and Responses

The following default challenge questions are localized automatically in Oracle Identity Manager:

- What is the name of your pet?

- What is the city of your birth?

- What is your favorite color?

- What is your mother's maiden name?

Localized default challenge questions are located in the xlWebAdmin_lang.properties file.

If you add custom challenge questions to Oracle Identity Manager Design Console for lookup code Lookup.WebClient.Questions, add corresponding properties to the custom resource bundles to localize the question text in the supported languages. Corresponding translations should be saved to the following file:

CustomResource_lang.properties

For example, you might add the new challenge question What is your favorite sport?. To localize this text, add properties to the property files in the following format:

```
global.Lookup.WebClient.Questions.question-text=value
```

Replace any white spaces in the question text with a hyphen (-). For example, to localize the "What is your favorite sport?" challenge question in French, add the following property to the customResources_fr.properties file:

```
global.Lookup.WebClient.Questions.What-is-your-favorite-sport?=
Quel est votre sport favori?
```

To modify the text of the default challenge questions, add corresponding properties to the custom resource bundles. For example, to modify the text of the "What is your favorite color?" question to use the British spelling (colour) instead of the American version (color), add the following new property in the CustomResource_en.properties file:

```
global.Lookup.WebClient.Questions.What-is-your-favorite-color?=W
hat is your favourite colour?
```

To modify the text of the default challenge questions for a specific locale, add properties for the modified questions to the customResources.properties file and the customResource_lang.properties file that represents the locale's language. For

example, the customResources_ja.properties file contains language property translations for Japanese.

8.6 Resetting Forgotten Password

If you have forgotten your Oracle Identity Manager password, you can reset it by entering your responses for a series of challenge questions.

To reset your forgotten password:

1. In Oracle Identity Manager Administrative and User Console login page, click **Forgot Password**. The Enter Your User Login page of the Forgot Password wizard is displayed.

2. In the User Login field, enter your user login to allow Oracle Identity Manager to locate your user record. Then click **Next**. The Answer Challenge Questions page is displayed. If you enter a wrong user login, then an error message is displayed stating, "Either user account is invalid or challenge questions are not defined for this account. Cannot reset the password".

3. In this page, the wizard provides the challenge questions that you set during user registration to verify your user identity. This page also displays the applicable password policies. Enter your responses to the challenge questions, and then click **Next**. The Set a New Password page is displayed. If your responses to challenge questions are incorrect, then an error message is displayed stating, "Either user account is invalid or challenge questions are not defined for this account. Cannot reset the password"

   > **See Also:** Chapter 7, "Configuring and Using Self-Service Registration" for information about registering to oracle Identity Manager

4. In this step, enter the new password that you want to set, and click **Save**. The following are the possible outcomes of these steps:

   - If the new password fails to satisfy the configured password policies, then an error message is displayed specifying the rules of the password policy that are not met by the specified password. Also, if you exceed the maximum number of reset password attempts, you will no longer be able to perform this operation. An error message will be displayed stating, "User has exceeded reset password attempts. Cannot proceed further to perform this operation".

   - If you satisfy the identity verification criteria and the password is successfully set, a message is displayed stating that the password has been reset and you will be automatically logged in to the Self-Service console.

     > **Note:** The configuration properties that control the challenge questions in the Forgot Password wizard are:
     >
     > - Number of Challenge Questions to Ask: Number that specifies how many challenge questions to display in the wizard and to collect responses for.
     >
     > - Number of Correct Responses Needed: Number that specifies how many challenge questions must be answered correctly to pass the identity verification test. This cannot be greater than the previous configuration property.

9

Managing Tasks

In the Welcome page of Oracle Identity Manager Self Service, when you click **Tasks**, the My Tasks page is displayed. This page displays the task instances of specific types. These types are associated with specific Oracle Identity Manager components. The task types are approvals, provisioning, and attestation. The My Tasks page can be used by both administrators and end-users. For example, an IT department personnel responsible for delivering a laptop to an employee may not be an Oracle Identity Manager administrator, but needs to view and change provisioning tasks.

The following task types are supported in Oracle Identity Manager:

- **Approval tasks:** These tasks are instantiated by request service and correspond to associated requests that are in the user or administrator's queue to be approved. For more information about approval tasks, see "Managing Approval Tasks" on page 9-1.

- **Provisioning tasks:** These tasks correspond to either pending manual provisioning tasks or failed automatic provisioning tasks in the user or administrator's queue. For more information about provisioning tasks, see "Managing Provisioning Tasks" on page 9-8.

- **Attestation tasks:** These tasks correspond to outstanding attestation process in the user or administrator's queue. For more information about attestation tasks, see "Managing Attestation Tasks" on page 9-14.

> **Note:** Only approval tasks are fetched from BPEL and rest of the tasks come from Oracle Identity Manager.

9.1 Managing Approval Tasks

In Oracle Identity Manager, the Oracle BPEL request service is used to handle various aspects of human interaction in Oracle Identity Manager workflows. This request service is used to assign tasks to identities, such as users and roles. You can perform various operations upon tasks assigned to you. For example, you can approve, reject, or claim a task, or request for more information. The process flow in corresponding Oracle Identity Manager workflow is dependent on the outcome of given tasks.

> **See Also:** "Approval Workflows" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information information about BPEL workflows

When a request is submitted, the request service eventually utilizes the BPEL request service and initiates the approval as a task in Oracle BPEL server. This task is assigned to the approver. Further processing of this request by request service remains pending,

which is subject to the outcome of the corresponding task. The approver must be able to access the Approvals tab in the All Tasks section that lists all the tasks assigned to the approver. The approver can now act upon this task and set its outcome, for example, approve or reject. After the task outcome has been set, the request service resumes the processing of the request that is based on the task outcome.

On successful submission of requests, the request service invokes request service, which creates BPEL Human Tasks and assigns them to users or roles in Oracle Identity Manager. Authenticated users can view the tasks waiting for action in the Approvals tab. When you click **Tasks** in Oracle Identity Manager Self Service, the Approvals tab is open by default.

In the first section of the Approvals tab page, you can search for requests based on task name, request ID, start date, and end date. The search results are displayed in a table in the lower part of the Approval tab page. From the View Tasks Assigned To list, you can select the following:

- You Only: To sort only the approval tasks assigned to you

- Roles You Have: To sort the requests assigned to the roles of which you are a member

- You and Roles You Have: To sort the requests assigned to you and to the roles of which you are a member

- Users You Manage: To sort the requests assigned to your reportees

The table in the lower part of the Approvals tab page lists all tasks that are assigned to you and Roles you have, by default. Using this table, you can perform operations on tasks and can also view the Task details. For information about task details, see "Viewing Task Details" on page 9-3.

Table 9 1 describes the columns in the full tasklist view table:

Table 9 1   Columns in the Full Tasklist View Table

Column	Description
Request ID	ID of the request associated with the approval task
Request Type	The type of request
Beneficiary	The beneficiary for the request
Request Target	The target entity associated with the request. It can be either role name or resource name or user name
	Example 1: For "Assign Roles" type of request, it is role name
	Example 2: For "Provision Resource" type of request, it is resource name
	Example 3: For "Modify User" type of request it is user display name
Requester	The user who created and submitted the request
Assignee	The user or role to whom the approval task is assigned
Date Assigned	The date when the task was assigned to you or the role

You can perform the following tasks in the Approvals tab:

- Viewing Task Details

- Claiming a Task

- Approving a Task

- Rejecting a Task

- Reassigning a Task

- Requesting for More Information

- Submitting Information

9.1.1 Viewing Task Details

When you click on Request ID link of any of the approval tasks in the table, Task details are shown for that approval task.

The Task Details page displays a detailed view of the request in the Basic Details and Request Information sections. This view type lists the complete details of a selected task. It allows complete management of the listed task. To display the task details view, select a row in the full tasklist table, and then select **Open Task Details** from the Actions list.

If some attributes are marked as approver-only in request dataset, then there will be an additional section called "Additional Data From Approver". It is in this section, where approver can provide data, without which the approver will not be allowed to approve a request. In the next level of approval, the approver can modify the data, if required. Similarly, if the approver sends the task to another user for more information (using "Request For Information" operation), then the user to whom it is assigned can see an additional section called "Additional Request Information" in Task details and the user can send a response to the information requested.

In addition, the following tabs display details associated to the request:

- **Resources or User or Role:** The Resources tab is dynamically generated based on the request type. It displays a list of beneficiaries, name of the target resources, and links to view the details about the target resources.

  The User tab shows the user details that is part of a request. For example, in case of CreateUser, User tab displays the user name and "View Details" link will provide the attributes of the user provided during the request creation.

  The Role tab shows the role details that is part of a request. For example, it can be a role name that you want to add or remove.

- **Request Comments:** This tab displays any request comments associated with the request. The comments recorded are questions and responses for Request for Information. For example, the comments that an approver requests for additional information from the user and the response provided by the user to those queries are recorded in this section.

- **Request History:** This tab displays the various changes the request has been through in the process of execution.

Modification of task details can only be performed in the Task Details page. Following modifications are supported:

- An approver might need to fill in some mandatory request information before approving the corresponding task. For this, the Task Details page displays the "Additional Data From Approver" section, where approver can fill in the required information.

- An approver can explicitly add comments in task. All the request comments are displayed in the Request Comments tab in the Task Details page. You can also add comments indirectly while requesting for more information or submitting information on a task. For information about requesting for more information and

submitting information, see "Requesting for More Information" on page 9-5 and "Submitting Information" on page 9-7 respectively.

9.1.2 Claiming a Task

If a task is assigned to a group, then all users who belong to that group view the task in their queue. You can claim a task that is assigned to the roles you have, and approve it later. For example, when a request is created to provision a laptop to a user, the request-level approval is configured to be provided by the requester's manager, and the operation-level approval is configured to be given by a user who is a member of the resource IT administrator group. Therefore, after the request-level approval is obtained, the request is submitted for operational-level approval. For this, the user who is a member of the resource IT administrators group must first claim the task to be able to approve or reject it later.

To claim a task:

1. In the Welcome page of Oracle Identity Manager Self Service, click **Tasks**.

2. From the View Tasks Assigned To list, select **Roles You Have**. The tasks assigned to the roles to which you are a member are displayed in the search results table.

3. Select the task that you want to claim.

4. From the Actions list, select **Claim Task**. A message is displayed asking for confirmation.

5. Click **OK**.

9.1.3 Approving a Task

The Approval Tasks displayed in the Approvals table can be of the following two levels of approval:

- Request Level

- Operational Level

To approve a request level task that is assigned to you:

1. Go to **Tasks**, **Approvals** and click **Search**. As an approver, if you are expected to provide some information before approving the task, then provide the information in the "Additional Data From Approver" section of the Task Details page.

> **Caution:** If no information is provided before approving a task for which information is requested, then you are not allowed to approve the request until you provide some information in the "Additional Data From Approver" section.

2. Select a request in the full tasklist view table.

3. From the Actions list, select **Approve Task**. The request is approved and is no longer displayed in the full tasklist view table.

To approve a operational level task that is assigned to you:

1. Go to **Tasks**, **Approvals** and click **Search**. The operational level requests are displayed.

2. Select a request in the full tasklist view table.

3. From the Actions list, select **Approve**. The request is approved and is no longer displayed in the full tasklist view table.

9.1.4 Rejecting a Task

To reject a request that is assigned to you:

1. Go to **Tasks**, **Approvals** and click **Search**.

2. Select a request in the full tasklist view table.

3. From the Actions list, select **Reject Task**. The system prompts you to enter comments for rejecting the request.

4. Enter the comments and click **Reject**. The task is rejected and is no longer displayed in the full tasklist view table. The comments that you enter here are recorded in the "Request Comments" section of the Task Details page.

9.1.5 Reassigning a Task

To reassign a request that is assigned to you:

1. Go to **Tasks**, **Approvals** and click **Search**.

2. Select a request in the full tasklist view table.

3. From the Actions list, select **Re-Assign**. The Re-Assign Task dialog box is displayed.

4. Search and select the user to whom you want to re-assign the task.

5. Click **Re-Assign**.

> **Note:** The functionality supported by Oracle Identity Manager task list is a subset of functionality offered by SOA human workflow component. For example, Oracle Identity Manager task list does not support reassigning tasks to roles. However, SOA human workflow does support this feature functionality.

9.1.6 Requesting for More Information

An approver can request the Requester or some other user (in Oracle Identity Manager) for more information about the request associated with the task. After this action is performed, the task is converted to Request For Information (RFI) type of task and is assigned to the specified user. This action is only available on the task details view. The exchange of information between the approver and the user is added to the Comments tab of the Task Details page.

To request for more information about a task:

1. Go to **Tasks**, **Approvals** and click **Search**.

2. In the Task Details window for a task, from the Actions list, select **Request More Information**. The Request More Information dialog box is displayed.

3. In the Send to field, select Requester or search and select some other user from whom you want more information about the task.

4. Enter the details about the required information.

5. Click **Submit Request**. A message is displayed stating that the task is sent for additional information.

6. Click **OK**.

When the user to whom the information is requested views the request in the Approvals tab page of Oracle Identity Manager Self Service, RFI is added to the task preview, as shown in Figure 9 1:

Figure 9 1   The RFI Task

When you select the task and expand the Actions menu, the Approve, Reject, Re-Assign, and Claim Task options are not available because you must provide the requested information before performing any of these actions. Only the Task Details option is available, as shown in Figure 9 2, so that you can view the details of the task and provide the requested information.

Figure 9 2   Available Option for an RFI Task

9.1.7 Submitting Information

This action is only applicable on the RFI type of tasks. You can provide the requested information by using task comment(s), and then use this action to submit the requested information. After this action is performed, the task is converted to original approval task again. It is then reassigned back to the original user who had requested for more information and task approval flow continues from there. This action is only available on the task details view.

User can submit the additional info requested by approver using this action. The requested query will be shown and the user needs to provide the details. The exchange of information is recorded as comments.

To submit information:

1. In the Task Details: Approval tab, click on the Request ID link of the RFI task. Alternatively, you can select the RFI task, and from the Actions menu, select **Task Details**. The Task Details view for the RFI task is displayed, as shown in Figure 9 3:

Figure 9 3   RFI Task Details

2. In the Additional Request Information section, in the Response field, enter the information that is requested about the task.

3. Click **Submit to Approver**. A message is displayed stating that the additional information is submitted successfully.

4. Click **OK**.

The task is no longer displayed as RFI task in the Approvals tab. This task can now be approved, rejected, reassigned, or claimed.

All the additional information submitted for a request can be viewed in the Request Comments tab of the Task Details page.

9.2 Managing Provisioning Tasks

This tab displays all provisioning tasks assigned to you or pending actions in your inbox. The list does not include automatic provisioning tasks, for example, the task for collecting a cell phone in the IT administrator's provisioning task queue. However, failed automatic provisioning tasks that you must review to take corrective action are displayed in your inbox. You must take corrective action, such as retry and manually complete, on those tasks.

The provisioning tasks feature is used by administrators as well as users. For example, the person in IT administration who is responsible for delivering a laptop computer to an employee may not be an administrator in Oracle Identity Manager, but must view and change provisioning tasks.

You can perform the following tasks in the Provisioning tab:

-   Searching Provisioning Tasks

-   Viewing Provisioning Task Details

-   Adding Notes to a Task

-   Reassigning a Task

-   Viewing Task Assignment History

-   Viewing Form Details

-   Modifying Form Details

■ Retrying a Task

9.2.1 Searching Provisioning Tasks

The first section in the Provisioning tab page allows you to search for the provisioning tasks assigned to you or on which your action is pending. Specify values in the following fields to search for the provisioning tasks:

■ **Match:** Select **All** if you want to match all the search criteria that you specify. Select **Any** if you want to match any search criteria that you specify.

■ **Task Name:** Specify a task name that you want to search. To do so, select any one of the equal, contains, begins with, or ends with search operations.

■ **Resource Name:** Specify a resource name whose provisioning task you want to search. To do so, select any one of the equal, contains, begins with, or ends with search operations.

■ **Status:** Select **Pending** or **Rejected** to search for tasks for which your action is pending or for rejected tasks respectively.

After specifying the search criteria, when you click Search, the search results table is displayed. Table 9 2 lists the fields in the search results table:

Table 9 2   Fields in the Provisioning Tasks Search Results Table

Field	Description
Task Name	The name of the task
Task Status	The status of the task, which is Pending or Rejected
Resource Name	The name of the resource, which is affected by this task
Beneficiary	The user whose provisioned resource will get affected because of this task
Date Assigned	The date and time when the Provisioning task has been assigned to the Assignee
Assignee	The user to whom the task is assigned

9.2.2 Viewing Provisioning Task Details

To view provisioning task details:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task whose detail you want to view.

3. From the Actions list, select Open Task Detail.

Table 9 3 lists the fields in the Task Details window:

Table 9 3   Fields in the Task Details Window

Field	Description
Task Name	The name of the task
Resource Name	The name of the resource, which is affected by this task
Description	A description of the task
User	The beneficiary user name
Status	The status of the task, Pending or Rejected

Table 9 3 (Cont.) Fields in the Task Details Window

Field	Description
Response	The response set by the user on the Set Response page **Note:** For information about setting response, see "Setting Response for a Task" on page 9-10.
Response Description	The description of the response that is defined in the Response tab of the Task Definition section in Oracle Identity Manager Design Console
Notes	The additional comments entered by the approver
Assigned to	The user to whom or role to which the task is assigned **Note**: If the task is assigned to a role, this property will come as "Assigned to Role" with the role details.
Error Details	The error, if any, while setting the response
Projected Start	The date when the task is scheduled to start
Projected End	The date when the task is suppose to end
Actual Start	The date when the task was started
Actual End	The date when the task was ended
Last Update	The date when the task was last updated

9.2.3 Setting Response for a Task

As an approver, you can set a response for the task while taking an action on the task. To set a response for a task:

> **Note:**   Response cannot be set if there are no response codes defined for the corresponding tasks. Response codes are defined by using Oracle Identity Manager Design Console. For more information about defining response codes, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task whose detail you want to view.

3. From the Actions list, select Open Task Detail. The Task Details window is displayed.

4. In the Specify Task Responses page, select one of the multiple responses defined and click **Set Response**.

9.2.4 Adding Notes to a Task

Notes are additional comments provided by the approver. These comments are optional.

To add notes to a task:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task whose detail you want to view.

3. From the Actions list, select Open Task Detail. The Task Details window is displayed.

4. In the Task Details window, click **Add Notes**. The Add Notes for Task window is displayed, as shown in Figure 9 4:

Figure 9 4   The Add Notes for Task Window
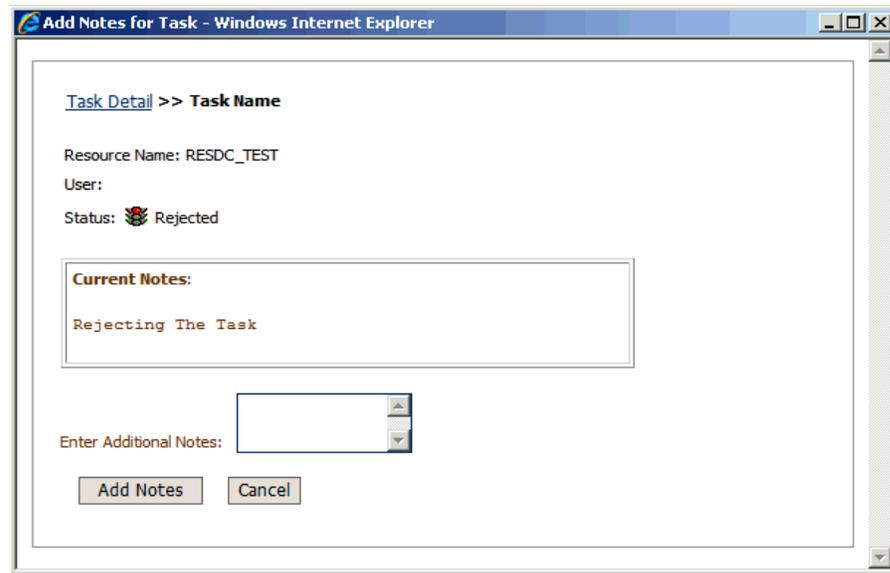
5. In the Enter Additional Notes field, enter the note that you want to add to the task.

6. Click **Add Notes**.

9.2.5 Reassigning a Task

As the approver, you can reassign a task to another user or role for taking appropriate action on the task. When the task is reassigned to another user, the assignee becomes the approver. When the task is reassigned to a role, any one member of that role can approve or reject the task.

To reassign a task to another user or role:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task whose detail you want to view.

3. From the Actions list, select Open Task Detail. The Task Details window is displayed.

4. In the Task Details window, click **Reassign**. The Select User Assignee for Task window is displayed, as shown in Figure 9 5:

Figure 9 5   The Select User Assignee for Task Window
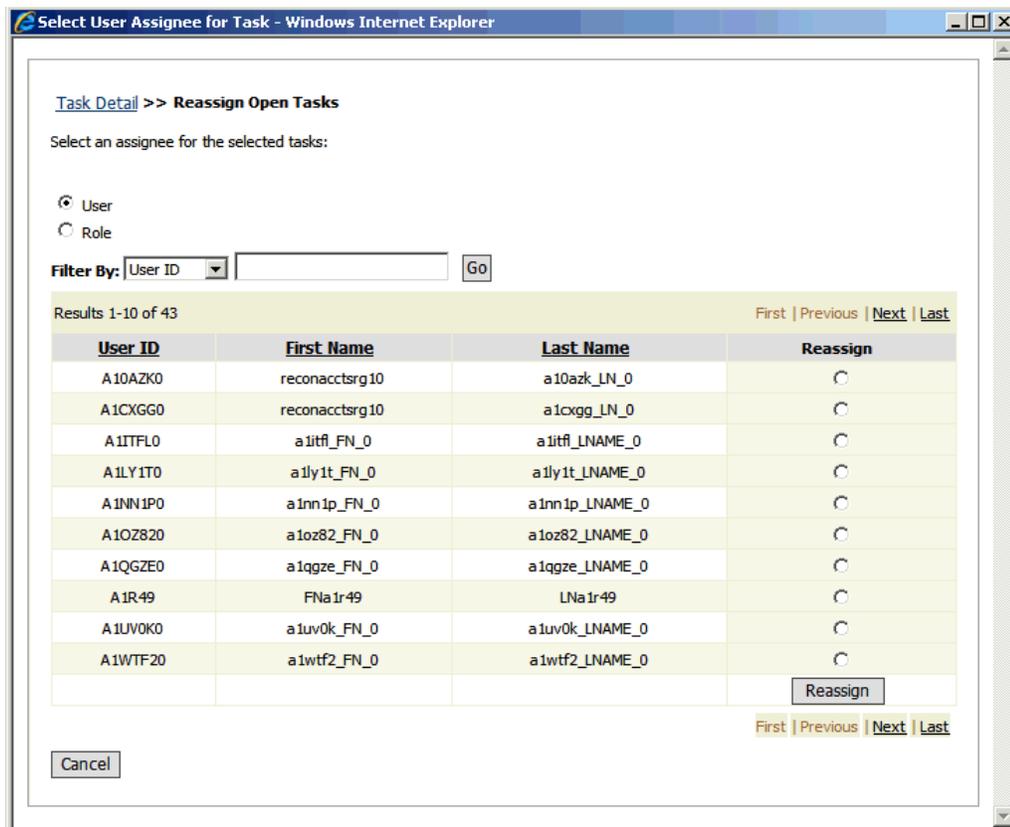
5. Select **User** or **Role** depending on what you want to search for. A list of users or roles is displayed, depending on your selection. You can also filter the search by specifying a criteria for filtering and entering a value in the Filter By field.

6. In the Reassign column, select a user or role to whom you want to assign the task.

7. Click **Reassign**.

8. In the Confirm Tasks to Reassign page, read the details of the action that you are performing and select **Confirm Re-assign Task** to reassign the task or select **Cancel Re-assign Task** to cancel the task reassignment.

9. Check whether the value in the Assigned to section is properly updated according to the above reassignment action.

9.2.6 Viewing Task Assignment History

To view the assignment history of a task:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task whose detail you want to view.

3. From the Actions list, select Open Task Detail. The Task Details window is displayed.

4. In the Task Details window, click **Task Assignment History**. The Task History window is displayed, as shown in Figure 9 6:

Figure 9 6   The Task History Window

The task assignment history is displayed in the fields, as shown in Table 9 4:

Table 9 4   Fields in the Task History Window

Field	Description
Task Status	The status of the task, Pending or Rejected
Task Action	The source details of the task, for example, when the task is first created it will be "Engine". If the user reassigns the task, it will be "User".
Assign Type	The type of the assignee of the task, for example, when the task is assigned for the first time, it is "Default Task Assignment". If the task is reassigned, then its value is either user or role.
Assigned to User	The user to whom the task is assigned
Assigned to Role	The role to which the task is assigned
Assigned By	The user who assigned the task
Assigned Date	The date when the task was assigned

9.2.7 Viewing Form Details

You can view the process form attached with a task. These are process forms associated with the underlying process definition. A task is embedded in the process definition.

To view the process form attached with a task:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task for which you want to view the process form.

3. From the Actions list, select **Open Form**. The View Form window is displayed.

9.2.8 Modifying Form Details

To modify the process form details:

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task for which you want to modify the process form.

3. From the Actions list, select **Edit Form**.

4. Modify the required details and click **Save**.

9.2.9 Retrying a Task

As the approver, you can retry a task when an error was generated while setting the response in the first attempt. To retry a task:

> **Note:** Only automated tasks can be retried, and an adapter must be attached to the task. Manual tasks cannot be retried.

1. Go to **Tasks**, **Provisioning** and click **Search**.

2. In the search results table of the Provisioning tab. select a task that you want to retry.

3. From the Actions list, select **Retry Task**. A message is displayed stating the status, whether the task is successfully retried or not.

9.3 Managing Attestation Tasks

Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe provisioned resources of other users. A reviewer can attest to the accuracy of the entitlements by providing a response. The attestation action, along with the response the reviewer provides, any associated comments, and an audit view of the data that the reviewer views and attests to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an attestation task.

An attestation process is the mechanism by which an attestation task is set up. Input that an attestation process requires includes information about how to define the components that constitute the attestation task and how to associate the attestation task with a schedule at which the task must be run. This definition is also the basis on which the attestation task can be initiated when required.

The Attestation tab in Oracle Identity Manager Self Service displays all attestation processes assigned to you or pending your actions in your inbox. In the My Tasks section, when you click the **Attestation** tab, the Attestation page is displayed.

You can perform the following tasks in the Attestation tab:

- Searching Attestation Tasks
- Viewing Attestation Request Detail

9.3.1 Searching Attestation Tasks

To search for attestation tasks:

1. Go to **Tasks**, **Attestation.**

2. In the Search Task section of the Attestation tab, select **All** to search all the tasks that match the criteria you specify. Otherwise, select **Any** to search any task that matches your criteria.

3. In the Task Name field, enter the name of the task that you want to search. To do so, select the equals, contains, ends with, or begins with search operators.

4. In the Start Date field, specify a start date of the task by using the Start Date icon next to the field. To do so, select the after, equals, or before search operators.

5. Click **Search**. The attestation tasks that match the search criteria are displayed in a search results table. Table 9 5 shows the fields in the search results table:

Table 9 5   Fields in the Attestation Task Search Results Table

Field	Description
Task Name	The name of the task.
Process Code	An unique identifier for the task that is entered by the user.
Start Date	The start date of the attestation task.
Type	The type of task. This is hard coded as 'Access Right'.
Number of records	The number of records displayed as the search result.

9.3.2 Viewing Attestation Request Detail

To view attestation request detail:

1. Go to **Tasks**, **Attestation.**

2. In the Attestation tab, select an attestation task for which you want to view the request detail.

3. From the Actions list, select **Attestation Request Detail**. The Attestation Request Detail window is displayed, as shown in Figure 9 7:

> **Note:**   Multiple users, designated as reviewers can view the attestation request details. However, only one user, whoever does it first, can submit the attestation.

Figure 9 7   The Attestation Request Detail Window
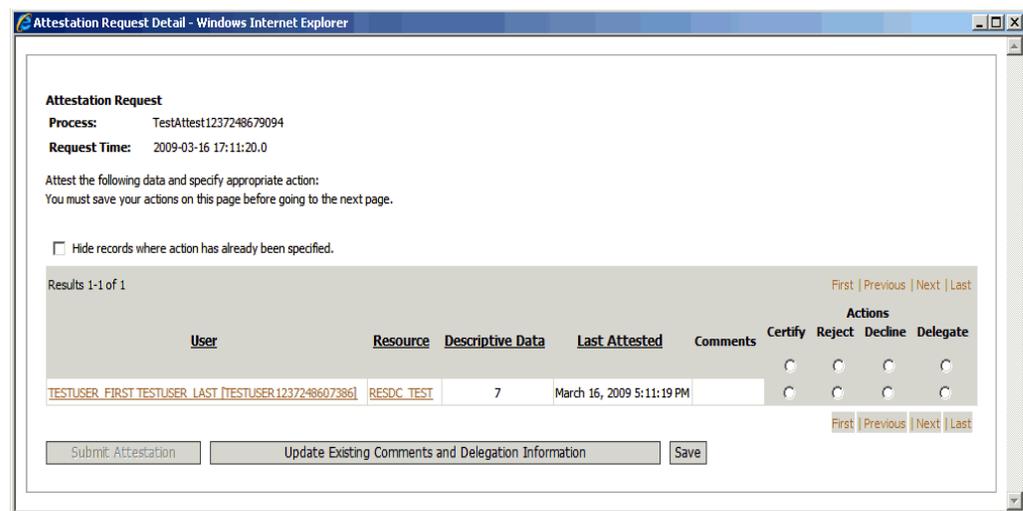
Table 9 6 lists the fields in the Attestation Request Detail window:

Table 9 6   Fields in the Attestation Request Detail Window

Field	Description
Process	Name of your attestation process created.
Request Time	The time when the request is created.
Hide records where action has already been specified	Whether or not the records for which action has been specified must be hidden from the list of attestation requests.
User	User whose entitlement is being attested. The data is displayed as a link. When you click the link, the user profile page is displayed with the user details for the attestation date.
Resource	Resource that is the basis for the entitlement being attested. The data is displayed as a link. When you click the link, a page is displayed with the process form data of the entitlement for the attestation date.
Descriptive Data	Description of the provisioned resource instance.
Last Attested	Last response that was provided for the attestation.
Comments	Reviewer comments. The comments will be updated in this field, when you click **Update Existing Comments and Delegation Information**. Long comments are truncated, and tooltips are used to show the full text of the comments.
Actions	Action to be performed on the request. The value can be one of the following: ■ Certify ■ Reject ■ Decline ■ Delegate
Submit Attestation	Click this button to submit the attestation request.
Save	Click this button to save the attestation request for future submission.

10

Managing Requests

In Oracle Identity Manager, various operations, such as creating a user or provisioning a resource, can be performed through requests. A request is an entity created by the users or administrators performing a specific action that requires a discretionary permission to be gained by someone or some process before the action can be performed. For example, a user can create a request to gain access to a laptop computer and a manager can create an open requisition based on the request.

A request has a requester, a beneficiary (optional), and a target entity. A *requester* is an entity that creates or raises a request. A requester can be a user or the system itself. The functional component decides on the requester for system-generated requests. For unauthenticated requests, the requester is not authenticated to Oracle Identity Manager and is therefore, not present in the system.

A *beneficiary* is an entity that benefits from the action performed after the request is completed and the request is completed only if it is executed successfully.

In Oracle Identity Manager, terms such as user, organization, roles, and resources are defined as entities. Each one of these entities maintains a list of attributes belonging to this entity. Each entity also defines a list of operations that it supports. Along with an operation, a subset of the entity attributes is specified as operational parameters to carry out that particular operation. *Target entity* is the resource that is requested for the beneficiary.

For instance, you create a request to provision a UNIX account for the user John Doe. Here, you are the requester, John Doe is the beneficiary, and the UNIX account is the target entity that is requested for John Doe.

Each request goes through a specific lifecycle after it is created in the system. This lifecycle is managed and controlled by the Request Service. The lifecycle transitions the request through various stages. The stage that a request is in determines what action the controller takes in that step, what operations are available on the request, and what possible stage the transitions are in at that time. Figure 10 1 outlines the process flow of a request:

Figure 10 1   Request Process Flow
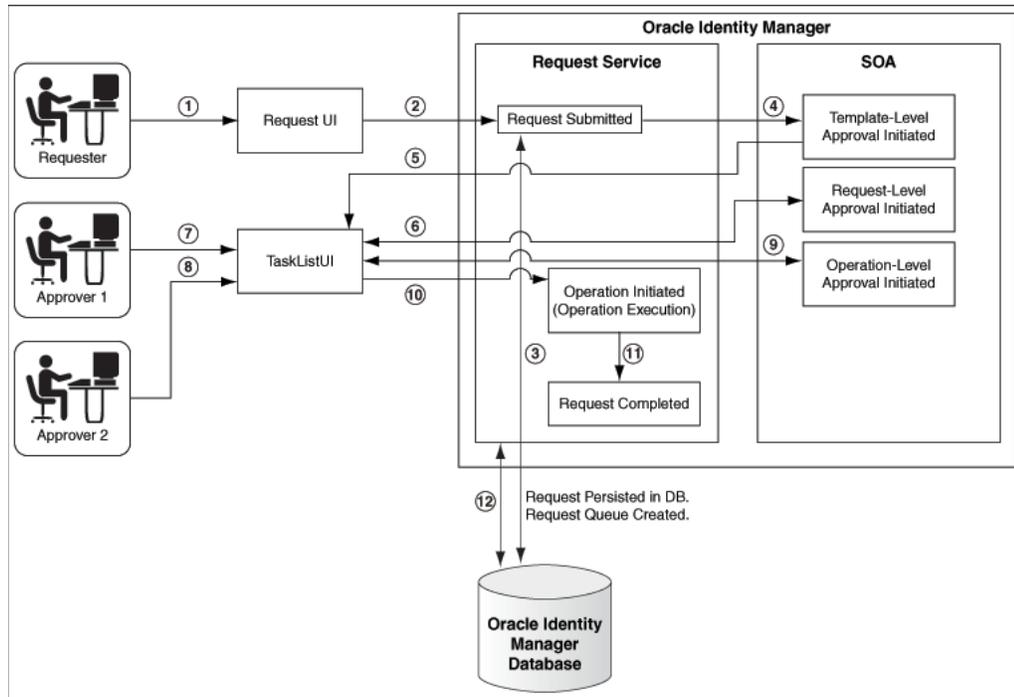
The request process flow is described with the help of an example of provisioning a laptop computer to a user through a request. The steps are:

1. The requester raises a request to assign a laptop computer to a user by using the Request UI.

    > **Note:**   Requests can be raised by using Oracle Identity Manager Self Service or Oracle Identity Manager Identity Administration.

2. The request is submitted to the request service.

3. The request is also stored in Oracle Identity Manager database.

4. Template-Level Approval workflow is initiated by request service in Service-Oriented Architecture (SOA).

5. If the template has approval process, then the request is submitted to the next level. If the template has no approval process, then the request gets auto approved.

6. Request-Level Approval workflow is initiated by request service in Service-Oriented Architecture (SOA). Based on the workflow configuration, associated tasks are assigned to the corresponding approvers.

    > **See Also:**   "Approval Workflows" for information about approval levels and approval workflows in the *Oracle identity Manager Developer's Guide*

7. The request-level approver approves the request by using the TaskList in Oracle Identity Manager Self Service. In this example, the requester's manager (Approver 1) is the request-level approver who decides whether to assign a laptop to user 1.

If the request-level approver rejects the request, the request goes to a Rejected stage.

8. If the Approver1 has designated his role to Approver 2 then Approver 2 is the request-level approver who decides whether to assign a laptop to user 1. If Approver 2 rejects the request, the request goes to a Rejected stage.

9. The operation-level approver approves the request by using the TaskList. In this example, the IT admin for the organization is the operation-level approver (Approver 2) who is responsible for issuing a laptop to the user. If the operation-level approver rejects the request, then the request goes to a Rejected stage.

10. The request operation is initiated in the request service, and the request is executed.

11. The request operation is completed. At this stage, the request operation has the Completed status.

12. The request status is updated in Oracle Identity Manager database.

This chapter describes request management in the following sections:

- Request Stages
- Bulk Requests and Child Requests
- Request Models
- Creating Requests for Self and Others
- Searching for Requests
- Withdrawing a Request
- Performing Request-Related Tasks by Using the Task List
- Closing Requests

10.1 Request Stages

Each request goes through a specific lifecycle after it is created in the system. This lifecycle is managed and controlled by the request service. The lifecycle transits the request through various stages. The stage a request is in determines what action the controller takes in that step, what operations are available on the request at that time, and what the possible stage transitions are. Figure 10 2 outlines the lifecycle flow of a request in the request service:

Figure 10 2   Request Stages
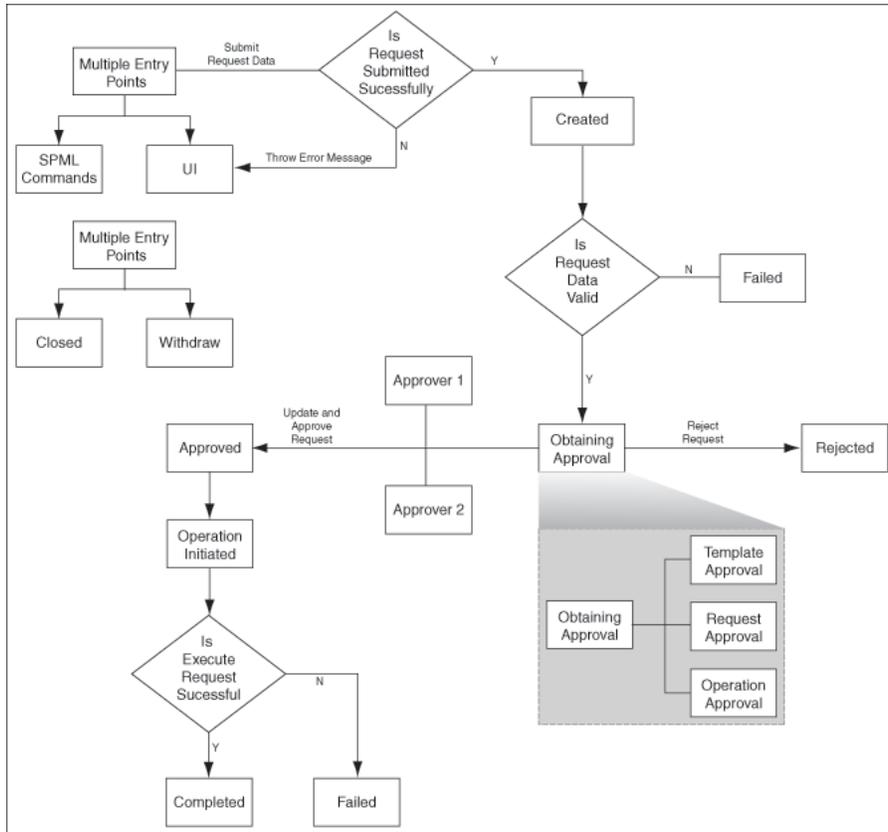
Figure 10 2 shows all the stages that a request can go through. This diagram specifies stages for a simple request. For information about bulk request, refer to Figure 10 3, "Bulk Request and Child Request Stages".

Each stage represents the logical next step in the request lifecycle. Only the successful execution of an operation can take the request from one stage to the next.

Table 10 1 describes how a request functions at various stages through its life cycle and how a request attains these stages:

Table 10 1   Request Stages

Request Stage	Description
Created	After successful submission of the request, the request moves to the Created stage.

Table 10 1   (Cont.) Request Stages

Request Stage	Description
Obtaining Approval	After the request attains the Submitted stage, request engine moves the request to "Obtaining Approval" stage automatically if there are approvals defined for this request. At this stage, the request engine looks at the request template first to find if there are any approvals defined. If it finds any, then the corresponding approvals are initiated through the request service. Upon completion of the same, the request engine looks at the model defined for this request to find out the approval selection methodology to find out the exact approval process to instantiate.
	When the request engine finds out the approvals that are required to be initiated, it again calls request service to instantiate the workflow.
	If a request is withdrawn or closed at this stage, then the request engine calls cancel workflow on each workflow instance. Notifications are sent to approvers about the withdrawn tasks.
	Note: Configuration of notification can be done in the human task of a SOA composite.
	The following request statuses are associated with Obtaining Approval stage:
	■ Obtaining Template Approval
	■ Obtaining Request Approval
	■ Obtaining Operation Approval
	For information about these request statuses, refer "Bulk Requests and Child Requests" on page 10-7.
	After the request successfully completes these statuses, it will attain the Request Approved stage.
	If a validation check is plugged-in after the request has been successfully created, the request is associated with the following statuses.
	■ SoD check not initiated
	A request attains this stage, if the SoD validation is not initiated for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.
	■ SoD check initiated
	A request attains this stage, if the SoD validation is initiated asynchronously for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.
	■ SoD check completed
	A request attains this stage, if the SoD validation is completed for provisioning resource based request. The request engine moves the request to this stage after submission of request and before Obtaining Approval.
	Note: These request statuses are possible in case the request is provision resource request or modify provision resource request.

Table 10 1   (Cont.) Request Stages

Request Stage	Description
Approved	Only after an Operation Approval is approved, the request is moved to the next stage and the request engine is updated with the current status of that instance. The outcome that the request engine finds is Approved, Rejected, or Pending.
	The following request statuses are associated with this stage:
	■ Template Approval Approved
	■ Request Approval Approved
	■ Operation Approval Approved
Rejected	Each time a workflow instance is updated, request service updates the request engine with the current status of that instance. The outcome that the request engine expects from request service is Approved or Rejected. If any of the workflow instances that are instantiated are rejected, then request engine moves the request to Rejected stage. If any workflow instance is rejected, then the controller calls cancel on all the pending workflows and moves the request to Rejected stage.
	The following request statuses are associated with this stage:
	■ Template Approval Rejected
	■ Request Approval Rejected
	■ Operation Approval Rejected
Operation Initiated	After the request is approved, the request engine moves the request to the Operation Initiated stage and initiates the operation.
	The following request statuses are associated with this stage:
	■ Operation Completed
	After completing the actual requested operation, the request engine moves the request to the Operation Completed stage. This happens after Operation Initiated status and is associated with Completed stage.
	■ Post Operation Processing Initiated
	After the actual requested operation is completed, if there exists any additional operation that needs to be executed as post-processing, the request engine moves the request to the Post Operation Processing Initiated stage, before initiating those operations. This happens after Operation Completed status.
Failed	When the associated operations specified in the request fails to execute, the request cancels any pending operations and moves the request to the Request Failed stage. The request statuses associated with this stage are Request Failed and Request Partially Failed, which is set based on the failing of all or any of the associated operations specified in the request respectively.

Table 10 1   (Cont.) Request Stages

Request Stage	Description
Withdrawn	A request can be withdrawn by the requester. At this stage, the request is associated to the Request Withdrawn status, and the initiation of all approvals are canceled, as indicated by multiple entry point in Figure 10 2.
	Note:
	■ A request can be withdrawn before Operation Initiated stage. Once the request attains the Operation Initiated stage, the request cannot be withdrawn.
	■ A request can always be withdrawn from Oracle Identity Manager Self Service and cannot be withdrawn from Advanced Administration.
Completed	After the execution of all operations specified in the request are completed, the request engine moves the request to the Request Completed stage.
	The following request statuses are associated with this stage:
	■ Request Completed with Errors
	A request attains this status, when an actual requested operation executes fine, but fails to execute any of the post-processing operations. The Request Completed with Errors stage is associated with the Failed stage.
	■ Request Completed
	A request attains this status, when an actual requested operation executes fine without any errors.
	■ Request Awaiting Completion
	When a request is scheduled to be executed on a future date, the request attains Request Awaiting Completion status till the operation is completed on an effective date.

The successful attainment of a stage also results in the status of the request being updated to the corresponding status.

Operations can be executed manually or automatically by the system in response to an event. Examples of manual operations are:

■ Submit request

■ Close/cancel (withdraw) request

■ Approve request when the service is notified that the approval workflow is successfully approved

Examples of automatic operations are:

■ Start approvals when the request is submitted

■ Execute request when the request is approved and execution date is in the past or not specified

10.2 Bulk Requests and Child Requests

A bulk request is a request with multiple beneficiaries, multiple target entities, or both. For example, a request to provision multiple roles to user John Doe generates a bulk request. A provisioning request to add users John Doe and Jane Doe to the Managers group also generates a bulk request. A bulk request has two parts:

- Parent requests: A request submitted with multiple beneficiaries, multiple target entities, or both is a parent request

- Child requests: When the request level approval happens for a parent request, multiple child requests are created. The parent request is divided into multiple child requests containing one beneficiary and one target entity, or both.

The entity data in bulk requests must be same for different beneficiaries specified in the request. For example, for a deprovisioning bulk request, the requester can select different resource instances to be deprovisioned for different beneficiaries. In such a situation, the association between the resource instances and their beneficiaries is maintained.

The number of child requests generated depends on the number of target entities associated with each beneficiary. For each beneficiary, one of its associated target entities is used to generate for each child request. A child request contains only one beneficiary and one target entity.

For a request with no beneficiaries, each child request is spawned for each target entity. Consider the following example:

For a deprovisioning bulk request, there are two beneficiaries. For the first beneficiary, three resource instances are to be deprovisioned and for the second beneficiary, two resource instances are to be deprovisioned. In this scenario, there are three child requests for the first beneficiary and two child requests for the second beneficiary. Each resource instance and its associated beneficiary are present in each child request. Therefore, for this bulk request, there are a total of one parent request and five child requests.

Consider another example. For a modify-user bulk request, two user instances are to be modified. For this request, two child requests are spawned addressing one user instance each.

Template-level approval is performed as a part of parent request. If the request template used to create the request has an associated approval process, then request will move to "Obtaining Template Approval" stage. If the template has no approval process, request will be auto-approved at template level and is moved to "Obtaining Request Approval" stage.

Request-level approval is performed as a part of parent request. After the parent request spawns child requests, the parent request goes to the Operation Initiated stage, where in the request awaits for the child requests to complete the operation-level approval. After all the child requests completes, the parent request moves to the Completed statehouse requester is the same for both parent request and child requests.

Operation-level approval is performed for child requests only. Approvers can approve or reject child requests individually. If all the child requests are approved, then the parent request will attain the Completed stage. If one of the child requests fail, then the parent request attain the Partially Failed stage. If all the child requests fail, the parent request attain the Failed stage.

outlines the lifecycle flow of a request in the request service:

Figure 10 3   Bulk Request and Child Request Stages
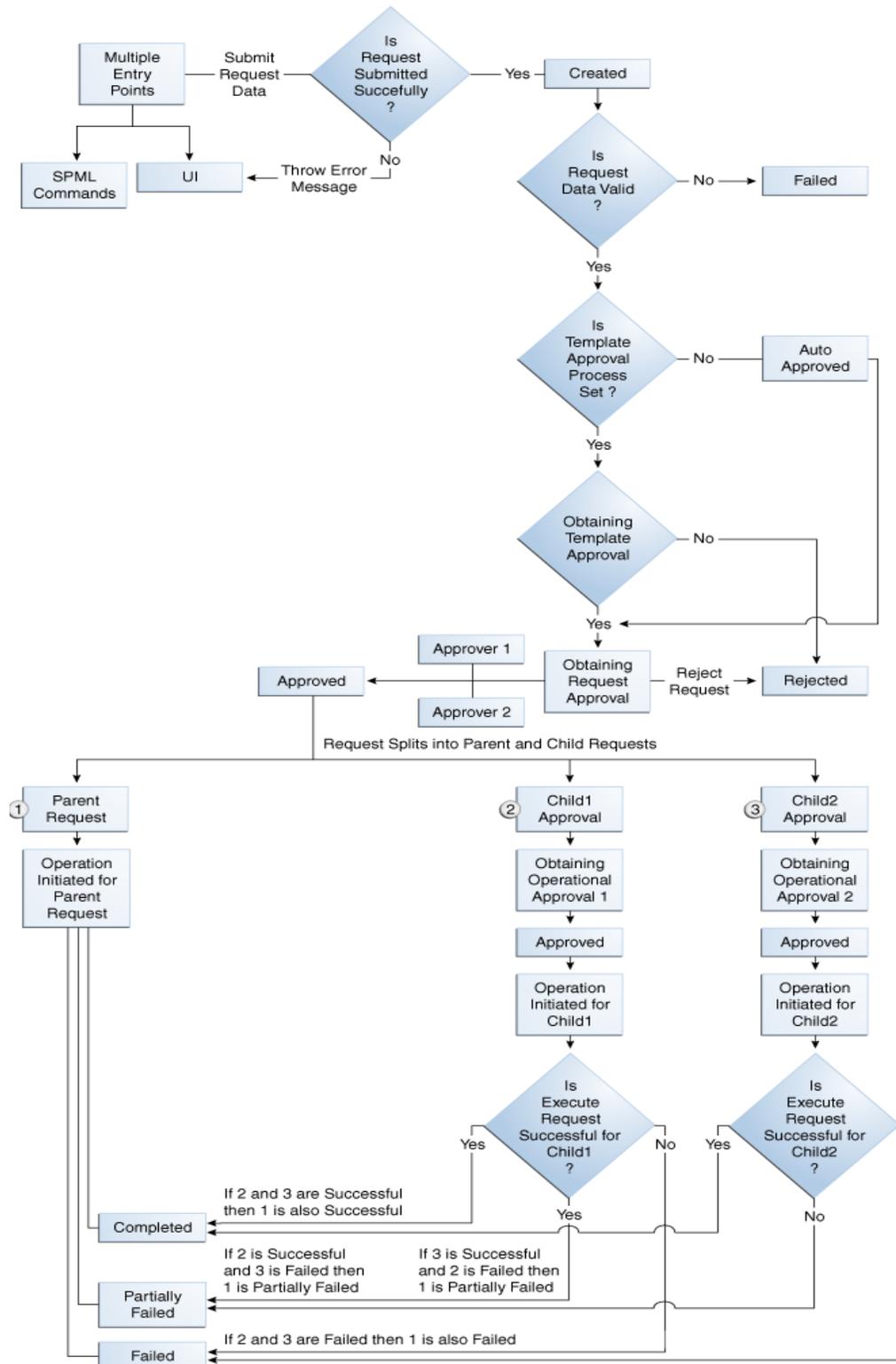
See Also:

- for information about the request models that support bulk request

- for information about request stages

10.3 Request Models

A request model is a specification that instructs the request management engine to behave in a specific way for a particular request type. Each request must have a request model associated with it. There is a one-to-one relation between a request model and a request type. A request model dictates what information to collect, how to get the approvals, and what action to perform. For example, the information defined for the Create User and Modify User request models are different, and as a result, the actions for each request type are different.

> **Note:** Oracle Identity Manager provides the request models by default. Request models cannot be modified.

Oracle Identity Manager provides a set of predefined request models. Table 10 2 lists the operations and request models that Oracle Identity Manager supports by default.

Table 10 2   Default Operations and Request Models

Catalog	Request Model	Bulk	Self or Admin	Beneficiary
User Management	Create User	N	Admin	N
	Self-Register User	N	Self	N
	Modify Self Profile	N	Self	N
	Modify User Profile	Y	Admin	N
	Enable User	Y	Admin	N
	Disable User	Y	Admin	N
	Delete User	Y	Admin	N
Provisioning	Provision Resource	Y	Admin	Y
	Self-Request Resource	Y	Self	Y
	Modify Provisioned Resource	Y	Admin	Y
	Enable Provisioned Resource	Y	Admin	Y
	Disable Provisioned Resource	Y	Admin	Y
	De-Provision Resource	Y	Admin	Y
	Self Modify Provisioned Resource	N	Self	Y
	Self De-Provision Resource	Y	Self	Y
Role Management	Create Role	N	Admin	N
	Delete Role	Y	Admin	N
	Modify Role	N	Admin	Y

Table 10 2   (Cont.) Default Operations and Request Models

Catalog	Request Model	Bulk	Self or Admin	Beneficiary
	Assign Roles	Y	Admin	Y
	Remove from Roles	Y	Admin	Y
	Self-Assign Role	Y	Self	Y
	Self-Remove Role	Y	Self	Y

> **Note:**   For the Create Role, Delete Role, and Modify Role request
> models, request creation is supported only by using APIs and not
> from the UI.

In Table 10 2, the Bulk column indicates the request models for which bulk operations
are supported. A bulk request is a request with multiple beneficiaries, multiple target
entities, or both. For example, a request to provision multiple roles to user John Doe
generates a bulk request. A provisioning request to add users John Doe and Jane Doe
to the Managers group also generates a bulk request.

A request model is an XML file that specifies how the request must flow after
submission, what approvals are required, and what data is required from the
requester. It contains the following information:

- Name of the model

- Whether or not a beneficiary is required:

   The requests in which a resource is provisioned to a user have a beneficiary.
   An example of this type of request is a request to create an entity and a
   relationship between a user or organization with that entity. Specifically the
   relationship is a 'has a' relation.

   Requests such as creating a user require creation of an entity, but they do not
   necessarily have a "has a' relation with any other entity.

- The beneficiary type that is being addressed, which is user.

- The entity-type that the model is associated with and whether or not the entity is a
   generic one.

   A generic entity type is a parent entity type for which the creation of entities is
   not possible unless a specific subtype is selected. For example Resource is a
   generic entity, where E-mail and Laptop are subtypes.

   If the entity type can be created without defining subtypes, then it is not a
   generic entity, such as user.

- Whether or not the model is a creation model. A creation model results in the
   creation of an entity. It creates an entity and its relation with a user or organization
   if the model has a beneficiary. A non-creation model requires a target entity to be
   selected.

- Reference to data collection. A model contains an implicit connection to an XML
   element to determine the data that needs to be collected. For a generic entity, the
   final reference is constructed by using the entity subtype selected at runtime,
   which allows the collection of different data for different entity subtypes.

- Approval workflow selection. A model may contain a reference to the algorithm(s) that are used to select the approval process to be associated for a request. The parameters to be passed to the algorithm are also mentioned.

- Whether or not the model supports an operation that is to be performed in bulk mode.

- Whether or not authentication is required. If true, then a model is available to all authenticated users creating requests. If false, then it is only available through unauthenticated self service, and not available in the authenticated self service.

10.4 Creating Requests for Self and Others

A user logged in to Oracle Identity Manager can create requests from Self Service and Advanced Administration . This section describes how to create requests by using Oracle Identity Manager Self Service in the following topics:

- Creating a Request to Register Yourself in Oracle Identity Manager
- Creating a Request From Welcome Page of Oracle Identity Manager Self Service
- Creating a Request By Using the Authenticated Oracle Identity Manager Self Service

10.4.1 Creating a Request to Register Yourself in Oracle Identity Manager

Using the login page of Oracle Identity Manager Self Service, you can create a request to register yourself in Oracle Identity Manager. This is called a Self-registration request and can be raised by users not present in Oracle Identity Manager (anonymous users).

To create a Self-registration request:

1. In the login page of Oracle Identity Manager Self Service, click **Register**. The Step 1: Basic Information page of the User Registration wizard is displayed.

2. Enter first name, last name, and e-mail ID in the respective fields, and then click **Next**. The Step 2: Login and Security Information page is displayed.

3. In the Select a User ID and Password section, enter login ID and password, and confirm the password in the respective fields.

4. In the Set your Challenge Questions and Answers section, select challenge questions and enter answers for the questions. These questions and answers are used if you forget your password and need to reset it.

5. Click **Register**. A confirmation page is displayed stating that the registration request is created. This page displays a request tracking number that you can use to check the status of your request.

6. Click **Track Registration** to track the self registration requests.

10.4.2 Creating a Request From Welcome Page of Oracle Identity Manager Self Service

Using the Welcome page of Oracle Identity Manager Self Service console, a logged in user can create requests for self or for others if authorized.

To create a request from the Welcome Page of Oracle Identity Manager Self Service:

1. In the Welcome page of Oracle Identity Manager Self Service, click **Create Request**. The Request Beneficiary Selection page is displayed.

2. Select **Request for Me** or **Request for Others** and click **Next**. The Select Request Template page is displayed.

> **Note:**
>
> ■ If "Request for Me" option is selected, all templates related to Self request types which are accessible to you are displayed.
>
> ■ If "Request for Others" option is selected, all templates related to non-Self request types which are accessible to you are displayed. If there are no such templates, you cannot create request with this option.

3. From the Request Template list, select the type of request and click **Next**. The Enter Details page is displayed.

4. From the available details list, enter last name and select Organization, Design Console Access, and User Type and then click **Next**. The Enter Justification page is displayed.

5. Enter the date and the justification for creating the request and then click **Finish**. The Request ID is created and displayed.

6. Click on the Request ID. The request details are displayed.

10.4.3 Creating a Request By Using the Authenticated Oracle Identity Manager Self Service

When you click Requests on the top of Oracle Identity Manager Self Service, the My Requests form is displayed.

In the My Requests form, you can search for requests by using the fields in the Search Requests section. A table is displayed in the form that lists the requests raised by you or the requests raised for you.

Table 10 3 lists the columns in the table that shows request information:

Table 10 3   Columns in the Table Showing Request Information

Column	Description
Request Type	The type of the request or the operation to be performed by raising the request
Request ID	A unique ID to identify the request
Status	A descriptive indication of the state the request is currently in
Date Requested	Date and time when the request was raised
Requestor	The user or the system component that created and submitted the request

To create a request:

1. From the Actions list, select **Create Request**. The Request Beneficiary page is displayed.

2. Select **Request for Me** or **Request for Others** and click **Next**. The Select Request Template page is displayed.

> **Note:**
>
> - If "Request for Me" option is selected, all templates related to Self request types which are accessible to you are displayed.
>
> - If "Request for Others" option is selected, all templates related to non-Self request types which are accessible to you are displayed. If there are no such templates, you cannot create request using this option.

3. From the Request Template list, select the type of request and click **Next**. The Enter Details page is displayed.

4. From the available details list, enter last name and select Organization, Design Console Access, and User Type and then click **Next**. The Enter Justification page is displayed.

5. Enter the date and the justification for creating the request and then click **Finish**. The Request ID is created and displayed.

6. Click on the Request ID. The request details are displayed.

In the My Requests form, you can also withdraw a request by selecting the request, and then selecting **Withdraw** Request. For more information about withdrawing requests, see "Withdrawing a Request" on page 10-20".

In the My Requests form, when you click the link in the "Request ID" column, the request details are displayed for that request. For information about the Request Details page and the operations that you can perform in this page, see "Searching for Requests" on page 10-14.

You can also create requests from the "My Profile" page in Oracle Identity Manager Self Service. The following request types are allowed:

- **Requesting roles:** See "Requesting Roles" on page 8-3 for details.

- **Removing roles:** See "Removing Roles" on page 8-4 for details.

- **Requesting a resource:** See "Requesting a Resource" on page 8-5 for details.

- **Modifying a resource:** See "Modifying a Resource" on page 8-6 for details.

- **Removing a resource:** See "Removing a Resource" on page 8-7 for details.

10.5 Searching for Requests

Using Oracle Identity Manager Self Service, various roles perform request searching and tracking:

- Request Search as a Requester

- Request Search as a Beneficiary

- Request Searching by Approver

- Request Searching by Unauthenticated User

10.5.1 Request Search as a Requester

As an authenticated user, you can view the requests raised by you in the Requests tab of Oracle Identity Manager Self Service. When you click Requests, the My Requests

form is displayed with a search facility and a list of requests that you raised. You can search for the following:

- **Requests Raised By Me:** Returns requests created by logged-in user
- **Requests Raised For Me:** Returns requests where login user exists as beneficiary or target user

In the Search Requests section of the Requests form, you can search for requests based on request ID, request type, status, start date, and end date. You can also sort the requests based on the Request ID.

> **Note:** Sorting on Request ID is string based and not number based.

The search results are displayed in a table. From the Show list, you can select Requests Raised By Me to display the requests for which you are the requester. Otherwise, select Requests Raised for Me to display the requests for which you are the beneficiary.

When you select a request in the table, the Request Details tab is displayed with detailed information about the request, as shown in Figure 10 4:

Figure 10 4   The Request Details Tab

The Request Details page displays the details of the request in the Request Information section. In addition, the following tabs display details associated to the request:

- Role/Resources/Users
- Request Comments
- Request History
- Approval Tasks

10.5.1.1 Role/Resources/Users

The Role tab is displayed only for the requests that are associated with Role Management models. If the request type is associated with provisioning, then the

Resource tab is displayed. If the request type is associated with user Management, then Users tab is displayed.

The Role tab shows the beneficiary and the role display name. For a bulk request, the table in this tab displays all the beneficiary and role names corresponding to each beneficiary, as shown in Figure 10 5:

Figure 10 5   The Role Tab

10.5.1.2 Request Comments

This tab shows the comments associated with the request, if any. You can see all the comments that might be added at various stages of the request life cycle and also add new comments. For example, the requester may add a comment before withdrawing the request, an administrator may add a comment before closing the request, an approver or requester may add comments as a part of attaining approvals.

10.5.1.3 Request History

This tab displays the request history, which consists of various changes the request has been through in the process of execution. Request history shows or tracks only the status changes to an request. The table in this tab shows the status of the request, the date on which the request is updated, and the user who updated the request, as shown in Figure 10 6:

Figure 10 6   The Request History Tab

10.5.1.4 Approval Tasks

This tab shows all Approval Tasks (pending or completed) that are associated with the request.

10.5.2 Request Search as a Beneficiary

To view the requests for which you are a beneficiary:

1. Log in to Oracle Identity Manager Self Service.

2. Click **Requests**. The My Requests form is displayed.

3. From the View Requests list, select Raised For Me, and then click Apply. The requests raised for you are displayed in a table as shown in Figure 10 7:

Figure 10 7 Requests Raised For You

4. Select a request to display detailed information about the request in the Request Details tab.

In the My Requests form, you cannot perform any action on the requests as a beneficiary, except for withdrawing the request. See "Withdrawing a Request" on page 10-20 for more information about withdrawing requests.

10.5.3 Request Searching by Approver

As an approver, you can view the requests waiting for your approval in the All Tasks section of Oracle Identity Manager Self Service. Figure 10 8 shows the Approvals tab of the All Tasks section:

Figure 10 8   The Approvals Tab
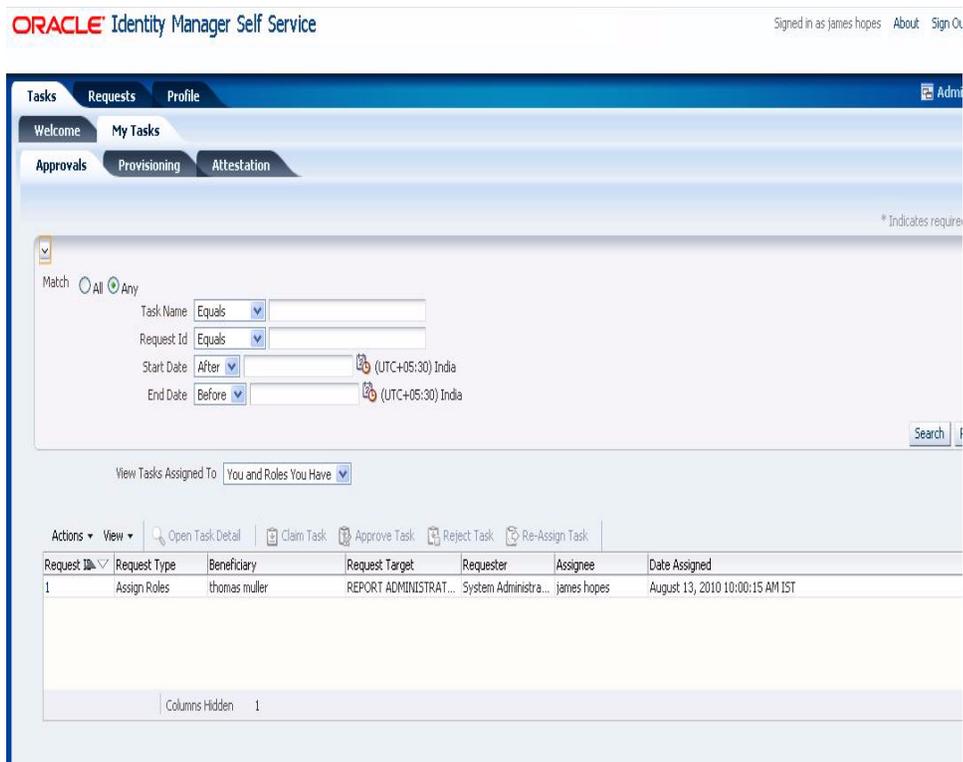
In the Search Tasks section of the Approvals tab, you can search for requests based on task name, start date, and end date. The search results are displayed in a table, as shown in Figure 10 8. From the View Tasks Assigned To list, you can select the following:

■   You Only: To sort only the requests assigned to you

■   Roles You Have: To sort the requests assigned to the roles of which you are a member

■   You and Roles You Have: To sort the requests assigned to you and to the roles of which you are a member

■   Users You Manage: To sort the requests assigned to the users you manage

When you select a request from the search results table, the Task Details page is displayed with detailed information about the request, as shown in Figure 10 9:

Figure 10 9   The Task Details Page
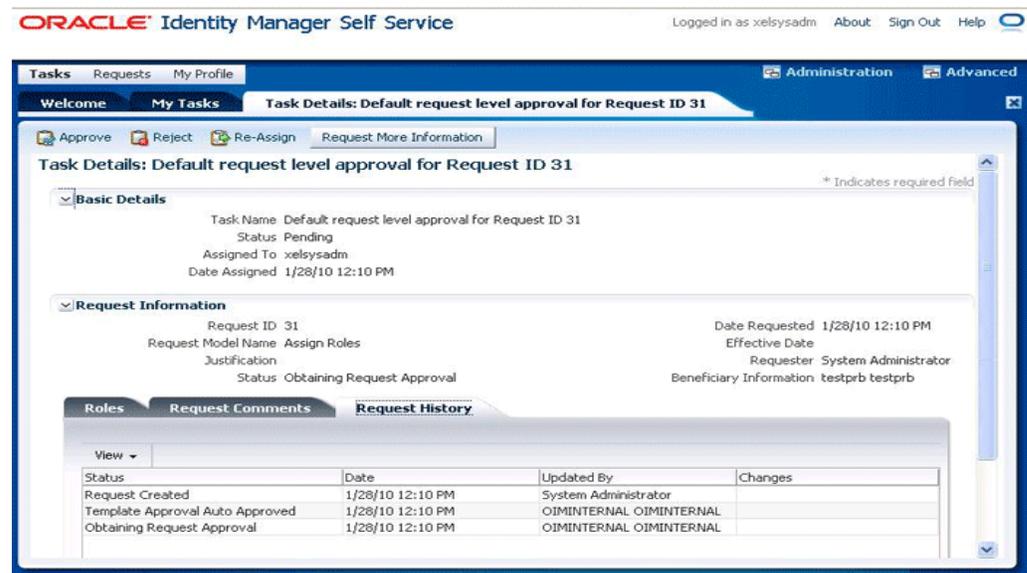
The request details are displayed in the Basic Details and Request Information sections.

If some attributes are marked as approver in request type/dataset, then there will be an additional section called "Additional Data From Approver". It is in this section, where approver can provide data, without which the approver will not be allowed to approve a request. In the next level of approval, the approver can modify the data, if required.

Similarly, if the approver send a task to a user for additional information, then task details of the received user will have an additional section called "Additional Request Information". It is in this section, where a received user can provide the information requested.

In addition, the following tabs display details associated to the request:

- Resources or User or Role: The Resources tab is dynamically generated based on the request type. It displays a list of beneficiaries, name of the target resources, and links to view the details about the target resources.

  The User tab shows the user details that is part of a request. For example, in case of CreateUser, User tab displays the user name and "View Details" link will provide the attributes of the user provided during the request creation.

  The Role tab shows the role details that is part of a request. For example, it can be a role name that you want to add or remove.

- Request Comments: This tab displays any comment or justification provided with the request. The comments recorded are questions and responses for Request for Information. For example, the comments that an approver requests for additional information from the user and the response provided by the user to those queries are recorded in this section.

- Request History: The various changes the request has already been through in the process of execution

From the All Tasks and the Request Details tabs, you can perform request operations, such as approving, rejecting, and reassigning requests. For detailed information about these procedures, see "Chapter 9, "Managing Tasks".

10.5.4 Request Searching by Unauthenticated User

As an unauthenticated user, you can only track the request for self-registration. After you create and submit a self-registration request, a request ID is displayed. You can use this request ID to track the request.

> **See Also:** "Tracking Registration Requests" on page 7-4 in the "Unauthenticated User Self Service" chapter for information about tracking a self-registration request

10.6 Withdrawing a Request

A request can be withdrawn by the requester and only the requests that have not started the execution phase can be withdrawn. Also, beneficiaries cannot withdraw requests. Requests having the following stages can be withdrawn:

- Obtaining Request Approval

- Obtaining Operation Approval

- Approved

To withdraw a request:

1. In Oracle Identity Manager Self Service, click **Requests**.

2. In the Requests form of Oracle Identity Manager Self Service, select the request that you want to withdraw.

3. From the Actions list, select **Withdraw Request**.

4. Click **OK** in the confirmation message box. The request is withdrawn and a notification is sent to the beneficiary and requester of the request.

10.7 Performing Request-Related Tasks by Using the Task List

For more information about request-related tasks, such as approving a request, claiming a task, requesting for more information, submitting information, rejecting a task, and reassigning a task using the Task List, see "Viewing Task Details" on page 9-3 in the "Authenticated User Self Service" chapter.

10.8 Closing Requests

Request Administrators (users with Request Administrators role) can prematurely close any request that has not started the execution phase. This includes all requests waiting for approvals or has completed approvals but no operation has been started. Requests with the following state can be closed:

- Obtaining Template Approval

- Obtaining Request Approval

- Obtaining Operation Approval

- Approved

> **Note:**
>
> - The requester or the beneficiary of a request cannot close the request.
>
> - If a request is closed while the request is in the Obtaining Approval stage, then all the approvals that are still pending in the approver task list are removed.

To close a request:

1. Go to Oracle Identity Manager Advanced Administration.

2. In the left pane of the Requests section, search for the request that you want to close.

3. From the search results table, select the request.

4. From the Actions list, select Close Request. The Close Request dialog box is displayed.

5. Enter a reason for closing the request, and then click **Close Request**. A message box is displayed asking for confirmation to close the request.

6. Click **OK** to confirm. A notification that the request is closed is sent to the requestor and target user for this request.

Part III

Identity Administration

This part describes Oracle Identity Manager delegated administration functionalities by using the identity administration features.

It contains the following chapters:

11

Managing Users

The user management feature in Oracle Identity Manager includes the creation, updation, deletion, enabling and disabling, locking, and unlocking of user accounts. This feature is described in the following sections:

- User Lifecycle

- User Entity Definition

- User Management Tasks

- User Management Authorization

- Username Reservation

11.1 User Lifecycle

User lifecycle is a term to describe the process flow of how a user entity is created, managed, and terminated in the system based on certain events or time factors.

A user entity goes through various stages in the lifecycle. The stages are non-existent, disabled, active, and deleted. Figure 11–1 depicts the different lifecycle stages, all possible transitions, and the operations that set up those transitions:

Figure 11–1   User Life Cycle
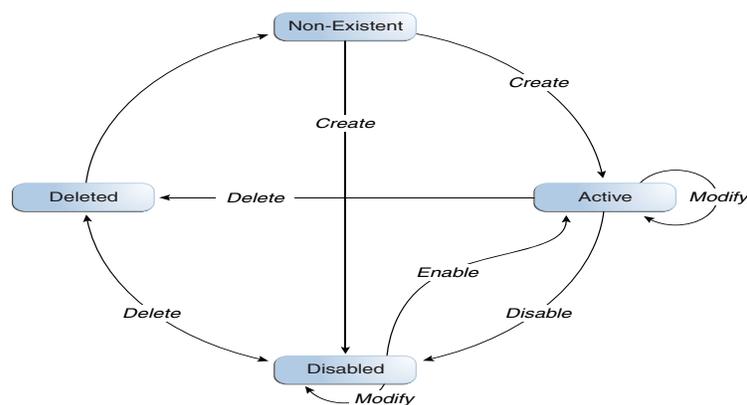
There is a possibility of process rules or business requirements being defined for each transition of the user lifecycle. You can use the sample scenarios listed in Table 11–1 to establish the link between user lifecycle transitions and business objectives.

Table 11–1 User Life Cycle and Business Objectives Sample Scenarios

Current State	Operation	Sample Scenario	Process Description
Non-existent	Create	HR enters user profile information for a new hire. If the new hire is not introduced to the system immediately, then HR sets a future start date for the user.	If the start is not a future date then the user is introduced into the system in an Active state. If the Start Date is in future then the create process creates the user in a disabled state.
Disabled	Enable	User's start date is in effect. The system initiates provisioning for the new hire.	User is marked enabled in the system and the user is now able to login and use the system. By default, all necessary memberships and accounts are established as part of the workflow.
Active	Modify	User is promoted to a new position. As a result, HR changes the job title of the user.	New resources are provisioned to the user, and old irrelevant resources are deprovisioned from the user.
Active	Disable	User takes one year sabbatical from the company. HR manually disables the user on the last working day of the user. The user re-joins the company after some period. HR can make the user Active again.	User is marked disabled in the system, and the user is no longer able to login to the system. The disabled users can be made Active again.
Active	Deleted	User retires from the company. HR manually disables the user on the last working day of the user.	User is marked disabled in the system, and the user is no longer able to login to the system. By default, all users' accounts are deprovisioned as part of the workflow.

The following concepts are integral to user lifecycle management:

- OIM Account
- Organization
- Role

11.1.1 OIM Account

OIM Account is an abstraction representing a means to be authenticated to access Oracle Identity Manager. In Oracle Identity Manager, the cardinality of relationship between user and OIM account is one-to-one. By default, users are associated with OIM accounts that allows users to access Oracle Identity Manager. However, there may be users who do not need to access Oracle Identity Manager, and therefore, may not be provisioned with an OIM account.

Some user operations, such as lock and unlock, are explicitly account operations. When locking or unlocking a user, you lock or unlock the user's OIM account.

In Oracle Identity Manager, each user has a Design Console Access attribute that controls the OIM account of the user. If the Design Console Access option for a user is

selected in the UI, then the user is End-User Administrator. If this option is not selected, then the user is an End-User.

11.1.2 Organization

Organization is a logical container for authorization and permission data. A user in Oracle Identity Manager must belong to one organization only. For detailed information about organizations in Oracle Identity Manager, see Chapter 13, "Managing Organizations".

11.1.3 Role

Oracle Identity Manager provides easy and controlled privilege management through roles. Roles are named groups of related privileges that you grant to users or other roles. Roles are designed to ease the administration of end-user system and schema object privileges. For detailed information about roles, see Chapter 12, "Managing Roles".

11.2 User Entity Definition

Attributes are defined for the user entity in Oracle Identity Manager. You can add your own attributes to the user entity.

For each attribute for a user entity, the following properties are defined in Oracle Identity Manager:

- **Attribute Name:** The name of the attribute.
- **Category:** All entity attributes are classified into a category. This categorization is used to organize the data in the UI. The category is only for display on the UI and is not used anywhere else. The default categories are:
  - Basic User Information: This category contains basic user attributes such as user first name, user last name, e-mail, manager, organization, and user type.
  - Account Settings: This category contains account-related attributes such as user login, identity status, account status, and global unique identifier (GUID).
  - Account Effective Dates: This category contains account start and end date attributes.
  - Provisioning Dates: This category contains provisioning date and deprovisioning date attributes.
  - Lifecycle : This category shows flags related to User Account such as anuallym locked, locked on , automatically delete on.

    All the attributes in the category are hidden by default so the category is also not visible.
  - System: This category contains the system controlled attributes for the user entity such as created on, password expiration date, password reset attempts, and so on.
  - Other User Attributes: This category contains a list of all the FA and LDAP related attributes.
  - CustomAttributes: This is an empty category where the user can add all the new custom attributes.

- Preferences: This category contains the attributes related to user preferences. It contains various attributes such as locale, timezone, currency, date format, and so on.

- **Data Type:** Indicates the type of data in the attribute. Supported types are Text, Numeric, Date, and Boolean.

- **Properties:** For each attribute, the following properties can be defined:

  - Required: Determines whether or not every user in the repository must have a non-null value for this attribute

  - System Controlled: Determines if the value can only be set and edited by the system itself

  - System Can Default: Determines if the value can be set by the system to a default if no value is provided

  - Encrypted: Determines if the value stored in the repository is encrypted. If true, then the value is encrypted but this encrypted value can be decrypted producing the original value. If false, then the value is stored clear, meaning that the stored value is not encrypted.

  - Searchable: Determines if the values can be used in searches

  - Support Bulk Update: Determines if the field can be modified as part of a bulk modification of multiple users. Fields that are expected to be unique to users, such as username, name fields, and password, do not support bulk update. For fields with System Controled=Yes or Unique=Yes, this property can never be set to Yes. For information about setting the properties of an attribute, see "Configuring User Attributes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

  - Display: Determines how the field is displayed in the UI for creating and modifying users. It can have any one of the following values:

    TEXT, TEXTAREA, NUMBER, DOUBLE, CHECKBOX, DATE_ONLY, SECRET, LOV, and ENTITY.

  - Multi-valued: Determines whether the attribute is multi-valued or not. The value of this property is either true or false. Oracle Identity Manager does not support multiple values, and therefore, this property is set to false for all user attributes.

  - Max Size: Indicates the maximum allowed length for the specified attribute.

  - Read Only: Indicates if the attribute has "read-only" permission only or if it is editable.

- **Dependency:** The value of some attributes can depend on the value of other attributes. The Dependency property lists the other attributes that this attribute depends on. If any of those attributes are changed, then the auto-generate or pre-populate adapters for this attribute is started.

- **LOV:** The list of values (LOV) is provided for a field. You can modify the list of available values if the LOV is marked as configurable. For other LOVs, you cannot add your own values. For some LOVs, the list of values are system defined.

Table 11–2 lists the attributes defined for the user entity in Oracle Identity Manager:

Table 11–2   Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
User Login	Account Settings	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
First Name	Basic User Information	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Middle Name	Basic User Information	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Last Name	Basic User Information	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Generation Qualifier	Other User Attribute	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	System LOV (configurable)
Display Name	Basic User Information	Single	Text	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Initials	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Description	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
User Type	Basic User Information	Single	Text	Required: Yes System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	System LOV (Configurable) Full-Time Part-Time Contractor
Employee Number	Other User Attributes	Single	Text	Required: No System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Organization	Basic User Information	Single	Reference	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	API-based
Department Number	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Title	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Manager	Basic User Information	Single	Reference	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	API-based
Hire Date	Other User Attributes	Single	Date	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	NA
Start Date	Account Effective Dates	Single	Date	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
End Date	Account Effective Dates	Single	Date	Required: No System Controlled: No System Can Default: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	NA
Identity Status	Account Settings	Single	Text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	Active Disabled Deleted Disabled Until Start Date

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Account Status	Account Settings	Single	Text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	Locked/Unlocked
Design Console Access	Basic User Information	Single	Check Box	Required: Yes System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	True/False
Account Locked	Lifecycle	Single	Boolean	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Account Locked On	Lifecycle	Single	Date	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: No Support Bulk Update: No	NA
Manually Locked	Lifecycle	Single	Boolean	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: No Support Bulk Update: No	NA
Password	Account Settings	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Encrypt Searchable: No Unique: No Support Bulk Update: No	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Password Generated	Account Settings	Single	Text	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: No Support Bulk Update: No	NA
Email	Basic User Information	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
Home Postal Address	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Postal Address	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Street	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Postal Code	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
PO Box	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Locality Name	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
State	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Country	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Fax	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
House Phone	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Mobile	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Pager	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Phone	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Locale	Preferences	Single	Text	Required: No System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	System LOV
Language	LDAP Attributes	Single	Text	Required: No System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	System LOV
Time Zone	Preferences	Single	Text	Required: No System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	System LOV

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
UID	Account Settings	Single	Numeric	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
LDAP Organization	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
LDAP Organization Unit	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
LDAP DN	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Common Name	Other User Attributes	Single	Text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Provisioning Date	Provisioning Dates	Single	Date	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
De-provisioning Date	Provisioning Dates	Single	Date	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	NA
Provisioned Date	System	Single	Date	Required: No System Can Default: No System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
De-provisioned Date	System	Single	Date	Required: No System Can Default: No System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Login Attempts	System	Single	Numeric	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: No Support Bulk Update: Yes	NA

Table 11–2   (Cont.) Attributes Defined for User Entity

Attribute Name	Category	Type	Data Type	Properties	LOV (Default attributes are in bold)
Automatically Delete On	Lifecycle	Single	Date	Required: No System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: No Support Bulk Update: No	NA
Created On	System	Single	Date	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Updated On	System	Single	Date	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

11.3 User Management Tasks

You can perform the following user management tasks in the Oracle Identity Administration:

- Searching Users
- Creating Users
- Viewing and Modifying User Information

11.3.1 Searching Users

In Oracle Identity Manager Administration, you can perform the following types of search operations for the user entity:

- Simple Search
- Advanced Search

11.3.1.1 Simple Search

The search operation lets you search user entities based on the search strings that you specify as search attributes. This operation is also referred to as simple search or quick search.

The search feature is described in the following topics:

- Searchable Attributes
- Search Comparators
- Search String

- Conjunction Operator

- Search Results

- Operations on Search Results

- Performing a Simple Search

11.3.1.1.1 Searchable Attributes The default set of attributes across which search is conducted are:

- User Login

- First Name

- Last Name

- Display Name

11.3.1.1.2 Search Comparators The search comparator for the search operation is set to Begins With. The search comparator can be combined with wildcard characters to specify a search condition.

11.3.1.1.3 Search String Search string is not case-sensitive. Only the asterisk (*) character is supported as a wildcard for the search string. Oracle Identity Manager Administration removes any leading or trailing white spaces from the search string. For performance reasons, any leading occurrences of (*) in the search string are removed.

11.3.1.1.4 Conjunction Operator The conjunction operator for the search operation is by default set to be OR.

The relationships between the search attributes, search comparator, search string, and conjunction operator is described by using the following query composition formula:

```
Query begins with ((attribute 1 begins with 'search string') or (attribute 2
begins with 'search string') or …)
```

For example, if you enter Jo* as a search text, then the search operation forms an internal query where User Name begins with Jo* or First Name begins with Jo* or Last Name begins with Jo*. As a result, all the users whose user name, first name, or last name starts with Jo are displayed.

11.3.1.1.5 Search Results Result attributes define the set of attributes that are to be returned by the search operation. The actual set of result attributes, however, are determined dynamically based on user's permissions.

> **Note:** The search results do not include deleted users, which means users with status = Deleted.

The limited search result table shows a subset of the columns of the full search result table. User configuration specifies the columns to display in the search results, and the subset to display in the limited search result table. For more details about configuration management, see "Configuring User Attributes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

The simple search result table displays the Display Name attribute only. Here, the Display Name of all those users whose Display Name, User Login, First Name, or Last Name attribute value equals search text are displayed in the search result.

You can perform sorting and paging of the displayed data in the search results table.

> **Tip:** When you scroll up or down, the page index changes. Each page contains a fixed set of entries. When page index changes and the next required page is not within the UI, the UI triggers an event. As a response to this event, the result page is displayed.
>
> There are up and down arrows provided on each attribute in the search result table. Clicking the up or down arrow of the attribute provides with the sort attribute and sorting order.

11.3.1.1.6 Operations on Search Results This section describes the operations that you can perform based on selection of row(s) in the search results table. It is divided into single selection operations and bulk or multiple selection operations.

You can perform the following single selection operations by selecting a user from the search results table:

- View detail
- Bulk modify, only if the user status is deleted
- Enable, only if the user status is enabled
- Disable, only if the user status is disabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Reset password
- Delete

You can perform the following bulk or multiple selection operations by selecting multiple users from the search results table:

- Enable, only if the user status is enabled
- Disable, only if the user status is disabled
- Lock, only if the selected user's account is unlocked
- Unlock, only if the selected user's account is locked
- Delete

11.3.1.1.7 Performing a Simple Search To perform a simple search and display the details of the user:

1. Login to Oracle Identity Manager Administration.

2. To search users, in the left pane, select **Users** from the drop-down list.

3. In the search field, enter a search criterion. You can include wildcard characters (*) in your search criterion.

4. Click the icon to the right of the search field. The search result is displayed in the left pane that shows the display names of the users that matches the search criterion you specified. Figure 11–2 shows the search results:

Figure 11–2   Simple Search Result

11.3.1.2 Advanced Search

The advanced search options are displayed in the right pane of Oracle Identity Manager Administration. The advance search allows you to specify more complex search criteria than the simple search criteria. The results are displayed in search results tables.

The advanced search operation is described in the following sections:

- Advanced Search Page

- Search Comparators

- Conjunction Operator

- Searchable Attributes

- Search Results

- Performing an Advanced Search Operation

11.3.1.2.1   Advanced Search Page You specify the search criteria in the Advanced Search page. This page lets you create a search query that consists of multiple criteria. Each criterion consists of:

- The attribute to search against

- The search comparator, such as equals and begins with

- The values to search for

The value can be multiple in the case where the comparator requires two or more values. You can specify multiple search criteria if the comparator requires two or more values, for example, range searches on numeric fields or data ranges on date fields. When you specify multiple search criteria, you must specify the AND or OR conjunction operator for the search operation.

11.3.1.2.2   Search Comparators The search comparators that the Advanced Search page supports are predefined in Oracle Identity Manager. Each comparator specifies the kind of attribute (data type) it supports, and also the number of input data fields it requires.

Table 11–3 lists the comparators supported by advanced search:

Table 11–3   Advanced Search Comparators

Comparator	Field Types Supported
Equals	Text, Date, Numeric, Boolean

Table 11–3   (Cont.) Advanced Search Comparators

Comparator	Field Types Supported
Begins With	Text

11.3.1.2.3   Conjunction Operator The conjunction operators for the search operation are:

- **All:** Search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

- **Any:** Search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

11.3.1.2.4   Searchable Attributes Searchable attributes define the set of attributes that you can use in the Advanced Search page. While creating the search criteria, you can select the attributes that you want to search against from this base list.

Only a subset of the searchable attributes, called default fields in Table 11–4, is displayed by default in the Advanced Search page. You can add additional searchable attributes to the page by using the Add Fields functionality. Each attribute also specifies the comparators it supports.

Table 11–4   Default Search Attributes

Attribute	Comparators Available	Default Fields
Display Name	Begins With, Equals	Yes
User Login	Begins With, Equals	Yes
First Name	Begins With, Equals	Yes
Last Name	Begins With, Equals	Yes
Identity Status	Equals, Not Equals	Yes
Organization	Equals, Begins With	Yes
Email	Begins With, Equals	Yes
Start Date	Equal, Before, After, Range	Yes
End Date	Equals, Before, After, Range	Yes

> **Note:**   You can configure the attributes that are searchable in User Management Configuration.
>
> The searchable attributes configured for advanced search must be a subset of the attributes defined for the User Entity that are marked with the Searchable = Yes property.

11.3.1.2.5   Search Results The search results table is displayed in the same tab as the Advanced Search page so that the user can view the query they searched by along with the search results. The table, being in the right pane, is always displayed as the full search results table.

If your search returns a lot of information, you can hide one or more columns in the search results table. For example, if your table contains 20 columns, you might want to display only the eight most-important columns, so you do not have to keep scrolling through the less important information.

To hide one or more columns, open the Search Results pane, click View, and deselect the columns you want to hide. A status message displays along the bottom of all search tables to identify how many columns are currently hidden in a particular table view. Figure 11–3 shows that the user has hidden three columns.

Figure 11–3   Advanced Search Result with Hidden Columns

The search results does not return deleted users, unless the user explicitly selects the Status attribute in the Advanced Search page and provides a value, Status Equals Deleted. In that case, deleted users will be returned as part of the search results.

11.3.1.2.6   Performing an Advanced Search Operation   To perform an advanced search operation and display the search result:

1.   In the Welcome page of Oracle Identity Manager Administration, under users, click **Advanced Search - Users**. Alternatively, you can click **Administration**, and under the Browse tab, click the **Advanced Search: Users**.

2.   Select All or Any conjunction operator. For information about these operators, see "Conjunction Operator" on page 11-18.

3.   Specify a search criteria in the fields. You can include wildcard characters (*) in your search criterion. For performance reasons, initial (prefix) wildcards will be removed. Select the search comparators in the lists adjacent to the fields. See Table 11–3, " Advanced Search Comparators" for information about the advanced search comparators.

> **Note:**   The asterix wildcard character (*) search for the Identity Status field returns only the users with Active , Disabled, and Disabled Until Start Date statuses, but not with Deleted status. To search for users with Deleted status, you must enter Deleted in the Identity Status field.

To add a field in the search criteria, click **Add Fields**, and then select the field name from the list.

4.   Click **Search**. The user records that match your search criteria are displayed in the search results table, as shown in Figure 11–4:

Figure 11–4 Advanced Search Result

11.3.2 Creating Users

You can create a new user in Oracle Identity Manager by using the Create User page. You can open this page only if you are authorized to create users as determined by the authorization policy on the Create User privilege on any organization in Oracle Identity Manager.

To create a user:

1. Login to Oracle Identity Manager Administration.

2. Open the Create User page. To do so, perform any one of the following:

   - In the Welcome page, under Users, click **Create Users**.

   - Click the **Administration** tab on the tool bar, and in the Welcome page, under Users, click **Create Users**.

   - Click the **Search Results** tab, and from the Action menu, select **Create User**.

   - In the Search Results tab, click the **Create User** icon on the toolbar.

   The Create User page displays input fields for user profile attributes. The attributes that are displayed in the create user page are determined by the configuration of the Create User page in User Management Configuration. In this configuration, each of the attributes defined for the user entity is marked as being available on the Create User page.

   > **See Also:** "Configuring User Attributes" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for information about configuring the Create User page

3. Enter details of the user in the Create User page. Table 11–5 describes the fields in the Create User page:

Table 11–5   Fields in the Create User Page

Section	Field	Description
Basic User Information	First Name	First name of the user.
	Middle Name	Middle name of the user.
	Last Name	Last name of the user.
	Design Console Access	The user of OIM User type. It can have one of the two possible values, End-User and End-User Administrator. The OIM User type tells whether or not the user can log in to Oracle Identity Manager Design Console. If the "Design Console Access" check box is selected, the user type will be "End-User Administrator" and the user will have access to design console.
	Email	E-mail address of the user.
	Manager	The reporting manager of the user.
	Organization	The organization to which the user belongs to.
	User Type	The type of employee, such as full-time employee, intern, contractor, part-time employee, consultant, or temporary.
	Display Name	The display name of the user. It can have two values, Localized Display Name and Manage Localizations. You can add the localization languages by clicking on Manage Localizations.
Account Settings	User Login	The user name to be specified for logging in to the Administration Console.
	Password	The password to be specified for logging in to the Administration console.
	Confirm Password	The password to be re-entered for confirmation.
Account Effective Dates	Start Date	The date when the user will be activated in the system.
	End Date	The date when the user will be deactivated in the system.
Provisioning Dates	Provisioning Date	Date when user is getting provisioned into the system.
	Deprovisioning Date	Date when the user is getting deprovisioned from the system.
Other User Attributes	Country	The country where user resides.
	Department Number	The department number of the user.
	Common Name	The common name of the user.
	Employee Number	The employee number of the user.
	Fax	The fax number of the user.
	Generation Qualifier	Whether the user qualifies the generation.
	Hire Date	The hiring date of the user.

Table 11–5 (Cont.) Fields in the Create User Page

Section	Field	Description
	Home Phone	The home phone number of the user.
	Locality Name	The name of the locality where user resides.
	Mobile	The mobile number of the user.
	Pager	The pager number of the user.
	Home Postal Address	The house address of the user.
	Postal Address	The postal address of the user.
	Postal Code	The postal code number of the user's address.
	PO Box	The post box number of the user's address.
	State	The state name of the user.
	Street	The street name where the user resides.
	Telephone Number	The telephone number of the user's residence.
	Title	The title for the user.
	Initials	The initials of the user.

You can enter attribute values in more than one language in the pages for creating or updating entities, such as users, organizations, and roles.

4. After you enter the user information, click **Save** to create the user.

> **Tip:** Users can be created by any one of the following methods:
>
> - By using Oracle Identity Administration
> - By self registration
> - By creating a request
> - By using SPML Web service or APIs
>
> For all the above methods, Oracle Identity Manager uses the default password policy or Password Policy against Default Rule. If you want to use a different password policy, then you must attach the new password policy to the default rule by using the Design Console. To do so, see "Managing Password Policies" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

11.3.3 Viewing and Modifying User Information

The view user operation allows you to view detailed user profile information in the User Detail page. You can open this page if you are authorized to view the user's profile as determined by the authorization policy through the View User Details privilege. If you have the authorization to modify the user, then you can modify the user by using this page.

To display user details, perform any of the following:

- Click the user login link in the search results table for simple search.

- Select a record in the user search results table for both simple and advanced search, and then select **Modify User** from the Actions menu. Alternatively, you can click **Modify User** on the toolbar.

The viewing and modifying operations are described in the following sections:

- User Details Page
- User Modifications
- Single User Operations
- Bulk User Modifications

11.3.3.1 User Details Page

The user details page for the user entity is auto-generated based on configuration and authorization. This page is divided into the following tabs:

- The Attributes Tab
- The Roles Tab
- The Resources Tab
- The Proxies Tab
- Direct Reports
- The Requests Tab

11.3.3.1.1 The Attributes Tab

This tab displays the attribute profile that includes details about basic user information, account settings, and other user attributes. You can modify any field to change the attribute profile information, and click **Apply**.

To eliminate the changes made in this page, click **Revert**.

11.3.3.1.2 The Roles Tab
This tab displays a list of roles to which the user belongs. You can click each role to display summary information about the role. For each role in the list, it displays the following:

- **Display Name:** The name displayed on the UI.
- **Role Name:** Name of the role assigned to a user.
- **Role Namespace**: Namespace to which the role is assigned.
- **Description:** A description of the role.

In the Roles tab, you can assign roles to the user and remove roles from the user. For more details, see "Adding and Removing Roles" on page 11-25.

11.3.3.1.3 The Resources Tab
This section displays a list of resources that a user has been provisioned. For each resource in the list, it displays the following:

- **Resource Name:** Name of the resource assigned to a user
- **Request ID**: If the provisioned instance is associated with a request
- **Service Account:** Yes if the account was provisioned as a service account, otherwise No.
- **Description**: If any, for the provisioned instance
- **Type:** The type of resource

- **Status:** The status of the resource such as Provisioned, Enabled, or Disabled

- **Provisioned On:** The date when the resource was provisioned to the user

11.3.3.1.4 The Proxies Tab This tab displays all proxies that are currently set up for the user. For each proxy in the list, it displays the following:

- **Proxy Name:** The display name of the proxy user

- **Start Date:** The start date for the proxy user

- **End Date:** The end date for the proxy user

- **Status:** The status of the proxy user

- **Relationship:** The relationship of the proxy user with the open user, such as manager

- **Last Updated:** The date when the proxy user was last updated

This section also displays the history of proxy information for the user in which the end date is shown. The **Current Proxies** display the current proxies for the user. The **Past Proxies** display the proxies history for the user. The Status column is not displayed in the Past Proxies table.

If you select a row in the table that displays proxies information, then a summary information about the proxy is displayed where you can edit the proxy name, relationship with the user, start date, and end date.

The Proxies tab allows you to add proxies to the user and to remove proxies from the user. For information about adding and removing proxies, see "Modifying Proxy Details" on page 11-28.

11.3.3.1.5 Direct Reports This tab displays a read-only table of users for whom the user is set as the manager. In other words, this tab lists the direct reportees of the user. For each user in the table, it displays the following:

- Display Name

- User Login

- Status

- Organization

If you select a row in the table, then summary information about the direct reportee is displayed at the bottom.

Direct reports allows you to open the user details of the direct reportees. To do so, select a row in the table of direct reportees, and form the Action menu, select **Open User**. Alternatively, you can click **Open User** on the toolbar.

11.3.3.1.6 The Requests Tab This tab displays the requests that are raised for the user. For each request, the following details are displayed:

- **Request ID:** An ID to uniquely identify the request

- **Model Name:** The request model name

- **Status**: Shows the current state of the request

- **Requested By:** The requester who raised the request

- **Parent ID:** An ID of the parent request, if any, to which the request is a child request

■ **Date Requested:** The date on which the request is created

> **See Also:** Chapter 14, "Creating and Searching Requests" for information about requests, request types, and parent and child requests

This tab allows you to open the details of the requests by clicking the request IDs.

11.3.3.2 User Modifications

You can perform administrative user modification tasks from the user details. The modification is broken up across the different tabs in the page that displays user details, which means that modifications done in each tab are independent of each other and must be saved individually. The modifications you can perform in each tab is outlined in the following sections:

■ Modifying Attribute Profile

■ Adding and Removing Roles

■ Adding and Removing Resources

■ Enabling and Disabling Resources

■ Displaying Resource Details

■ Displaying Resource History

■ Modifying Proxy Details

11.3.3.2.1 Modifying Attribute Profile The attribute profile information is displayed in the Attributes tab of the user details page. To modify the attribute profile, edit the fields in the Attributes tab, and click **Apply**.

11.3.3.2.2 Adding and Removing Roles To add a role:

1. In the Roles tab, from the Action menu, select **Assign Roles**. Alternatively, you can click **Assign Roles** on the toolbar. The Assign Role to User window is displayed.

2. From the Search Roles list, select the type of role or role category. The default role categories are OIM Roles and Default. In addition, you can create custom role categories. See "Creating and Managing Role Categories" on page 12-24 for detailed information about role categories.

3. Search can be performed on the following fields:

   ■ Display Name

   ■ Name

   ■ Role Namespace

   Select All or any conjunction operator. For information about these operators, see "Conjunction Operator" on page 11-18.

4. Enter a search criterion in the search field. You can specify the asterix (*) wildcard character in the search criterion. Then, click the search icon. All roles that belong to the category you selected are displayed in the Available Roles list.

5. Select one or more roles from the Available Roles list (Shift + Click for contiguous row selection and Ctrl + Click for non-contiguous selection). Then click the **Move** or **Move All** buttons to move the selected roles to the Roles to Assign list.

> **See Also:** Table 12–5, " Default Roles in Oracle Identity Manager" for information about the default roles in Oracle Identity Manager

6. Click **OK**. A confirmation message is displayed and the roles you selected are assigned to the user.

The Roles tab allows you to select one or multiple roles in the list, and then allows you to remove roles. To remove a role:

1. Select the role or roles that you want to remove.

2. From the Action menu, select **Revoke Roles**. Alternatively, you can click **Revoke Roles** on the toolbar. A message is displayed asking you to confirm.

3. Click **OK**. A success message is displayed on the user details page for successful role assignment.

11.3.3.2.3 Adding and Removing Resources The Resources tab allows you to select one or multiple resources in the list, and then perform various operations, such as adding and removing resources, enabling and disabling resources, and displaying resource details and history.

To add a resource to a user:

1. In the Resources tab, from the Action menu, select **Add**. Alternatively, you can click **Add Resource** on the toolbar. The Provision Resource to User wizard is displayed.

2. In Step 1: Select a Resource page, select the resource you want to provision.

3. Click **Continue**. The Step 2: Verify Resource Selection page is displayed. This page displays the resource that you selected for provisioning to the target user.

4. Click **Continue**. The Step 3: Process Data page is displayed.

5. Enter values in the fields to specify information about the selected resource.

6. Click **Continue**. The Step 4: Verify Process Data page is displayed with details about the resource.

   Figure 11–5 shows the Step 4: Verify Process Data page with sample values for the ebusiness Suite User TCA Foundation resource to be provisioned to the user John Doe with user ID JohnD.

Figure 11–5   Sample Process Data

7. If you want to edit any information displayed in this page, click **Edit** on the top-right corner of the page. The Step 3: Provide Process Data page is displayed that allows you to edit process data. When finished, click **Continue** to go back to the Step 4: Verify Process Data page.

   After verifying all information, click **Continue**.

   > **WARNING: Make sure that you verify the process data before clicking Continue. This is because clicking Continue starts provisioning.**

8. Click **Continue** to start provisioning the selected resource to the user. A message is displayed stating that the provisioning has been started.

To remove a resource from a user:

1. In the Resources tab, select a resource that you want to remove.

2. From the Action menu, select **Remove Resource**. Alternatively, you can click **Revoke** on the toolbar. A confirmation message is displayed.

3. Click **OK**. The resource is removed, and a success message is displayed.

11.3.3.2.4   Enabling and Disabling Resources A resource can be enabled if the status of the selected resource is Disabled or Provisioned. To enable a resource:

1. In the Resources tab, select a resource that you want to enable.

2. From the Action menu, select **Enable**. A confirmation message is displayed.

3. Click **OK**. The resource is enabled, and a success message is displayed.

A resource can be disabled if the status of the selected resource is Enabled. To disable a resource:

1. In the Resources tab, select a resource that you want to disable.

2. From the Action menu, select **Disable**. A confirmation message is displayed.

3. Click **OK**. The resource is disabled, and a success message is displayed.

11.3.3.2.5 Displaying Resource Details   To display resource details:

1. In the Resources tab, select a resource whose details you want to display.

2. From the Action menu, select **Open**. A page is displayed with the resource details. You can edit resource details in this page. When finished, click **Save**.

11.3.3.2.6 Displaying Resource History   To display resource history:

1. In the Resources tab, select a resource whose history you want to display.

2. From the Action menu, select **Resource History**. A page is displayed with the provisioning details of the resource. The details include task name, task details, date assigned, and the user to whom the task is assigned. A retry checbox is also displayed. You must enable this to retry all failed tasks.

11.3.3.2.7 Modifying Proxy Details   The Proxies tab allows you to add a proxy and select one or multiple proxies in the list, and then invoke the following operations:

- Edit a proxy, only if a single user is selected

- Remove a proxy

To add a proxy:

1. In the Proxies tab, from the Action menu, select **Add**. The Add Proxy dialog box is displayed.

2. In the Proxy Name field, select an appropriate proxy. Your proxy can be any user. Search for proxy user's name from the search field below the Proxy Name field or select **Manager** to add your manager as a proxy.

3. Specify a start date and end date for the proxy to operate on your behalf.

4. Click **OK**. A message is displayed asking for confirmation.

5. Click **OK**. A confirmation message is displayed stating that the proxy is assigned.

To remove a proxy, select the proxy in the Proxies tab, and click **Remove Proxy**.

To modify proxy details:

1. Select a row in the table displaying proxy information. The details of the proxy are displayed at the bottom of the tab.

2. Edit the fields to modify proxy information.

3. Click **Save**.

11.3.3.3 Single User Operations

You can perform user management operations for a single user from the page that displays user details. These operations are:

- Enabling a User

- Disabling a User

- Locking a User

- Unlocking a User

- Resetting the Password for a User

- Deleting User

11.3.3.3.1 Enabling a User This operation is available only if the user status is Disabled. To enable a user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of Advanced Search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Enable User**. Alternatively, you can click the **Enable User** icon on the toolbar. If the user details page for the user is open, then you can click **Enable User** on the toolbar. A message box is displayed asking for confirmation.

3. Click **OK** to confirm. A confirmation message is displayed stating that the user is enabled.

    If you enable a user from the user detail page, then it's successful completion refreshes the Attributes tab. If you perform this operation from a user list, such as simple or advanced search results, then the corresponding row in the list is refreshed.

11.3.3.3.2 Disabling a User This operation is available only if the user status is Enabled. To disable a user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of Advanced Search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Disable User**. Alternatively, you can click the **Disable User** icon on the toolbar. If the user details page for the user is open, then you can click **Disable User** on the toolbar. A message box is displayed asking for confirmation.

3. Click **OK** to confirm. A confirmation message is displayed stating that the user is disabled.

    If you disable a user from the user detail page, then it's successful completion refreshes the Attributes tab. If you perform this operation from a user list, such as simple or advanced search results, then the corresponding row in the list is refreshed.

11.3.3.3.3 Locking a User This operation is available only if the user account is unlocked. To lock a user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of advanced search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Lock Account**. Alternatively, you can click the **Lock Account** icon on the toolbar. If the user details page for the user is open, then you can click **Lock Account on the toolbar**. A message is displayed asking for confirmation.

3. Click **OK**. A confirmation message is displayed stating that the user is successfully locked.

If you lock an account from the user detail page, then it's successful completion refreshes the Attributes tab. If you perform this operation from a user list, such as simple or advanced search results, then the corresponding row in the list is refreshed.

11.3.3.3.4 Unlocking a User This operation is available only if the user account is locked. To unlock as user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of advanced search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Unlock Account**. Alternatively, you can click the **Unlock Account** icon on the toolbar. If the user details page for the user is open, then you can click **Unlock Account** on the toolbar. A message is displayed asking for confirmation.

3. Click **OK**. A confirmation message is displayed stating that the user is successfully unlocked.

If you unlock an account from the user detail page, then it's successful completion refreshes the Attributes tab. If you perform this operation from a user list, such as simple or advanced search result, then the corresponding row in the list is refreshed.

11.3.3.3.5 Resetting the Password for a User You can reset the password for a user by performing any one of the following:

- **Generate the password manually:** You can reset the password of a user manually in instances such as the user has forgotten the password and has called HelpDesk to reset the password quickly. Helpdesk can immediately reset the password manually by entering a password, and the user can login by using the new password. This resolves the issue faster than the user waiting for an e-mail notification.

- **Generate a random password:** When a password has to be reset by someone other than the target user, an administrator for example, random password generation is useful so that the person changing the password will not know the new password. A random password can be generated in the following instances:

  - A user has forgotten the password and it needs to be reset.

  - The password has expired. A user has been locked.

  - A user has been locked.

  In such scenarios, when the password is reset, Oracle Identity Manager can automatically generate a new random password that conforms to the given password policy. Also, when the password is reset, the administrator gets an option to check a check box, which when checked will send out an e-mail notifying the user about the password change. This method enables you to generate temporary passwords randomly that cannot be easily guessed by anyone. After you generate the random password, at the next login, the user is prompted to reset the randomly generated password.

To reset the password for a user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of Advanced Search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Reset Password**. Alternatively, you can click the **Reset Password** icon on the toolbar. If the user details page for the user is open, then you can click **Reset Password** on the toolbar. The Reset Password dialog box is displayed, as shown in Figure 11–6:

Figure 11–6   The Reset Password Dialog Box

3. To manually change the user's password:

   a. Select the **Manually change the Password** option.

   b. In the New Password field, enter the new password that conforms to the password policy that is displayed in the Password Policy section.

   The Password Policy section displays the password policy assigned to the user. This section does not display the password policy if no password policy is defined. For information about password policies, see Section 10.6, "Password Policies Form" in *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

   c. In the Confirm new password field, re-enter the password.

4. To generate a random password, select the **Auto generate the Password (Randomly generated)** option.

5. Verify that the **Email the new password to the user** option is selected so that the new password is sent to the user through e-mail.

6. Click **Reset Password**. A confirmation message is displayed stating that the password is changed successfully.

> **Tip:** If the user forgets the password and tries to retrieve it, then the challenge questions are prompted to the user. The user must enter the same answers provided while creating a password. You can configure the challenge questions for the users by using Oracle Identity Manager Design Console.
>
> To configure challenge questions for the user:
>
> 1. Login to Oracle Identity Manager Design Console.
> 2. Navigate to **Administration**, **Lookup Definition**.
> 3. Search for the Lookup for challenge questions, that is, lookup Code = Lookup.WebClient.Questions.
> 4. In the Lookup Code Information tab, add questions by entering the appropriate values in the Code Key and Decode fields.
> 5. Click **Add**.
> 6. Add this key to the custom resource bundle.
>
> For more information about the Lookup Definition form, see Section 10.3, "Lookup Definition Form" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

11.3.3.3.6 Deleting User This operation is available only if the user status is not Deleted.

If the user is currently disabled, and the Automatically Delete On attribute is set to a future date, then the disable operation fails, and a message is displayed stating that the user cannot be deleted because it is currently scheduled to be deleted at a future date.

To delete a user:

1. In the user search result on the left pane of Oracle Identity Manager Administration, select a user. Alternatively, you can select the user from the search results of advanced search. In addition, you can perform this operation from the page that displays user details.

2. From the Action menu, select **Delete User**. Alternatively, you can click the **Delete User** icon on the toolbar. If the user details page for the user is open, then you can click **Delete User** on the toolbar. A message is displayed asking for confirmation.

3. Click **OK**. A confirmation message is displayed stating that the user is successfully deleted.

4. Click **OK** to close the message box.

   If you delete a user from the user detail page, then the successful completion refreshes the Attributes tab. If you perform this operation from a user list, such as simple or advanced search results, then the corresponding row in the list is refreshed.

Sometimes, you might not want a delete operation to immediately delete the user. Instead, you might want a delete operation to disable the user for a predefined period of time, during which the delete operation can be canceled. After that predefined period of time, the user is deleted. This is called a delayed delete.

To configure delayed delete in Oracle Identity Manager, you must define the Period to Delay User Delete configuration property, which specifies the predefined wait period in days to hold on the delete operation. If you do not want to configure delayed delete, then set the value of the Period to Delay User Delete configuration property to 0 or a negative number. After a user is deleted, if you want to disable the user entity with a date counter that specifies the date and time when the user must be permanently

deleted, then set the value of the Period to Delay User Delete configuration property to greater than 0.

> **Note:** To configure delayed delete:
>
> 1. In the Welcome page for Oracle Identity Manager Administration, under System Management, click **System Configuration**.
> 2. In the left pane, search for system properties.
> 3. In the search result, select the Period to Delay User Delete property.
> 4. Edit the property value to specify a delay period to delete the user.
> 5. Save the property.
>
> For more information about system properties, see "Administering System Properties" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

As a result of delayed delete:

- The disable status is similar to a regular disable operation that prevents the user from logging into Oracle Identity Manager and disables all provisioned resources.

- When a user is in disabled status, enabling the user cancels the delete operation. The date on which the user will be deleted is displayed on the user profile.

- If a user stays disabled and the predefined period expires, then the user is deleted at that time.

11.3.3.4 Bulk User Modifications

The bulk operations are performed from the search results for simple and advanced search. You can select multiple users and then select the available option from the Action menu. You can perform the following bulk operations:

- **Enabling users:** If all the selected users are in Disabled state

- **Disabling users:** If all the selected users are in Enabled state

- **Locking users:** If all the selected user are in Unlocked state

- **Unlocking users:** If all the selected users are in Locked state

- **Deleting users:** If all the selected users are not in Deleted state

> **Note:** For all the bulk modify operations, you must have the required authorization and you must select multiple users.

You can use the Bulk Modify page to make changes to multiple users at a time. You can open this page if you are authorized to modify users as determined by the authorization policy on the Modify User Profile privilege on any organization in Oracle Identity Manager.

You can open the Bulk Modify page in any one of the following ways:

- Selecting **Bulk Modify** from the Action menu in a user search results page, after selecting multiple users

- Selecting the **Bulk Modify** icon on the toolbar in a user search results page, after selecting multiple users

Table 11–6 describes the fields in various sections of the Bulk Modify page:

Table 11–6   Fields in the Bulk Modify Page

Section	Field	Description
Basic User Information	Design Console Access	Design Console Access check box that indicates whether or not the users can login to the Design Console.
	Manager	The reporting manager of the selected users.
	Organization	The organization to which the selected users belong.
	User Type	The type of selected employees, such as full-time employee, intern, contractor, part-time employee, consultant, or temporary.
Account Effective Dates	Start Date	The date when the selected users will be activated in the system.
	End Date	The date when the selected users will be deactivated in the system.
Provisioning Dates	Provisioning Date	The date when the users are provisioned.
	Deprovisioning Date	The date when the users are provisioned.

Only those attributes configured as part of the modify operation in user management configuration are displayed as fields in the Bulk Modify page. The attributes displayed are restricted to those defined in the user entity definition with the Support Bulk Update property set to Yes. The attributes are further filtered based on authorization policies that specify the attributes for the selected users that you have privileges to modify.

The permissions are based on OES policy. For instance, if the OES policy mentions that you can modify only the first name for one user and only the last name for another user, based on the users selected, it is possible that you select these names and the attributes to display on the page, results in no fields being allowed. As a result, the Bulk Modify page displays an error message stating that the attributes of the selected users cannot be modified in bulk, and the user selection must be changed.

11.4 User Management Authorization

Run-time security is enforced in the user management service through authorization policies. Each role in Oracle Identity Manager can be associated with one or more such authorization policies. Users that are members of a role are authorized to perform various user tasks based on the privileges granted to the role by its associated authorization policies. Because a user may have many roles, the privileges of a user are the cumulative privileges of his collective roles.

The access controls are implemented in the form of authorization policies that are managed by the Oracle Entitlements Server (OES). These policies define the controls in terms of roles and targets. The target is a combination of privilege, entity, and entity attribute.

> **See Also:** Chapter 15, "Managing Authorization Policies" for detailed information about authorization policies in Oracle Identity Manager

If a user has multiple roles that have different authorization policies applicable in the same context, then the user's access rights are the cumulative rights across those

policies. In other words, if a policy with read permission is granted to a role, and a policy with write permission is granted to another role, then a user with both the roles has read and write permission.

The authorization model is described in the following topics:

- Privileges
- Attributes
- Data Constraints
- Authorization with Multiple Policies

11.4.1 Privileges

All authorization privileges are controlled by authorization policies. Oracle Identity Manager explicitly defines privileges that control access rights for performing various operations in the application.

Table 11–7 lists the authorization privileges available in Oracle Identity Manager for the user management feature that and can be assigned to roles as part of an authorization policy definition:

> **Note:** For the Entity Instance Level, there must be a qualifier that determines over which users the logged in user has the privilege for all the privileges.

Table 11–7   Authorization Privileges for User Management

Privilege	Description
Search for Users	You can define this qualifier in terms of organizations, role memberships, or attribute-based rules. For information about defining this qualifier, see Chapter 15, "Managing Authorization Policies".
	Note:
	■ The "Search for Users" privilege depends on the "View User Details" privilege to determine which attributes can be included in the search results and which attributes can be included in the search criteria for a user search. Consequently, any User Management policy that provides the "Search User" permission should also provide the "View User Details" permission. The "View User Details" permission should include the User Login, Account Status, Identity Status, and Display Name attributes. If you do not provide these attributes, the user might not be fully viewable or editable.
	■ To enable users to perform a search based upon an user attribute, you must also configure that attribute as "Searchable" in the user configuration.
	There is a default authorization policy for the search operation that decides what the user can search. For information about default authorization policies for user management, see "User Management" on page 15-9.

Table 11–7 (Cont.) Authorization Privileges for User Management

Privilege	Description
View User Details	This privilege determines if you have the ability to display the User Details page for a user from the search results table.
	This privilege supports the following fine-grained controls:
	■ Entity Instance Level: The qualifier can be defined in terms of the organization membership and/or the management chain. Refer "Creating an Authorization Policy for User Management" on page 15-4 for details on how to define these qualifiers. Refer "Data Constraints" on page 11-37 for information about data constraints used in authorization policies for user management.
	■ Attribute Level: There must be qualifiers that determine your privilege to view attributes in the User Details page. This qualifier must list all the attributes from the user entity definition that you can view.
	Note: The View User Details privilege cannot specify which detail sections can be viewed by the user. This privilege determines whether or not complete user details page with all sections can be viewed. If the user details page can be viewed, then this privilege determines which attributes are displayed in the Attribute Profile of a user.
Modify User Profile	This privilege determines if you have the ability to modify the user profile attributes of a user on the User Details page.
	This privilege supports the following fine-grained controls:
	■ Entity Instance Level: The qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
	■ Attribute Level: There must be qualifiers that determine your privilege to modify attributes in the User Details page. This qualifier must list all the attributes from the user entity definition that you can edit. You must also grant the View User Details privilege for all these attributes.
Provision Resource to User	This privilege determines if you have the ability to provision or deprovision resources to a user on the Resource Profile section of the User Details Page. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
Modify User Proxy Profile	This privilege determines if you have the ability to modify the user's proxy details on the Proxy Details section of the User Details page. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
Modify User Status	This privilege determines if you have the ability to enable or disable a user. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
Modify OIM Account Status	This privilege determines if you have the ability to lock or unlock a user. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.

Table 11–7 (Cont.) Authorization Privileges for User Management

Privilege	Description
Delete User	This privilege determines if you have the ability to delete a user. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
Change Password	This privilege determines if you have the ability to change a user's enterprise password. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.
Create User	This privilege determines if you have the ability to create users in Oracle Identity Manager. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier must be defined in terms of organizations.
Evaluate Access Policies	This privilege determines if you have the ability to initiate access policy evaluation for a user when necessary. **Note**: There is no UI operation to initiate on-demand access policy evaluation.
View User Requests	This privilege determines if you have the ability to view the requests raised for a user.
Change User Password	This privilege determines if you have the ability to change the password of a user. There must be a qualifier that determines over which users the logged in user has this privilege. This qualifier can be defined in terms of organizations, role memberships, or attribute-based rules.

> **Note:** The Modify Role Membership permission for role management determines if the user can perform add or remove role operations from the Roles tab of the modify user page. For more information about this permission, see "Managing Authorization for Roles" on page 12-26.

11.4.2 Attributes

The read/write permissions for attributes define the actual set of readable or modifiable attributes in the context of the view or modify operation.

11.4.3 Data Constraints

The following data constraints are used in the authorization policies for user management:

- List of organizations: This limits the scope of the privilege for the assignee to only the organizations listed. Organization membership can be controlled by the Hierarchy Aware option in the authorization policies UI.
  - When the Hierarchy Aware option is set to false, then the scope of the privilege is only to the users that are direct members of the organization. For example, if the organization is Development Center and it has USA Development Center and China Development Center as the suborganizations, then the privilege can be exercised against users that are directly under the Development Center organization.

        – When the Hierarchy Aware option is set to true, then the scope of the privilege is applicable to users who are direct members of the listed organization and the users who are members of any of the sub-organizations of these organizations. For example, if the organization is Development Center and it has USA Development Center and China Development Center as the suborganizations, then the privilege can be exercised against users in all of these organizations.

- Assignee must be in the same organization: This flag limits the scope of the privilege for the assignee to only the assignee's organization. For example, the organization list in the policy is USA, China, and Canada. If this flag is set and the assignee's organization is USA, then the privilege can be exercised only in the USA organization.

- Management chain of user: This flag limits the scope of the privilege for the assignee to only the assignee's direct and indirect reports. For example:

  DR1, DR2, and DR3 are direct reports of M1.

  DR1_1, DR1_2, DR1_3, and DR1_4 are direct reports of DR1.

  DR2_1, DR2_2, and DR2_3 are direct reports of DR2.

  DR2_2_1 and DR2_2_2 are direct reports of DR2_2.

  Here, M1 can exercise the privilege on all of DR1, DR2, and DR3 and their direct and indirect reports if the **Management Chain of User** option is selected.

11.4.4 Authorization with Multiple Policies

When an authorization check is performed for the Search for Users permission, the OES and Oracle Identity Manager layer prepares an authorization result based on the result obtained from OES. There can be multiple authorization policies with each policy having different set of viewable attributes. Collecting all such policies provides a way to determine all viewable attributes for a searched user.

The authorization check for the Search for Users permission returns a list of obligations. This is a list of obligations from each applicable authorization policy. These obligations from multiple policies are combined to get a unified search result.

This section describes how obligations are handled for various user management operations. it contains the following topics:

11.4.4.1 Search Operation Authorization with Multiple Authorization Policies

There can be the following types of obligations for the search operation:

- **List of organizations:** The list of organizations can be for direct or indirect organization membership, which is controlled by the Hierarchy Aware data constraint. A special value here can be list of all organizations in Oracle Identity Manager. The logged in user can search only within this set of organizations.

- **Is in the same organization:** This obligation means that the logged in user can search for users only in the user's own organization.

- **Is in management hierarchy:** This obligation means that the logged in user can search for any users in the user's management hierarchy.

- **Viewable Attributes:** This obligation contains the list of authorized viewable attributes. The search operation can be performed only against these attributes.

If there are multiple authorization policies that grant the search privilege to a user, then the search behavior is as follows:

1. The set of users who can be searched by the logged in user will be the union of set of users on which search privilege is provided by each of these policies.

2. The set of attributes returned as part of the search results is the union of sets of attributes on which View User Details privilege is granted by each of the these policies.

This is described with the help of the following example:

Policy1 returns the First Name, Last Name, and Middle Name attributes, and Policy2 returns the User Login, User Type, and OIM User Type attributes. When obligations from both the policies are enforced, the returned attribute list is First Name, Last Name, Middle Name, User Login, User Type, and OIM User Type for all users. The policy due to which the user is selected as part of the results is not checked. Therefore, do not configure attributes from the configuration service that might display confidential data in the search results.

In an another example, suppose there are three authorization policies defined for the search operation. The following table lists the details of the sample authorization policies:

Policy Name	Entity Name	Permissions	Data Constraints	Assignment
Policy1	User management	Search Modify User Profile. Attributes include First Name, Last Name, and Middle Name View User Details. Attributes include Display Name, First Name, Last Name, and Middle Name	Users that are members of the Org1 and Org2 organizations Hierarchy Aware (include all Child Organizations) = TRUE	Role: Role1 Management Chain of User = FALSE Assignee must be a member of the User's Organization = TRUE
Policy2	User management	Search Modify User Profile. Attribute includes User Type View User Details. Attributes include User Login, User Type, and OIM User Type	Users that are members of the Org3 organization Hierarchy Aware (include all Child Organizations) = FALSE	Role: Role2 Management Chain of User = FALSE Assignee must be a member of the User's Organization = FALSE
Policy3	User management	Search Modify User Profile. Attribute includes Designation View User Details. Attributes include User Login, User Type, OIM User Type, and Designation	All Users	Role: Role2 Management Chain of User = TRUE Assignee must be a member of the User's Organization = FALSE

In this example:

- Org1 has Org1Child1 and Org1Child2 as child organizations.

- Org1Child1 has Org1Child1_Child1 as the child organization.

- Org3 has Org3Child1 and Org3Child2 as child organizations.

Consider the following scenarios:

Scenario I:

User1 has Role1 only and belongs to the Org1Child1 organization. The user can:

- Search for users who are members of Org1Child1 organization. The search can be performed on the basis of First Name, Last Name, and Middle Name, and Display Name user attributes and also the search result can contain a subset of the set of these attributes.

- Modify the First Name, Last Name, and Middle Name user attributes from the Org1Child1 organization.

Scenario II:

User2 has Role1 and Role2 and belongs to the Org2 organization. User2 has direct reports DR1 and DR2 belonging to the Org2 organization. The user can:

- View the User Login, User Type, and OIM User Type user attributes from the Org3 organization because of Policy2.

- Modify the User Type attribute from the Org3 organization because of Policy2.

- View the First Name, Last Name, and Middle Name user attributes from the Org2 organization, because of Policy1.

- Modify the First Name, Last Name, and Middle Name user attributes from the Org2 organization, because of Policy1.

- View the User Login, User Type, OIM User Type, and Designation user attributes of all the user's direct reports because of Policy3.

- Modify the Designation attribute of all the user's direct reports because of Policy3.

If the user being tried to modify is DR1, then the list of modifiable attributes are First Name, Last Name, Middle Name because of Policy1, and Designation because of Policy3.

The user cannot view, modify, and search users from child organizations of Org3, which are Org3Child1 and Org3Child2.

Based on these scenarios, for the search operation, a union of the viewable attributes from all the three authorization policies are displayed to the user. In other words, the user is able to see User Login, User Type, OIM User Type, First Name, Last Name, Middle Name, Display Name, and Designation attributes in the search results irrespective of the authorization policy. Here, the Designation attribute is displayed not only for DR1 and DR2, who are direct reports of User2, but are displayed for all the users in the results.

11.4.4.2 Modify Operation Authorization with Multiple Authorization Policies

If the logged in user is allowed to modify a user profile as defined by multiple policies, then a union of the set of attributes from individual policies is used for performing the operation. Refer to Scenario II of the "Search Operation Authorization with Multiple Authorization Policies" on page 11-38 for the example related to the modify operation in case of multiple applicable authorization policies.

11.5 Username Reservation

A request for creating a user can be raised from Oracle Identity Manager Self Service or Oracle Identity Manager Administration. When the request is submitted, the following scenarios are possible:

- While the request is pending, another create user request is submitted with the same username. If the second request is approved and the user is created, then the first request, when approved, fails because the username already exists in Oracle Identity Manager.

- While the request is pending, another user with the same username is directly created in the LDAP identity store. When the create user request is approved, it fails while provisioning the user entity to LDAP because an entry already exists in LDAP with the same username.

To avoid these problems, you can reserve the username in both Oracle Identity Manager and LDAP while the create user request is pending for approval. If a request is created to create a user with the same username, then an error message is displayed and the create user request is not created.

> **See Also:** "Creating a Request To Create a User" on page 14-1 for information about creating requests to create a user

For reserving the username:

- The USER ATTRIBUTE RESERVATION ENABLED system property must be set to TRUE for the functionality to be enabled. For information about searching and modifying system properties, see "Administering System Properties" in the *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

- Reservation in LDAP is done only if reservation functionality is enabled, and LDAP is in sync with Oracle Identity Manager database. For information about synchronization between Oracle identity Manager and LDAP identity store, see ""Integration Between LDAP Identity Store and Oracle Identity Manager" on page 4-20.

> **Note:**
>
> - If LDAP provider is not configured, then the reservation is done only in Oracle Identity Manager.
>
> - When LDAP synchronization and user attribute reservation features are enabled, it is recommended to enable UID uniqueness in the directory server. Without this, user reservation in the directory does not work properly because while the user is reserved in the reservation container, the user with the same user ID can be created in the user container. This results is user creation failure when Oracle Identity Manager tries to move the user from the reservation container to the user container.

If user attribute reservation is enabled, the reservation happens in two phases:

In the first phase, an entry is created in Oracle Identity Manager database and a user is created in reservation container. This entry in Oracle Identity Manager database is removed after successful creation of user, rejection by approver, or request failure.

In the second phase, in LDAP, on successful creation, the user is moved to the reservation container. In other cases such as rejection by approver or request failure, the user is removed from the reservation container.

After the request-level and operation-level approvals are obtained for the create user request, the username is no longer reserved in the username container in LDAP. The

username is moved to the container in which the existing users are stored. The user is also created in Oracle Identity Manager.

This section consists of the following topics:

- Enabling and Disabling Username Reservation
- Configuring the Username Policy
- Releasing the Username

11.5.1 Enabling and Disabling Username Reservation

The username reservation functionality is enabled by default in Oracle Identity Manager. This is done by keeping the value of the USER ATTRIBUTE RESERVATION ENABLED system property to TRUE. You can verify the value of this system property in the System Configuration section of Oracle Identity Manager Administration.

To disable username reservation:

1. Log in to the Administration console.

2. Click **System Management**.

3. Click **System Configuration**.

4. On the left pane, click the search icon to search for all existing system properties. A list of system properties are displayed in the search results table.

5. Click **User Attribute Reservation Enabled**. The System Property Detail page for the selected system property is displayed, as shown in Figure 11–7:

Figure 11–7   The System Property Detail Page

6. In the Value field, enter **False**.

7. Click **Save**. The username reservation functionality is disabled.

11.5.2 Configuring the Username Policy

Username Policy is a plugin implementation for username operations such as username generation and username validation. The policies follow Oracle Identity Manager plug-in framework. You can add your own policies by adding new plug-ins and changing the default policies from the System Configuration section in Oracle Identity Administration.

> **See Also:** "Developing Plug-ins" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about the plug-in framework

In case of create user request, the plugins are invoked only if the user login is not provided. In such a case, the plugin to be invoked is picked up from the system property, "Default policy for username generation".

Table 11–8 lists the predefined username policies provided by Oracle Identity Manager. In this table, the dollar ($) sign in the username generation indicates random alphabet:

Table 11–8   Predefined Username Policies

Policy Name	Expected Information	Username Generated
oracle.iam.identity.usermgmt.impl.plugins.EmailUserNamePolicy	E-mail	If e-mail is provided, then e-mail is generated as username.
oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstInitialLocalePolicy	First name, last name, and locale	last name + first initial_locale, last name + middle initial + first initial_locale, last name + $ + first initial_locale (all possibilities of single random alphabets), last name + $$ + first initial_locale
oracle.iam.identity.usermgmt.impl.plugins.FirstInitialLastNameLocalePolicy	Firstname, Lastname, Locale	first initial + lastname_locale, first initial + middle initial + first name_locale, first initial + $ + lastname_locale, first initial + $$ + lastname_locale
oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstInitialPolicy	Firstname, Lastname	lastname+firstInitial, lastname+middleinitial+firstInitial, lastname+$+firstInitial (all possibilities of single random alphabets) , lastname+$$+firstInitial
oracle.iam.identity.usermgmt.impl.plugins.FirstInitialLastNamePolicy	Firstname, Lastname	firstInitial+lastname, firstInitial+middleInitial+firstname, firstInitial+$+lastname, firstInitial+$$+lastname
oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstNamePolicy	Firstname, Lastname	lastname.firstname, lastname.middleinitial.firstname, lastname.$.firstname (all possibilities of single random alphabets) , lastname.$$.firstname
oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicy	Firstname, Lastname	firstname.lastname, firstname.middleinitial.lastname, firstname.$.lastname (all possibilities of single random alphabets) , firstname.$$.lastname

Table 11–8 (Cont.) Predefined Username Policies

Policy Name	Expected Information	Username Generated
oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy	E-mail	If e-mail is provided, then username is generated based on the e-mail. If e-mail is not available, then it generates username based on firstname and lastname by appending a user domain to it. The user domain is configured as the Default user name domain system property, and the default value is @oracle.com
oracle.iam.identity.usermgmt.impl.plugins.LastNamePolicy,	Lastname	lastname, middle initial + lastname , $ + lastname, $$ + lastname
oracle.iam.identity.usermgmt.impl.plugins.LastNameLocalePolicy	Lastname, Locale	lastname_locale, middle initial + lastname_locale , $ + lastname_locale, $$ + lastname_locale

Values must be provided for all the parameters of the username generation format. If any of the parameters are not provided, then Oracle Identity Manager generates an error. For example, If the firstname.lastname policy is configured and the firstname is not provided, then the error would be "An error occurred while generating the Username. Please provide firstname as expected by the firstname.lastname policy".

The UserManager exposes APIs for username operations. The APIs take the user data as input and return a generated username. The APIs make a call to plug-ins that return the username. This allows you to replace the default policies with custom plug-ins with your implementation for username operations.

> **Note:**
>
> ■ For user name generation and validation, public APIs are exposed in UserManager.
>
> ■ While creating the policy, ensure that the attributes used in generating the username are defined in the request data set. For information about request data set, see "Request Dataset" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

You can plug-in your own username policies by implementing the plug-in interface, as shown:

```
package oracle.iam.identity.usermgmt.api;
public interface UsernamePolicy {
        public String getUserNameFromPolicy(HashMap<String, String> reqData)
throws UserNameGenerationException;

        public boolean isUserNameValid(String userName, HashMap<String, String>
reqData);
        public String getDescription(Locale locale);
}
```

This plug-in point is exposed as a kernel plug-in that takes request data as input and returns the username. Each plug-in expects some information and generates username based on that information provided. The policy implementations generate the username, check for its availability, and if the username is not available, then generate

other username based on the policy in the order mentioned in Table 11–8, and repeat the procedure. The dollar ($) sign in the username generation indicates random alphabet. If any of the expected information is missing, then the policies generate errors.

The username generation is exposed as public APIs in User Manager. Oracle Identity Manager provides an utility class for accessing the functionality of generating user names. The class that contains utility methods is as shown:

```
oracle.iam.identity.usermgmt.api.UserManager
```

This class exposes the following main methods:

```
//Method that will generate username based on default policy
        public String generateUserName(HashMap<String, String> requestData)
                                   throws UserNameGenerationException

//Method that will generate username based on policy
        public String generateUserName(String policyID, HashMap requestData)
                                   throws UserNameGenerationException

//Method that will check whether username is valid against default policy
        public boolean isUserNameValid(String userName,
HashMap<String, String> reqData)

//Method that will check whether username is valid against given policy
        public boolean isUserNameValid(String userName, String
userNamePolicyPluginID, HashMap<String, String> requestData)

//Method to return all policies (including customer written)
        public List<Map<String, String>> getAllUserNamePolicies(Locale locale)

//Method that will return policy description in given locale
        public String getPolicyDescription(String policyID, Locale locale)
```

Table 11–9 lists the constants defined in the UserManager class to represent the policy ID of the default username policies:

Table 11–9   Constants Representing Policy IDs

Policy Name	Constant
EmailUserNamePolicy	EMAIL_ID_POLICY
LastNameFirstInitialLocaleP olicy	FIRSTNAME_LASTNAME_POLICY
FirstInitialLastNameLocaleP olicy	LASTNAME_FIRSTNAME_POLICY
LastNameFirstInitialPolicy	FIRSTINITIAL_LASTNAME_POLICY
FirstInitialLastNamePolicy	LASTNAME_FIRSTINITIAL_POLICY
LastNameFirstNamePolicy	FIRSTINITIAL_LASTNAME_LOCALE_POLICY
FirstNameLastNamePolicy	LASTNAME_FIRSTINITIAL_LOCALE_POLICY
DefaultComboPolicy	DEFAULT_COMBO_POLICY
LastNamePolicy	LASTNAME_POLICY
LastNameLocalePolicy	LASTNAME_LOCALE_POLICY

When called to generate username, the policy classes expect the attribute values to be set in a map by using the key constants defined in the oracle.iam.identity.utils class.Constants. This means that a proper parameter value must be passed to call the method by using the appropriate constant defined for it, for example, the FirstName parameter has a constant defined for it.

The default username policy can be configured by using Oracle Identity Manager Administration. To do so:

1. Navigate to the System Configuration section.

2. Search for all the system properties.

3. Click **Default policy for username generation**. The System Property Detail page for the selected property is displayed, as shown in Figure 11–8:

Figure 11–8   The Default Username Policy Configuration

The XL.DefaultUserNameImpl system property is provided for picking up the default policy implementation. By default, it points to the default username policy, which is oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy displayed in the Value field.

4. In the Value field, enter **oracle.iam.identity.usermgmt.impl.plugins.***POLICY*. Here, *POLICY* is one of the policy implementations.

> **Note:**   All the plug-ins must be registered with Oracle Identity Manager by using the /identity/metadata/plugin.xml file. A sample plugin.xml file is as shown:
>
> ```
> <plugins
> pluginpoint="oracle.iam.identity.usermgmt.api.UserNamePolicy">
> <plugin
> pluginclass="oracle.iam.identity.usermgmt.impl.plugins.LastNameFirs
> tNamePolicy"
> version="1.0" name="LastNameFirstNamePolicy"/>
> </plugins>
> ```

5. Click **Save**.

11.5.3 Releasing the Username

The username is released in the following scenarios:

- When the request is approved, and the user is successfully created in Oracle Identity Manager and provisioned to LDAP, and the username from the reserved table is removed. The reserved username is removed after successful user creation after the approvals. The reserved entry in LDAP is removed and the actual user is created.

- If the request is rejected, then the reserved entry of username in LDAP and Oracle Identity Manager are removed.

- If the request fails while or before creating a user in Oracle Identity Manager or LDAP, then the reserved username is deleted.

12

Managing Roles

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

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

Using roles, you can:

- View the menu items that the users can access through Oracle Identity Manager Administration Web interface.

- Assign users to roles.

- Assign a role to a parent role

- Designate status to the users so that they can specify defined responses for process tasks.

- Modify permissions on data objects.

- Designate role administrators to perform actions on roles, such as enabling members of another role to assign users to the current role, revoke members from current role and so on.

- Designate provisioning policies for a role. These policies determine if a resource object is to be provisioned to or requested for a member of the role.

- Assign or remove membership rules to or from the role. These rules determine which users can be assigned/removed as direct membership to/from the role.

This chapter describes roles and functionalities related to roles in the following sections:

- Role Membership Inheritance

- Role Permission Inheritance

- Role Entity Definition

- Default Roles

- Role Management Tasks

- Managing Authorization for Roles

12.1 Role Membership Inheritance

Membership inheritance means that the members of the inheritor role inherit from the inherited role. For example:

• Role B inherits memberships from Role A. Role B is parent role to Role A.

• Role C also inherits memberships from Role A. Role C is also parent role of Role A

In this example, all members of Role A are also implicit or indirect members of Role B and Role C, but members of Role B are not automatically members of Role A. In other words, Role B and Role C are the parents of Role A. Similarly, Role A is the child of Role B and Role C. A real example for this is that the Employee Role (Role B) inherits memberships from the Manager Role (Role A).

12.2 Role Permission Inheritance

Permission inheritance means that the permissions of the inheritor role inherit from the inherited role. For example:

- Role B inherits permissions from Role A.

- Role C also inherits permissions from Role A.

In this example, Role B and Role C are the children of Role A. Similarly, Role A is also the parent of Role B and Role C.

A real example for this is that the Manager role inherits permissions from the Employee role.

Note how membership inheritance and permission inheritance go in different directions.

The Administrative and User Console represents role permission inheritance through the following sections in the Hierarchy tab:

> **See Also:** "The Hierarchy Tab" on page 12-14 for more information about the Hierarchy tab

- **Inherited From:** Displays the parent roles from which the open role is inherited. The base role has the same permissions and privileges on the members as the inherited roles. Only inherited roles can be added or removed from the base role, but the base role cannot be added or removed from the inherited role.

- **Inherited By:** Lists the child roles that are inherited by the open role. This is a read-only display of the roles. You can use the Open Role action to modify the relationship from the base role.

For example, you create three roles: role1, role2, and role3. Open role3 and assign role2 as the parent role. Similarly, open role2 and assign role1 as the parent role. When you open role3, the Inherited From section displays the role2 parent role, and role1 is displayed under role2. When you open role1, the Inherited By section displays the role2 child role, and role3 is displayed under role2.

12.3 Role Entity Definition

Attributes are defined for the role entity in Oracle Identity Manager. For each attribute for a role entity, the following properties are defined in Oracle Identity Manager:

> **Note:** You cannot add your own attributes for the role entity.

- **Attribute Name:** The name of the attribute.

- **Category:** All entity attributes are classified into a category. This categorization is used to organize the data in the UI. It is also used for delegated authorization. This is a category for display and authorization, and is different than role categories.

    See Also:

    -

    -

- **Type:** Indicates whether the attribute is a single-valued attribute or not.

- **Data Type:** Indicates the type of data in the attribute. Supported types are: Text, Numeric, Date, which indicates both date and time), Boolean, and Reference, which is a pointer to another entity.

- **Properties:** For each attribute, a bunch of properties can be defined. The properties are:

    - **Required:** Determines whether or not every entity in the repository must have a non-NULL value for this attribute

    - **System Controlled:** Determines if the value can be set and edited by Oracle Identity Manager exclusively, which is read-only for the user

    - **System Can Default:** Determines whether or not the value can be set by Oracle Identity Manager to a default if no value is provided

    - **Encrypted:** Determines if the value is stored in the repository as reversible encrypted or clear

    - **Searchable:** Determines if the values can be used in searches or not

    - **Support Bulk** Update: Determines if the field can be modified as part of a bulk modification of multiple users. Fields that are expected to be unique to users, such as username, name fields, and password, must not support bulk update. For fields that are System Controled=Yes, this property can never be set to Yes.

    - **Display:** Determines how the field is displayed in the UI. It can have any one of the following values:

        * **Clear:** Show the value as clear text

        * **Masked:** Mask the value in any UI

        * **Partial Mask:** Mask part of the value in the UI (de-scoped to 9.3)

- **Dependency:** The value of some attributes can depend on the value of other attributes. This property lists the other attributes that this attribute depends on. If any of those attributes are to be changed, then the autogenerate or prepopulate adapters for this attribute must be run.

- **LOV:** For some attributes, the value the field can take may be constrained to a list of values. You can modify the available values in the LOV that are marked configurable. In others, you cannot add your own values. In addition, the list of values can come from a predefined list of values. In others, the list of values must come from an API call primarily for attributes of Data Type=Reference.

This section describes the default attribute definition of the following entities:

- Role Entity

- Role Category Entity

- Role Grant Relationship

- Role Parent Relationship

12.3.1 Role Entity

Table 12–1 lists the default attributes for the role entity. You can add your own attributes to the role entity.

Table 12–1 Default Attributes for the Role Entity

Attribute Name	Category	Type	Data Type	Properties	LOV
Key	Basic	Single	Numeric	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
Unique Name	Basic	Single	Text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: No Unique: Yes Support Bulk Update: No	NA
Display Name	Basic	Single	Text (multi-language)	Required: Yes System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Namespace	Basic	Single	Text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

Table 12–1   (Cont.) Default Attributes for the Role Entity

Attribute Name	Category	Type	Data Type	Properties	LOV
Name	Basic	Single	Text (multi-language)	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Description	Basic	Single	Text (multi-language)	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
LDAP GUID	LDAP	Single	Text	Required: Yes System Can Default: No System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
Role Category	Basic	Single	Reference to role category	Required: Yes System Can Default: Yes System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: Yes	NA
Role Email	Basic	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

12.3.2 Role Category Entity

Table 12–2 lists the default attributes for the role category entity. You cannot add your own attributes to the role category entity.

Table 12–2   Default Attributes for the Role Category Entity

Attribute Name	Category	Type	Data Type	Properties	LOV
Key	Basic	Single	Text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: Yes Support Bulk Update: No	NA
Name	Basic	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
Description	Basic	Single	Text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

12.3.3 Role Grant Relationship

Table 12–3 lists the default attributes for role grant relationship. You cannot add your own attributes for the role grant relationship.

Table 12–3   Default Attributes for Role Grant Relationship

Attribute Name	Category	Type	Data Type	Properties	LOV
UGP_KEY	Basic	Single	Reference to role	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
USR_KEY	Basic	Single	Reference to user	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

12.3.4 Role Parent Relationship

Table 12–4 lists the default attributes for the role parent relationship. You cannot add your own attributes to the role parent relationship.

Table 12–4   Default Attributes for Role Parent Relationship

Attribute Name	Category	Type	Data Type	Properties	LOV
UGP_KEY	Basic	Single	Reference to role	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA
GPP_UGP_KEY	Basic	Single	Reference to role	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No Support Bulk Update: No	NA

12.4 Default Roles

Table 12–5 lists the default roles in Oracle Identity Manager:

Table 12–5   Default Roles in Oracle Identity Manager

Role	Description
USER CONFIGURATION ADMINISTRATORS	Members of this role have access to the UI to perform various tasks to create and manage entity attributes for user management.
SYSTEM CONFIGURATION ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks related to system configuration, such as system properties, scheduled jobs, and notification templates.
SYSTEM ADMINISTRATORS	Members of this role have full permission to create, edit, and delete records in Oracle Identity Manager, except for system records. These users can control the permissions of other users, change the status of process tasks even when the task is not assigned to them, and administer the system from the highest level.
USER NAME ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI.
SELF OPERATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. It contains one user, XELSELFREG, who is responsible for modifying the privileges that users have when performing self-registration actions within Oracle Identity Manager. **Note:** Oracle Identity Manager recommends that you do not modify the permissions associated with the SELF OPERATORS user role. In addition, you should not assign any users to this role.
SCHEDULER ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. The user with this role can perform all scheduler jobs administration.
ROLE ADMINISTRATORS	Members of this role have access to the UI to administer and manage roles in Oracle Identity Manager.
RESOURCE ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to manage resources.
REQUEST TEMPLATE ADMINISTRATORS	The user with this role can perform all request template administration.
REQUEST ADMINISTRATORS	Members of this role have access to the UI to perform various tasks to create and manage requests.
REPORT ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to manage reports in BI Publisher.
RECONCILIATION ADMINISTRATORS	The user with this role can perform reconciliation administration.
PLUGIN ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Member of this role have permissions to register and unregister plugins to Oracle Identity Manager.
OPERATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the pages related to organizations, users, and Task List. These users can perform a subset of functions on these pages.

Table 12–5   (Cont.) Default Roles in Oracle Identity Manager

Role	Description
NOTIFICATION TEMPLATE ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to create and manage notification templates.
IT RESOURCE ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to create and manage IT resources.
IDENTITY USER ADMINISTRATORS	Members of this role have access to the UI to perform various tasks to create and manage users in Oracle Identity Manager.
IDENTITY ORGANIZATION ADMINISTRATORS	Members of this role have access to the UI to perform various tasks to create and manage organizations in Oracle Identity Manager.
GENERIC CONNECTOR ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to configure generic connectors.
DEPLOYMENT MANAGER ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the Deployment Manager to import and export deployment configurations from an Oracle Identity Manager deployment to another.
Administrators	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. It is the administrators role for SOA.
ATTESTATION EVENT ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to manage attestation events.
ATTESTATION CONFIGURATION ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to configure attestation.
APPROVAL POLICY ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to the UI to perform various tasks to create and manage approval policies.
ALL USERS	Members of this role have minimal permissions, including the ability to access the user's own user record. By default, each user belongs to the All Users role.
ACCESS POLICY ADMINISTRATORS	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role can access the UI to perform various tasks to manage access policies.
SPML_App_Role	This role is for internal use only, meaning it is for OIM users and other users can only view it on UI. Members of this role have access to submit requests via the SPML interfaces.

You can modify the permissions associated with the default roles. You can also create additional roles. However, you cannot assign/remove menu items to/from any roles.

12.5 Role Management Tasks

This section discusses the following topics:

- Creating Roles
- Managing Roles
- Creating and Managing Role Categories

Note:

- A user cannot be removed from the All Users role.

- A role, SELF OPERATORS, is added to Oracle Identity Manager by default. This role contains one user, XELSELFREG, who is responsible for modifying user permissions for performing self-registration in the Administration Console.

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

12.5.1 Creating Roles

When you first create a new role, the Role Details page shows the role name. You can add information to a role by using the Additional Detail menu as described in "Managing Roles" on page 12-11.

To create a role:

1. Login to Oracle Identity Administration.

2. In the Welcome page, under Roles, click **Create New Role**.

   Alternatively, in the Browse tab of the left pane, expand Roles, and from the Actions menu, select **Create Role**. Otherwise, click the **Create Role** icon on the toolbar.

   The Create Role page is displayed.

3. Enter values in the fields. Table 12–6 lists the fields in the Create Role page.

Table 12–6   Fields in the Create Role Page

Field	Description
Role Name	The name of the role
Display Name	The role name as displayed in the UI
Email	The e-mail ID of the role
Description	The description for the role
Role Category	The category to which the role belongs
	If a role category is not specified in this field, then the role is created in the Default category. See "Creating and Managing Role Categories" on page 12-24 for information about role categories.

Table 12–6 (Cont.) Fields in the Create Role Page

Field	Description
Owned By	The owner of the role
	The role owner is a user who has permissions to view, modify, and delete the role without having to create custom authorization policies. See "Managing Authorization for Roles" on page 12-26 for information about authorization policies for role management.

Note that **Manage Localizations** is displayed with the Display Name fields because these are multi-language fields. This means that you can enter and save attribute values in more than one language.

4. Click **Save**. The role is created successfully and role name, role namespace, LDAP Attributes such as LDAP GUID and LDAP DN are displayed in a new page.

12.5.2 Managing Roles

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

This section discusses the following topics:

- Browsing Roles
- Searching for Roles
- Deleting Roles
- Viewing and Administering Roles
- Viewing Menu Items
- Viewing, Assigning, and Revoking Access Policies
- Viewing, Assigning, and Revoking Membership Rules
- Updating Data Object Permissions

12.5.2.1 Browsing Roles

You can browse the roles that exist in Oracle Identity Manager in the Roles tab. To browse roles:

1. In the left pane of Oracle Identity Administration, click the **Browse** tab.

2. Expand **OIM Roles**. The role categories are displayed. For more information about role categories, see "Creating and Managing Role Categories" on page 12-24.

In the Browse tab, you can perform various tasks related to roles and role categories. For details, see "Viewing and Administering Roles" on page 12-13.

12.5.2.2 Searching for Roles

Oracle Identity Management Administration allows you to perform the following types of search operations for roles:

- Performing Simple Search for Roles
- Performing Advanced Search for Roles

12.5.2.2.1 Performing Simple Search for Roles To perform a simple search for roles:

1. In the left pane of Oracle Identity Administration, under Search, select **Roles**.

2. Specify a search criterion in the field next to the list. You can include wildcard characters (*) in your search criterion. For performance reasons, initial (prefix) wildcards will be removed. However, a trailing (prefix) wildcard will be added to all searches.

   > **Note:** "*" is the only wildcard search allowed in Oracle Identity Management Administration.

3. Click the search icon to the right of the field. A list of roles that match the search criterion is displayed in the Search Results tab.

   In the Search Results tab, you can edit and delete roles. For details, see "Viewing and Administering Roles" on page 12-13 and "Deleting Roles" on page 12-13.

12.5.2.2.2 Performing Advanced Search for Roles To perform an advanced search for roles:

1. In the Welcome page, under Roles, click **Advanced Search - Roles**.

   Alternatively, in the Browse tab for roles in the left pane, you can click the **Advanced Search: Roles** icon on the toolbar.

   The Advanced Search: Roles page is displayed.

2. Select any one of the following options:

   - **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

   - **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

3. In the Name field, enter the role name that you want to search. You can use wildcard characters in your search criteria. Select a search comparator in the list adjacent to the Name field. The default search comparator is "Begins With". The comparator "Equals" is available in the pulldown list as an alternative.

4. Similarly, enter search criteria in all the other fields. You can add fields to the Advanced Search: Roles page. To do so, click **Add Fields**, and then select the field name from the list.

5. Click **Search**. The roles that match your search criteria are displayed in the search results table.

   > **Note:** Clicking Search without any value returns all roles.

6. Click **View** and select Columns to view additional columns in the search results.

7. Click **View** and **Reorder Columns** to reorder the columns in the search results.

From the search results in the Advanced Search: Roles page, you can create new roles, edit roles, and delete roles. For details, see "Creating Roles" on page 12-10, "Viewing and Administering Roles" on page 12-13, and "Deleting Roles" on page 12-13.

12.5.2.3 Deleting Roles

To delete a role:

1. Search for a role as described in "Searching for Roles" on page 12-11. Alternatively, you can click the Browse tab for roles in the left pane.

2. Select the role that you want to delete.

3. From the Actions list, select **Delete**.

   Alternatively, you can click the delete icon on the toolbar. A message box is displayed asking for confirmation.

4. Click **OK** to confirm.

> **Note:** You are not allowed to delete a role, which is the parent/child of some other role. To delete such a role, you must first remove the associated parent-child role relationships. Once the role is no longer involved in any role relationships, it can be deleted.

12.5.2.4 Viewing and Administering Roles

You can open the details of a role and edit the role attributes, and modify the role inheritance and membership. To open the details of a role and modify it, perform one of the following:

- In the role browse tree, select the role that you want to open. From the Actions menu, select **Open**. Alternatively, you can click the **Open Role or Category Detail** icon on the toolbar.

- In the Search Results tab of the left pane, select the role that you want to open. From the Actions menu, select **Open**. Alternatively, you can click the **Open Role Detail** icon on the toolbar.

- In the Advanced Search: Roles page, select the role that you want to open. From the Actions menu, select **Open**. Alternatively, you can click **Open Role** on the toolbar.

The details of the role is displayed in a page. The role display name is displayed at the top of the page. You can display the details of the role and modify role information in the following tabs of this page:

- The Attributes Tab

- The Hierarchy Tab

- The Members Tab

12.5.2.4.1 The Attributes Tab The Attributes tab displays the role attributes in the following sections:

- **Basic Role Information:** This section displays the basic attributes of the role such as role name, role namespace, display name, e-mail, and description.

- **Other Information:** This section displays the information about the category to which the role belongs and the owner of the role.

The fields in the Attributes tab are same as available in the Create Role page. For information about all the fields in the Attributes tab, see Table 12–6, " Fields in the Create Role Page".

12.5.2.4.2 The Hierarchy Tab The Hierarchy tab displays the role hierarchy information in the following sections:

- **Inherited From:** This section is active by default. It displays the parent roles from which the open role is inherited. The base role has the same permissions and privileges on the members as the inherited roles. Only inherited roles can be added or removed from the base role, but the base role cannot be added or removed from the inherited role.

- **Inherited By:** This section lists the child roles that are inherited by the open role. This is a read-only display of the roles. You can use the Open Role action to modify the relationship from the base role.

In the Hierarchy tab. you can perform the following:

- Adding a Parent Role to a Child Role
- Removing a Parent Role from a Role
- Opening a Parent/Child Role

12.5.2.4.3 Adding a Parent Role to a Child Role

To add a parent role to a role:

1. Open the role.

2. Click the **Hierarchy** tab.

3. Verify that the Inherited From section is active.

4. From the Actions menu, select **Add** Parent Role. Alternatively, click **Add Parent Role** on the toolbar. The Add Inherited Role to: dialog box is displayed.

5. From the Search Roles list, select a role category whose roles you want to search.

6. In the search field, specify a search criterion. You can include wildcard characters (*) in your search criterion. Then, click the search icon. A list of roles that matches your search criterion and selected role category is displayed in the Available Roles list.

   > **Note:** "*" is the only wildcard search allowed in Oracle Identity Management Administration.

7. From the Available Roles list, select one or more roles that you want to add as parent roles. Then, click **Move** or **Move All** to move the selected roles to the Roles to Add list.

8. Click **Save**. The selected roles are added as parent roles to the opened role and the role hierarchy is displayed in the Inherited From section of the Hierarchy tab.

9. Select the inherited role that is added. A Summary Information of the role selected is displayed below the table.

12.5.2.4.4 Removing a Parent Role from a Role

To remove a parent role from a role:

1. In the Inherited From section of the Hierarchy tab, select the role that you want to remove.

2. From the Actions menu, select **Remove** Parent Role. Alternatively, click **Remove** Parent Role on the toolbar. A message box is displayed asking for confirmation.

3. Click **OK**. The inherited role is removed from the Inherited From section of the Hierarchy tab.

12.5.2.4.5 Opening a Parent/Child Role

You can open parent roles from the "Inherited From" section and child roles from the "Inherited By" section of the Hierarchy tab.

You can also open the roles that are linked parent and child roles (like grand parents and grand child roles) of the current opened role with the "Open Role" link in "Inherited From" and "Inherited By" section of the Hierarchy tab respectively.

To open a parent role:

1. In the Inherited From section of the Hierarchy tab, select the role that you want to open.

2. From the Actions menu, select **Open** (Open Role Detail). Alternatively, click **Open** (Open Role Detail) on the toolbar. A page with details about the inherited role is displayed. In this page, you can view and edit the role attributes, and modify the role inheritance and membership, assign and remove membership rules, access policies and permissions, update permissions and also to view the menu items assigned.

To open a child role:

1. In the Inherited From or Inherited By section of the Hierarchy tab, select the role that you want to open.

2. From the Actions menu, select **Open** (Open Role Detail). Alternatively, click **Open** (Open Role Detail) on the toolbar. A page with details about the inherited role is displayed.

12.5.2.4.6 The Members Tab
The Members tab displays the members assigned to the open role. This information is displayed in the following sections:

- **All Members:** This section displays all the members, direct and indirect, assigned to the open role.

- **Direct Members:** This section displays the members that are directly assigned to the open role. It also displays all members that are assigned via membership rules.

- **Indirect Members:** This section displays the members that are indirectly inherited by the role.

In the Members tab, you can perform the following:

- Assigning Members to a Role

- Revoking Members from a Role

- Opening Member Details

12.5.2.4.7 Assigning Members to a Role

To assign members to a role:

1. In any section of the Members tab, from the Actions menu, select **Assign** (Assign Users). Alternatively, click **Assign User to** on the toolbar. The Assign User to: dialog box is displayed.

2. Search for users by specifying a search criterion in the Search Users field and clicking the search icon. The list of users that matches your search criterion is displayed in the Available list.

> **Note:** An indirect member can be assigned as a direct member.

3. Select one or more users that you want to assign to the open role. Then, click **Move** or **Move All** to move the selected users to the Selected list.

4. Click **Save**. A confirmation message is displayed in role details page.

5. These users are displayed as members in Direct Members section, because the users are assigned directly to the role. Also note that they are also displayed in the All Members section.

> **Tip:**
> - If the member users are not displayed in the Members tab immediately after they are added, then refresh the view.
> - If users are created or updated to match membership rules criteria, they will be assigned directly to this role and the table must be refreshed to view those members in both sections, "All Members" and "Direct Members".

12.5.2.4.8 Revoking Members from a Role

To revoke members from a role:

1. In any section of the Members tab, select the member that you want to revoke.

2. From the Actions menu, select **Revoke** (Revoke Members). Alternatively, click **Revoke Members from:** on the toolbar. The Revoke User from: dialog box is displayed.

3. Search for members by specifying a search criterion in the Search Users field and clicking the search icon. The list of members that matches your search criterion is displayed in the Available list.

> **Note:** Only direct members can be revoked except for the members that are assigned via membership rules.

4. Select one or more members that you want to revoke from the open role. Then, click **Move or Move All** to move the selected members to the Selected list.

5. Click **Save**. A confirmation message is displayed on the role details page.

6. The members that you have revoked are removed from the list of members in the Members tab.

12.5.2.4.9 Opening Member Details

To open the member user details of the open role:

1. In any section of the Members tab, select the member whose details you want to open.

2. From the Actions menu, select **Open** (Open Member Detail). Alternatively, click **Open User** on the toolbar. The user details page for the member is displayed that allows you to view and modify the member details.

12.5.2.5 Viewing Menu Items

You can display all menu items that are permitted for the role. In 11*g* Release 1 (11.1.1), new menu items cannot be assigned to any role. By default, menu items are already assigned to some default roles in Oracle Identity Manager.

> **Note:** The existing menu items cannot be revoked.

To display the menu items for a role:

1. In the browse tree for roles on the left pane, select a role for which you want to display the permitted menu items.

2. From the Actions menu, select **Menu Items**. The Role Details >> Menu Items page is displayed with a list of menu items permitted for the selected role.

12.5.2.6 Viewing, Assigning, and Revoking Access Policies

You can display all available access policies for this role and assign and revoke access policies for the role.

To assign access policies to a role:

1. In the browse tree for roles on the left pane, select the role for which you want to assign access policy.

2. From the Actions menu or Role Details page select **Access Policies**. The Access Policies page is displayed.

3. To assign a new access policy, click **Assign Policy**. The Assign Access Policies page is displayed.

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

4. Select the **Assign** option for the access policies that you want to assign to this role, and then click **Assign**. The Confirmation page is displayed.

5. To assign the access policy, click **Confirm Assign**. The Access Policies page is displayed.

6. To remove this access policy, select the **Delete** option for the access policies that you want to remove from this role, and then click Delete. In the confirmation page, Click **Confirm Delete** to remove access policies from this role

12.5.2.7 Viewing, Assigning, and Revoking Membership Rules

You can display all available membership rules for this role, assign a new membership rule for the role, and remove membership rules.

To work with membership rules:

1. In the browse tree for roles, select the role for which you want to assign or revoke membership rules.

2. From the Actions menu, select **Membership Rules**. The Membership Rules page is displayed.

3. To assign a new membership rule, click **Assign Rules**. The Assign Membership Rules page is displayed. This page displays the name of the membership rule.

4. Select the **Assign** option for the membership rules that you want to assign to this role, and then click **Assign**. The Confirmation page is displayed.

5. To assign the membership rule, click **Confirm Assign**. Otherwise, click **Cancel**. The Membership Rules page is displayed.

6. To revoke this membership rule, select the **Delete** option for the membership rule that you want to remove from this role, and then click **Delete**. In the confirmation page click **Conform Delete** to remove the rules from this role.

12.5.2.8 Updating Data Object Permissions

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

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

12.5.2.8.1 Explicit Insert/Update/Delete Permission Required

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

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

Table 12–7 lists the data objects listed in this category and the entities of these data objects.

Table 12–7   Data Objects Requiring Explicit Insert/Update/Delete Permissions

Data Object Type	Entities
com.thortech.xl.dataobj.tcACS	Organization.Lnk_Act_Svr
com.thortech.xl.dataobj.tcADL	Adapter Factory Logic/SetVariable tasks
com.thortech.xl.dataobj.tcADM	Adapter Factory Input/output parameters
com.thortech.xl.dataobj.tcADP	Adapter Definitions
com.thortech.xl.dataobj.tcADS	Adapter Factory Stored Procedure tasks
com.thortech.xl.dataobj.tcADT	Adapter Tasks
com.thortech.xl.dataobj.tcADU	Adapter Factory WebServices tasks
com.thortech.xl.dataobj.tcADV	Adapter Factory Variables
com.thortech.xl.dataobj.tcAPA	Attestation Process Administrators
com.thortech.xl.dataobj.tcARS	Adapter Statuses
com.thortech.xl.dataobj.tcATP	Adapter Factory Parameter Task Table
com.thortech.xl.dataobj.tcDAV	Data Object Adapter Variable
com.thortech.xl.dataobj.tcDVT	Event handlers associated with data objects
com.thortech.xl.dataobj.tcEMD	Email Definitions
com.thortech.xl.dataobj.tcERR	Error Message Definitions

Table 12–7   (Cont.) Data Objects Requiring Explicit Insert/Update/Delete Permissions

Data Object Type	Entities
com.thortech.xl.dataobj.tcEVT	Event Handlers
com.thortech.xl.dataobj.tcGPY	role Properties
com.thortech.xl.dataobj.tcLKU	Lookup Definitions
com.thortech.xl.dataobj.tcLKV	Lookup values for a lookup
com.thortech.xl.dataobj.tcOBA	Resource object authorizers
com.thortech.xl.dataobj.tcODF	Object To Process Data Flow
com.thortech.xl.dataobj.tcODV	Resource object Events
com.thortech.xl.dataobj.tcOOD	Resource Objects Organization Object Dependencies
com.thortech.xl.dataobj.tcOUD	Resource Objects User Object Dependencies
com.thortech.xl.dataobj.tcPDF	Process Integration Data Flow Mappings
com.thortech.xl.dataobj.tcPKH	Package Hierarchy
com.thortech.xl.dataobj.tcPOC	Access Policies Child Table Data
com.thortech.xl.dataobj.tcPOF	Policy parent data
com.thortech.xl.dataobj.tcPOG	roles defined on access policy
com.thortech.xl.dataobj.tcPOL	Access policy definition
com.thortech.xl.dataobj.tcPOP	Assigned Objects on access policies
com.thortech.xl.dataobj.tcPRF	Process Reconciliation Field Mappings
com.thortech.xl.dataobj.tcPTY	System Configuration
com.thortech.xl.dataobj.tcPWP	Policy Process Targets
com.thortech.xl.dataobj.tcPWR	Password Policies
com.thortech.xl.dataobj.tcPWT	Policy User Targets
com.thortech.xl.dataobj.tcRAV	Prepopulate Adapter Mappings
com.thortech.xl.dataobj.tcRCA	Reconciliation Matched Organizations
com.thortech.xl.dataobj.tcRCH	Reconciliation Event Action History
com.thortech.xl.dataobj.tcRCP	Reconciliation Event Processes Matched
com.thortech.xl.dataobj.tcRCU	Reconciliation Event Users Matched
com.thortech.xl.dataobj.tcRCX	Reconciliation Exceptions
com.thortech.xl.dataobj.tcRES	Adapter Factory Resources
com.thortech.xl.dataobj.tcRGP	Role Membership Rules
com.thortech.xl.dataobj.tcRML	Task Assignment Rules
com.thortech.xl.dataobj.tcRPG	Reports on roles
com.thortech.xl.dataobj.tcRUL	Rules
com.thortech.xl.dataobj.tcRUE	Rule Element
com.thortech.xl.dataobj.tcSDC	User defined columns on system user-defined forms
com.thortech.xl.dataobj.tcSDH	Parent child hierarchy of user defined forms
com.thortech.xl.dataobj.tcSDL	Form Definition Version Label

Table 12–7 (Cont.) Data Objects Requiring Explicit Insert/Update/Delete Permissions

Data Object Type	Entities
com.thortech.xl.dataobj.tcSDP	Form Definition Properties
com.thortech.xl.dataobj.tcSPD	IT Resources Type Parameter Definition
com.thortech.xl.dataobj.tcSRE	Association between user defined columns and pre-populate adapters
com.thortech.xl.dataobj.tcSRS	IT Resource Link
com.thortech.xl.dataobj.tcSUG	IT Resources Administrators
com.thortech.xl.dataobj.tcSVD	IT Resources Type Definition
com.thortech.xl.dataobj.tcTDV	Process Event Handlers
com.thortech.xl.dataobj.tcTLG	System Log
com.thortech.xl.dataobj.tcTSA	Schedule Task Attributes
com.thortech.xl.dataobj.tcTSK	Scheduled Tasks
com.thortech.xl.dataobj.tcUHD	Users Objects History Details
com.thortech.xl.dataobj.tcUPL	User Defined Field Lookups
com.thortech.xl.dataobj.tcUPT	User Defined Field Values
com.thortech.xl.dataobj.tcUPY	System Configuration Users
com.thortech.xl.dataobj.tcWIN	Form Information

12.5.2.8.2 Explicit Permission Not Required

Data objects for which explicit permission is not required are the ones for which permissions do not need to be defined because either there are no permissions enforced or they simply follow parent data object permissions. Data objects that use parent data object permissions follow a simple paradigm that if a role has update permissions on a parent data object, the same role will have insert, update, and delete permissions on child data objects. Table 12–8 lists these data objects and their entities.

Table 12–8 Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
Com.thortech.xl.dataobj.tcMEV	Email definitions defined on task statuses	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcMIL	Process task definitions	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcRSC	Process task response codes	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcUNM	Undo milestones	Follows parent (TOS) permissions.
Com.thortech.xl.dataobj.tcRPC	Reconciliation Matched Processes Child Table	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcAAD	Organization Administrators	Follows parent data object (ACT) permissions.
Com.thortech.xl.dataobj.tcRCE	Reconciliation events	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcPCQ	User Questions	No permission check. Always returns true.
Com.thortech.xl.dataobj.tcUSG	Users in a role	Follows parent data object (UGP) permissions.

Table 12–8   (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcGPP	Role administrators	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcUWP	roles.Navigation Tree Layout	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcMAV	Process Data.Milestone.Adapter Variable	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcAtomic Process	Process Definition	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcATR	Attestation Requests	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIF	Export Import File history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcCIH	Connector Installation history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcORR	Reconciliation Action Rules	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRRE	Reconciliation User Matching Elements	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRPW	Password Policy Rules on resources	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcOBD	Resource Object Dependencies	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcACP	Objects allowed	Follows parent data object (ACT) permissions.
com.thortech.xl.dataobj.tcRCM	Reconciliation Data Multi-Value	No permission check. Always returns true.
com.thortech.xl.dataobj.tcATD	Attestation Task Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcOST	Statuses defined on resource	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcEIS	Export import history substitution	No permission check. Always returns true.
com.thortech.xl.dataobj.tcAPT	Attestation Tasks	No permission check. Always returns true.
com.thortech.xl.dataobj.tcGCD	Generic Connector Definition	No permission check. Always returns true.
com.thortech.xl.dataobj.tcDEP	Process Task Dependencies	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcROP	Process determination rules	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcGPG	Sub roles	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcSEL	roles.Set Up Permissions	Follows parent data object (UGP) permissions.
com.thortech.xl.dataobj.tcQUM	Queue Members	Follows parent data object (QUE) permissions.
com.thortech.xl.dataobj.tcQUG	Queue Administrators	Follows parent data object (QUE) permissions.
com.thortech.xl.dataobj.tcMSG	Milestone.Status.role	This data object has been deprecate
com.thortech.xl.dataobj.tcPUG	Process Integration.Administrators	Follows parent (TOS) permissions.

Table 12–8   (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcOUD	Resource Objects.User Object Dependencies	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRQE	Request Queues	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRVM	Recovery Milestones	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcOUG	Resource Objects.Administrators	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcMST	Process Definition.Tasks.Object Status	Follows parent (TOS) permissions.
com.thortech.xl.dataobj.tcRRT	Reconciliation.User Matching Rule Element Properties	No permission check. Always returns true.
com.thortech.xl.dataobj.tcSVP	IT Resource Properties table	Follows parent (SVR) permissions.
com.thortech.xl.dataobj.tcORF	Resource Objects.Object Reconciliation Fields	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj.tcRCD	Reconciliation Event Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIO	Export and import objects	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRRL	Reconciliation Rules	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRQC	Requests.Comments for Requests	No permission check. Always returns true.
com.thortech.xl.dataobj.tcRCB	Reconciliation Events.Unprocessed Data	No permission check. Always returns true.
com.thortech.xl.dataobj.tcPXD	Proxy Definitions	No permission check. Always returns true.
com.thortech.xl.dataobj.tcEIH	Export and import history	No permission check. Always returns true.
com.thortech.xl.dataobj.tcMAP	Map Information	Not using maps any more.
com.thortech.xl.dataobj.tcORC	Process Detail	Permissions are given to all users role.
com.thortech.xl.dataobj.tcSTA	Process task status Definitions	We do not allow define custom statuses on tasks.
com.thortech.xl.dataobj.tcSchedulEItem	Process task instances	Permissions are given to all users role.
com.thortech.xl.dataobj.tcSCH	Task instance information	Permissions are given to all users role.
com.thortech.xl.dataobj.tcOIO	Requests Object Instance for Organization	Users can never directly create these entities.
com.thortech.xl.dataobj.tcOIU	Requests Object Instance for User	Users can never directly create these entities.
com.thortech.xl.dataobj.tcOBI	Requests.Object Instance	Users can never directly create these entities.
Com.thortech.xl.dataobj.tcREQ	Requests	No permission check for insert. Update and delete permissions are computed using the user relationship to request.

Table 12–8 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcRequest Object	Request Object	No permission check. Always returns true.
com.thortech.xl.dataobj.tcDOB	Data Objects	OIM Users never create data object
Thor.CarrierBase.tcACN	Contacts.Organization Information	Not used anymore.
Thor.CarrierBase.tcAFM	Adapter Factory.Form	Not used anymore.
Thor.CarrierBase.tcAHY	Organization.Parent-Child	Not used anymore.
Thor.CarrierBase.tcCCG	Contact.Organization Roles	Not used anymore.
Thor.CarrierBase.tcESD	Structure Utility.Encrypted Columns	No UI or APIs exposed to define data.
Thor.CarrierBase.tcGSC	Contact.Schedule Items	Not used anymore.
Thor.CarrierBase.tcGSI	Schedule Items.roles	Not used anymore.
Thor.CarrierBase.tcPGP	Process Integration.Request Permissions	Not used anymore.
Thor.CarrierBase.tcUDF	User Defined Field Definition	Not used anymore.
com.thortech.xl.orb.dataobj.tcAOA	Adapter Factory.Open Adapter	Not used anymore.
com.thortech.xl.orb.dataobj.tcOrganizationContact	Organization.Contact Information	Not used anymore.
com.thortech.xl.orb.dataobj.tcRPT	Report Definition	Not used anymore.
com.thortech.xl.dataobj.tcRPP	Report Parameters	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSC	Task Instance.Contact Information	Not used anymore.
com.thortech.xl.orb.dataobj.tcUserScheduleItem	User Tasks	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSI	Users.User Defined Tasks	Not used anymore.
com.thortech.xl.orb.dataobj.tcUSK	Email Notification.USI.Contacts	Not used anymore.
com.thortech.xl.dataobj.tcAAG	roles.Organization Members	Not used anymore.
com.thortech.xl.dataobj.tcORD	Orders	Not used anymore.
com.thortech.xl.dataobj.tcRLO	External JAR File Directory	Not used anymore.
com.thortech.xl.dataobj.tcAGS	Organization.Contact roles	Not used anymore.
com.thortech.xl.dataobj.tcATS	Organization.Services Per Organization	Not used anymore.
com.thortech.xl.dataobj.tcSGK	System Generator Key Values	Not used anymore.
com.thortech.xl.dataobj.tcSRP	Service Rate plan	Not used anymore.
com.thortech.xl.dataobj.tcSRS	Service Rate plan	Not used anymore.
com.thortech.xl.dataobj.tcUDP	User Defined Fields	Not used anymore.
com.thortech.xl.dataobj.tcUPD	Users Objects Policy Details	Users can never directly create thes entities.
com.thortech.xl.dataobj.tcUPP	Users Objects Policy Profile	Users can never directly create thes entities.
com.thortech.xl.dataobj.tcUPH	Users Objects Policy History	Users can never directly create thes entities.

Table 12–8 (Cont.) Data Objects Not Requiring Explicit Permissions

Data Object	Description	Permission Type
com.thortech.xl.dataobj.tcRQU	Request Object Target User Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQA	Request Target Organization Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQO	Request Object Information	Follows associated request permissions.
com.thortech.xl.dataobj.tcRIO	Request Organizations Resolved Object Instances	Follows associated request permissions.
com.thortech.xl.dataobj.tcRIU	Request Users Resolved Object Instances	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQY	Request Organizations Requiring Resolution	Follows associated request permissions.
com.thortech.xl.dataobj.tcRQZ	Request Users Requiring Resolution	Follows associated request permissions.
com.thortech.xl.dataobj. tcUserProvisionObject	User Provision Object	Follows parent (OBJ) permissions.
com.thortech.xl.dataobj. tcOrgProvisionObject	Organization Provision Object	Follows parent (OBJ) permissions.
Com.thortech.xl.dataobj.tcMEV	Email definitions defined on task statuses	Follows parent (TOS) permissions.

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

- To assign a data object to a role with, say insert and update permissions, a user who is logged in must have insert and update permissions on that data object.

- In order to modify any data permission (insert/update/delete) on a role, a user who is logged in must have the same permissions on that data object.

- To be able to delete a data object permission from a role, a user who is logged in must have insert and update permissions on the same data objects.

- If a user who is logged in updates data object permissions that result in no permissions on a data object, the system automatically deletes that entry from the role.

12.5.3 Creating and Managing Role Categories

Role categories are a way of categorizing roles for the purpose of navigation and authorization. Role categories are internally stored in Oracle Identity Manager as an attribute of the role and is reconciled with the multivalued business category attribute in the LDAP identity store. If the value in LDAP is empty, then the role is assigned to the system-managed Uncategorized role category. If the value in LDAP has multiple values or a single, unrecognized value, then the role reconciliation process does not reconcile the role and generates reconciliation errors in Oracle Identity Manager.

The default role categories in Oracle Identity Manager are:

- **OIM Roles:** All the predefined roles in Oracle Identity Manager are assigned to this category. These are roles that exist in Oracle Identity Manager by default and are primarily used for managing permissions. There will not be any corresponding entity in LDAP store for these predefined roles

- **Default:** A newly created role must have a role category. Therefore, if a role category is not specified at the time of creating the role, then the role is assigned to this category by default.

This section describes the following topics:

- Creating a Role Category
- Searching Role Categories
- Modifying a Role Category
- Deleting a Role Category

12.5.3.1 Creating a Role Category

To create a role category:

1. Login to Oracle Identity Administration.

2. In the Welcome page, under Roles, click **Create Role Category**.

    Alternatively, in the Browse tab of the left pane, expand Roles, and from the Actions menu, select **Create Category**. Otherwise, click **Create Category** icon on the toolbar.

    The Create Role Category page is displayed.

3. In the Category Name box, enter the name of the role category.

4. In the Description box, enter a description for the role category. This step is optional.

5. Click **Save**. A page is displayed with a message on the top of the page stating that the role category is created. The page consists of the Attributes and Roles tabs.

    The Attributes tab displays the attributes of the role category. You can edit the fields in this tab to edit the role category.

    The Roles tab displays the list of roles belonging to the role category.

12.5.3.2 Searching Role Categories

To search for role categories:

1. In the Welcome page, under Roles, click **Advanced Search - Role Categories**. The Advanced Search: Categories page is displayed.

2. In the Category Name field, enter a search criterion. You can enter the asterix wildcard character (*) in the search criterion.

3. From the list adjacent to the Category Name field, select a search comparator. The default search comparator is Begins With. However, Equals search comparator can be used.

4. If you want to add a field to the search condition, then click **Add Fields**. From the list, select **Description**. The Description field is added to the Advanced Search: Categories page. You can specify a search criterion in the Description field to search by description.

    To remove the Description field from the search condition, click the cross icon adjacent to the Description field.

5. Click **Search**. The categories that match search criteria you specified are displayed in the search results table.

12.5.3.3 Modifying a Role Category

To modify a role category:

1. In the Browse tab of the left pane, expand **Roles**.

2. Select the role category that you want to modify.

3. From the Actions menu, select **Open**. Alternatively, click the **Open Role or Category Detail** icon on the toolbar. A page with details about the role category is displayed.

4. The Attributes tab is open by default. Edit the fields in this tab to modify basic category information such as name and description. When finished, click **Apply**.

5. Click the **Roles** tab. In this tab, you can view all roles that are assigned to this category.

   To view role details assigned to a role category:

   a. In the Roles tab of the role category details page, select the role that you want to view details.

   b. From the Actions menu, select **Open** (Open Role Detail). Alternatively, you can click **Remove Role** on the toolbar. The Role Detail page for the selected role is displayed.

12.5.3.4 Deleting a Role Category

To delete a role category:

1. In the browse tree for roles in the left pane, select a role category that you want to delete.

2. From the Actions menu, select **Delete Role Category** in role category detail page. Alternatively, click the **Delete Role or Category** icon on the toolbar. A message box is displayed asking for confirmation.

3. Click **Yes**. The role category is deleted.

12.6 Managing Authorization for Roles

When a user logs in to Oracle Identity Manager, the links, buttons, and menus associated with the actions that the user can perform are displayed. For example, on the Welcome page of Oracle Identity Manager Administration, the **Advanced Search - Roles** link is displayed if the user is authorized to perform advanced search for roles. The actions that the user is authorized to perform is determined by the authorization policies. These authorization policies are defined for Oracle Identity Manager and stored in Oracle Entitlements Server (OES). The policies are enforced at runtime to control the authorization to perform various tasks in the UI.

> **See Also:**   Chapter 15, "Managing Authorization Policies" for detailed information about authorization policies

Authorization policies control the access to various operations with the help of permissions. Table 12–9 lists the permissions for role management operations:

Table 12–9   Role Management Permissions

Permission	Description
Create Role	Determines if the user can create a role **Note:** This permission is not associated with a specific role.
Modify Role	Determines if the user can update a specific role
Delete Role	Determines if the user can delete a specific role
View Role Detail	Determines if the user can view a specific role and the complete hierarchy of the specific role
Search for Role	Determines if the user can search for roles **Note:** This permission is not associated with a specific role.
Modify Role Membership	Determines if the user can grant or revoke a specific role to a user.
Modify Role Hierarchy	Determines if the user can add or remove a child role to or from a specific role
View Role Membership	Determines the user to whom the specific role is granted
Create Role Category	Determines is the user can create a role category **Note:** This permission is not associated with a specific role category or role.
Modify Role Category	Determines if the user can update a role category **Note:** This permission is not associated with a specific role category or role.
Delete Role Category	Determines if the user can delete a role category **Note:** This permission is not associated with a specific role category or role.
View Role Category Detail	Determines if the user can view the details of a role category **Note:** This permission is not associated with a specific role category or role.
Search for Role Categories	Determines if the user can search for role categories **Note:** This permission is not associated with a specific role category or role.

> **Note:** When a role is granted to a user, the Modify Role Membership permission must be granted to the specific role that you are trying to grant.

Permissions are enforced by authorization policies, which regulate the way permissions are granted. The default authorization policies for the role management feature allow Oracle Identity Manager to function properly. Without these policies, you cannot access or perform any task in Oracle Identity Manager. This applies to the administrators and users.

You can create custom authorization policies to enforce delegated administration by using the Authorization Policy tab of Oracle Identity Administration. The following must be specified while creating an authorization policy:

- Policy name and description
- Oracle Identity Manager feature for which the policy is being created

- Set of permissions associated with various actions

- Assignment of policy to roles decides who gets the permissions via the role membership

- Data constraint, which is a set of roles on which the actions specified in the policy can be performed. Hierarchy is supported in the data constraints. Therefore, all roles that are part of the hierarchy are included in the data constraint. This allows you to create a simple policy with only few roles listed in the constraint, but that includes a much bigger set of roles based on the hierarchy.

> **See Also:**
>
> - "Role Management" on page 15-13 for information about the default authorization policies for this feature
>
> - "Creating an Authorization Policy for Role Management" on page 15-5 for information about creating custom authorization policies for role management

13

Managing Organizations

An organization entity represents a logical container of entities such as users and other organizations in Oracle Identity Manager.

Organizations are containers that can be used for delegated administrative models. In addition, an organization defines the scope of other Oracle Identity Manager entities, such as users. Oracle Identity Manager can have a flat organization structure or a hierarchical structure, which means that an organization can contain other organizations. The hierarchy represents departments, geographical areas, or other logical divisions facilitating management of Oracle Identity Manager entities.

To scale the ability to manage a large number of roles and people in an organization of a significant size by using delegated administration, Oracle Identity Manager provides the ability to define delegated administration policies based on the membership of an object within a hierarchy. This also supports recursive organization membership, such as the hierarchy shown in Figure 13–1:

Figure 13–1 Recursive Organization Membership
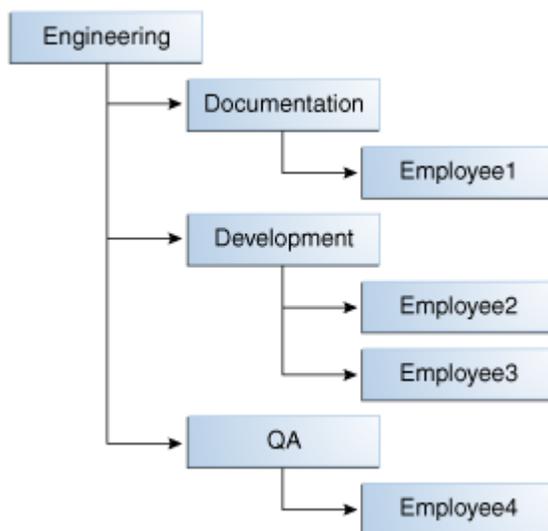
If a hierarchical delegated administration policy is defined to provide Delegated Administrator1 the permission to reset password starting from Engineering, then the permission is granted for Employee1, Employee2, Employee3, and Employee4. If the membership root is Development, then Bob has the permission for Employee2 and Employee3 only.

The functional description of the organization services and the UI components that support these services are described in the following sections:

- Organization Entity Definition

- Organization Management Tasks

- Organization Management Authorization

13.1 Organization Entity Definition

In Oracle Identity Manager, attributes are defined by default for the organization entity. You can also add your own attributes to the organization entity.

The following attributes are defined for organization entity attributes:

- **Attribute Name:** The name of the attribute.

- **Category:** The category for the attribute. The categorization is used to organize the data in the UI.

- **Type:** The type of the attribute, such as string, data, number, or boolean.

- **display-type:** The display type of the attribute in the UI, such as single line text, multi-line text, e-mail address, radio button, List of Values (LOV).

> **Note:** The list of values can come from an API call or a system defined list of values, or you can add your own values.

- **Properties:** For each attribute, you must configure the following properties:

  - **Required:** Determines if the organization in the repository must have a non-null value for this attribute or not

  - **System Controlled:** Determines if the value can only be set and edited by the system itself

  - **System Can Default:** Determines if the value can be set by the system to a default if no value is provided

  - **Encrypted:** Determines if the value is stored in the repository as hashed (Hash), reversible encrypted (Encrypt), or clear (Clear)

  - **Searchable:** Determines if the value can be used in searches or not

  - **Unique:** Determines if the value must be unique across all organizations in the repository or not

Table 13–1 lists the default attributes of the organization entity:

Table 13–1   Default Attributes of the Organization Entity

Attribute Name	Category	Type	Data Type	Display Type	Properties
Organization	Basic	Single	String	Single line text	Required: Yes System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: Yes
Organization Type	Basic	Single	String	LOV	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No
Parent Organization	Basic	Single	String	Single line text	Required: No System Can Default: No System Controlled: No Encrypted: Clear Searchable: Yes Unique: No
Status	Basic	Single	String	Single line text	Required: Yes System Can Default: Yes System Controlled: Yes Encrypted: Clear Searchable: Yes Unique: No

13.2 Organization Management Tasks

The tasks related to organization management are performed in the Organization Management section of Oracle Identity Management Administration. The tasks are described in the following sections:

- Searching Organizations
- Browsing Organizations
- Creating an Organization
- Viewing and Modifying Organizations
- Disabling and Enabling Organizations
- Deleting an Organization

13.2.1 Searching Organizations

Oracle Identity Administration allows you to perform the following types of organization search operations:

- Performing Simple Search

- Performing Advanced Search

13.2.1.1 Performing Simple Search

The simple search operation lets you search organization entities based on the search strings that you specify as search attributes. This operation is also referred to as simple search or quick search.

To perform a simple search for organizations:

1. Login to Oracle Identity Administration.

2. In the Administration tab on the left pane, from the drop-down list, select **Organizations**.

3. In the Search field, enter an organization name as a search criterion. You can include wildcard characters (*) in your search criterion. For performance reasons, initial (prefix) wildcards will be removed. However, a trailing (prefix) wildcard will be added to all searches.

4. Click the search icon. In the Search Results tab, the search result is displayed in a table that shows the organization names that matched the search criterion. Figure 13–2 shows the search results table:

Figure 13–2 Organization Search Result

13.2.1.2 Performing Advanced Search

Advanced search for organizations allows you to specify more complex search criteria than the simple search operation. The results are displayed in search results table.

To perform advanced search for organizations:

1. Login to Oracle Identity Administration.

2. In the Welcome page, under Organizations, click **Advanced Search - Organizations**. The Advanced Search page is displayed on the right pane.

3. Select any one of the following:

   - **All:** Search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

   - **Any:** Search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

4. In the Organization Name field, enter the organization name search attribute that you want to search. To do so, select a search comparator. The default search comparator is "Begins With". The comparator "Equals" is available in the pulldown list as an alternative. See "Search Comparators" on page 11-17 for more information about search comparators.

You can use wildcard characters to specify the organization name.

5. From the Organization Customer Type list, select the organization type. The organization type can be Branch, Department, or Company.

6. From the Add Fields button, select **Organization Status**.

7. From the Organization Status list, select the organization status, which can be Active, Deleted, or Disabled.

8. Click **Search**. The results are displayed in the search results table, as shown in Figure 13–3. The search results table displays the organization name, parent organization, organization customer type, and organization status.

Figure 13–3 Advanced Search

13.2.2 Browsing Organizations

You can browse data in the Organizations section in Oracle Identity Manager Administration. The browse functionality is available in the left pane of the UI.

Using the browse operation, you can navigate through the organization tree in the system, starting at the root organization. If there are multiple organization trees, then all the trees are displayed. Each tree starts at a root organization node, which has no parent organization. The users defined in the organization are not displayed as nodes in the tree.

To browse through organizations, in the left pane of Oracle Identity Manager Administration, under the Browse tab, click **Organization**. All the organizations in Oracle Identity Manager are displayed in the browse list, as shown in Figure 13–4:

Figure 13–4   Organization Browse List

The organization browse list shows the organizations trees with the root and child organizations.

In the organization browse list, you can perform the following:

- Create an organization. See "Creating an Organization" on page 13-6.

- Open the details of an organization. See "Viewing and Modifying Organizations" on page 13-8.

- Delete an organization. See "Deleting an Organization" on page 13-14.

- Manage administrative roles: See "Managing Administrative Roles" on page 13-11.

13.2.3 Creating an Organization

You create an organization by using the Create Organization page. You can access this page only if you are authorized to create an organization.

> **Note:**   You are allowed to create an organization only if you have the Create Organization privilege for one or more organizations.

To create an organization:

1. Open the Create Organization page. To do so, perform any one of the following:

    - In the Welcome page of Oracle Identity Manager Administration, under Organizations, click **Create New Organization**.

    - In the left pane, click the **Browse** tab. Under Organizations, from the Action menu, select **Create**. You can also click the Create icon on the toolbar.

    - In the left pane, click the **Search Results** tab with Organizations selected in the search list. From the Actions menu, select **Create**. You can also click the Create icon on the toolbar.

    - In the Advanced Search: Organization page, from the Actions menu, select **Create Org**, or click **Create** on the toolbar.

    Figure 13–5 shows the Create Organization page.

Figure 13–5   The Create Organization Page

2. Enter values in the fields in the Create Organization page. Table 13–2 lists the fields in the Create Organization page:

Table 13–2   Fields in the Create Organization Page

Field	Description
Name	The name of the organization
Type	The type of the organization, either Company, Department, or Branch
Parent Organization	The organization to which the newly created organization will belong

3. In the Name field, enter the name of the organization.

4. In the Type field, select the type of the organization, such as Company, Department, or Branch.

5. Specify the parent organization to which the newly created organization will belong. To do so:

   a. Click the search icon next to the Parent Organization field. The Search: Organizations dialog box is displayed, as shown in Figure 13–6:

Figure 13–6   The Search: Organizations Dialog Box

   b. Select any one of the following options:

   – **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

–   **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

c.   In the Organization Name field, enter the organization name that you want to search. You can use wildcard characters in your search criteria. Select a search condition in the list adjacent to the Organization Name field. The search conditions include "Equals" or "Begins With".

d.   In the Organization Customer Type field, enter the organization type of the parent organization. You can use wildcard characters in your search criteria. Select a search condition in the list adjacent to the Organization Customer Type field.

e.   Click **Search**. The organizations that match the search criteria you specified are displayed in the search results table.

f.   From the search results table, select the organization that you want to specify as the parent organization.

g.   Click **Finish**. The selected organization is added as the parent organization.

6.   Click **Save** to create the organization.

13.2.4 Viewing and Modifying Organizations

The view organization operation allows you to view detailed organization profile information in the User Details page. You can view this page only if you are authorized to view the organization profile as determined by the authorization policy on the View Organization Detail privilege. If you have the authorization to modify the organization, then you can also modify the organization by using this page.

> **Note:**   The organization details page for the organization entity is auto-generated by the system based on configuration and fine-grained authorization. In Oracle Identity Manager, there is no mechanism to override the system-generated page with a custom-defined page.

To open the details of an organization, perform any one of the following:

■   In the left pane of Oracle Identity Manager Administration, click the **Browse** tab. Under Organization, select the organization whose details you want to display. From the Actions menu, select **Open**. Alternatively, click the Open icon on the toolbar.

■   Perform a simple search for the organization whose details you want to display. From the search result, select the organization. From the Actions menu, select **Open**. Alternatively, click the Open icon on the toolbar.

■   Perform an advanced search for the organization whose details you want to display. From the advanced search result, select the organization, and from the Actions menu, select **Update Org**. Alternatively, click **Open** on the toolbar.

The organization details page is displayed, as shown in Figure 13–7:

Figure 13–7   The Organization Details Page

You can perform administrative organization modifications in the organization details page. The modification is divided across the different sections of the organization details page, which means that modifications done in each section are independent of each other and must be saved individually. The modification for each section is described in the following sections:

> **Note:**   You must have "organization create" permission to update or delete organizations.

- Modifying Organization Attributes
- Viewing Child Organizations
- Viewing User Information
- Modifying Resources

13.2.4.1 Modifying Organization Attributes

The Attributes tab, as shown in Figure 13–7, of the organization details page displays attributes of the organization. If you are authorized to modify the organization profile as determined by authorization policy on the Modify Organization Profile privilege, then the organization details page opens in editable mode and you can modify organization information. You can modify the values for the attributes, and then click **Save** to save the changes.

Whether or not the logged-in user is allowed to modify the organization is controlled by authorization policies. If you are not allowed to modify the organization, then the organization details page is displayed in read-only mode with no editable fields. See "Organization Management Authorization" on page 13-14 for information about authorization of the organization management feature.

> **Note:**   The Status attribute in the organization details page is read-only.

13.2.4.2 Viewing Child Organizations

The Hierarchy tab is a read-only tab that displays a list of child organizations that the selected organization has. For each child organization in the list, the following are displayed:

- Organization name

- Type

- Status

From the Hierarchy tab, you can open the details of a child organization by selecting the organization, and selecting **Open** from the Actions menu. Alternatively, you can click **Open** on the toolbar, or simply click the name of the organization.

To modify a child organization, click the child organization name that you want to modify. The organization details page for the selected organization is displayed, by using which you can modify the details of that organization.

13.2.4.3 Viewing User Information

The Members tab is a read-only tab that displays a list of users in the selected organization. For each user in the list, the following are displayed:

- User Name

- First Name

- Last Name

- Manager Name

From the Members tab, you can open the details of a user by selecting the user, and selecting **Open** from the Actions menu. Alternatively, you can click **Open** on the toolbar, or simply click the name of the user.

> **Tip:** You can add or remove users to and from organizations by using the Attributes tab of the user details page. For more information, see "The Attributes Tab" on page 11-23.

13.2.4.4 Modifying Resources

The Resources tab displays the permitted resources for the selected organization. You can select one or multiple resources in the list, and then perform the following:

- Provisioning Resources

- Revoking Resources

13.2.4.4.1 Provisioning Resources To provision resources to the organization:

1. From the Actions menu, select **Provision**. Alternatively, click **Provision** on the toolbar. This brings up a wizard " Step 1: Select a Resource".

2. Search for the resource that you want to provision. Select the resource and click **Continue**.

3. In the Step 2: Verify Resource Selection page, the resource that you selected for adding to the organization is displayed. Verify the information and click **Continue**. Provisioning the selected resource to the organization starts.

4. Close the Provision Resource to Organization wizard. The resource is added to the Hierarchy tab.

> **Tip:** If the provisioned resource is not displayed in the Hierarchy tab, then click **Refresh** on the toolbar.

13.2.4.4.2 Revoking Resources To revoke a resource:

1. Select the resource that you want to remove.

2. From the Actions list, select **Revoke**. Alternatively, click **Revoke** on the toolbar. A message is displayed asking for confirmation.

3. Click **OK** to confirm.

13.2.5 Disabling and Enabling Organizations

> **Note:**
>
> - You cannot disable organizations with child orgs or users. You can force delete it only by setting the system property ORG.DISABLEDELETEACTIONENABLED to true. Once you set the property, the users and sub orgs will be deleted while deleting the parent org.
>
> - You can disable an organization only if you have the "Write" permission for that organization.

To disable an organization with enabled state:

1. In the organization details page, click **Disable Organization** on the top of the page. A message is displayed asking for confirmation. Alternatively, in the simple search result for organizations, select the organization, and from the Actions menu, select **Disable**.

2. Click **OK** to confirm. A message is displayed stating that the organization is successfully disabled.

3. Click **OK**.

To enable an organization with disabled state:

1. In the organization details page, click **Enable Organization** on the top of the page. Alternatively, in the simple search result for organizations, select the organization, and from the Actions menu, select **Enable**. A message is displayed asking for confirmation.

2. Click **OK** to confirm. A message is displayed stating that the organization is successfully enabled.

3. Click **OK**.

> **Note:** You can enable an organization only if you have the "Write" permission for that organization.

13.2.6 Managing Administrative Roles

The organization details page allows you to view and define a list of administrative roles and associated permissions that can administer the selected organization. To assign administrative roles to an organization, you must have the appropriate permission to create an organization. To assign permission to create organization:

1. On the role detail page for the role to which you want to assign administrative privileges for organizations, click **Data Object Permissions**. The Role Details >> Permissions page is displayed.

2. Click **Assign**. The Assign Permissions page is displayed with a list of permission names that you can select to assign the permissions to the role.

3. For the Organizations permission, select the **Allow Insert** option. This grants the "create organization" permission to the orgadmin role. Then select the **Assign** option to the right of the "Organizations" permission.

4. Click **Assign**. A message is displayed asking for confirmation.

5. Click **Confirm Assign**. The permission is assigned to the role.

To assign administrative roles to an organization:

> **Note:** The "Insert" permission is a prerequisite to Write and Delete permissions. Expanding the "Insert" permission allows you to create new organizations. The "Write" permission allows to update, enable, and disable organizations. The "Delete" permission enables to delete the organization.

1. Open the Administrative Roles page by selecting any one of the following:

   - In the organization simple search result, select an organization. From the Actions menu, select **Administrative Roles**.

   - In the Browse tab on the left pane, select an organization. From the Actions menu, select **Administrative Roles**.

   - In the organization detail page, click **Administrative Roles**.

2. On the Administrative Roles page, in the Filter By Role Name, enter a search criterion to search for administrative roles that can administer the organization. Then, click **Search**. A list of roles with associated permissions are displayed.

3. To unassign any role from the organization, select the **Unassign** option to the right of the administrative role, and click **Unassign**.

4. To assign an administrative role to the organization:

   a. Click **Assign**. The Assign page is displayed with a list of available roles.

   You can filter the role names by entering a search criteria in the Filter By Role Name box, and clicking **Find**.

   Note that the Read options are selected by default for all the roles.

   b. Select the **Write**, **Delete**, and **Assign** options for the administrative roles to provide write, delete, and assign administrative permissions respectively.

   c. Click **Assign**.

5. To update permissions for the administrative roles:

   a. Click **Update Permissions**. The Update page is displayed with a list of administrative roles, whose permissions you can modify.

   You can filter the role names by entering a search criteria in the Filter By Role Name box, and clicking **Find**.

   Note that the Read options are selected by default for all the roles.

    b. Select or deselect the **Write** and **Delete** options for the administrative roles to modify the write and delete permissions respectively.

    c. Click **Update**.

6. When finished, close the Administrative Roles page. Figure 13–8 shows the Administrative Roles page.

Figure 13–8   Assign Administrative Roles

13.2.7 Managing Permitted Resources

The Permitted Resources page allows you to assign and update a list of permitted resources to the users of the selected organization.

1. To assign permitted resources to the users in the selected organization:

    a. In the Browse tab on the left pane, select an organization. From the Actions menu, select **Open**.

    b. In the organization detail page, click **Permitted Resources**.

    c. In the Permitted Resources page, select the resources and click **Assign**.

2. To update the resources allowed to the selected organization:

    a. In the Browse tab on the left pane, select an organization. From the Actions menu, select **Open**.

    b. In the organization detail page, click **Permitted Resources**.

    c. In the Permitted Resources page, select the resources and click **Update**.

Figure 13–9 shows the Assign Permitted Resources page.

Figure 13–9   Assign Permitted Resources
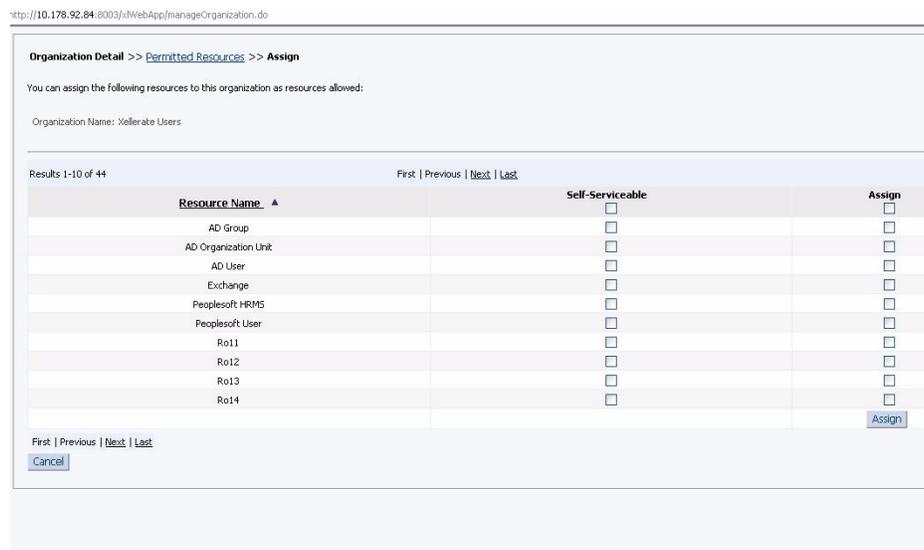
13.2.8 Deleting an Organization

> **Note:**
>
> ■   You cannot delete organizations with child orgs or users. You can force delete it only by setting the system property ORG.DISABLEDELETEACTIONENABLED to true. Once you set the property, the users and sub orgs will be deleted while deleting the parent org.
>
> ■   You can delete an organization only if you have the "Delete" permission for that organization.
>
> ■   The deleted record would still exist in the database, marked deleted.

To delete an organization:

1.   In the advanced search result for organizations, select the organization that you want to delete.

2.   From the Actions menu, select **Delete**. A message is displayed asking for confirmation. Alternatively, in the simple search result for organizations, select **Delete** from the Actions menu. Otherwise, in the Browse tab, select **Delete** from the Actions menu, or on the organization details page, click **Delete Organization**.

3.   Click **OK** to confirm. A message is displayed stating that the organization is successfully deleted.

4.   Click **OK**.

13.3 Organization Management Authorization

Authorization of the organization management feature is based on organization administrative roles. The following sets of distinct permissions is required by a role to manage an organization:

- The role must have the following data object permission on organization entities:

  - Insert - This enables the user (with this role) to create new organizations and manage them.

  - Enable/Disable/Update

  These permissions are not specific to a particular organization.

- When role is assigned as an administrative role for an organization, the following permissions are required:

  - "Read and View" permissions are implicit by virtue of being administrative role

  - Write

  - Delete

  These permissions are configured per organization.

Permission to get access to Oracle Identity Manager Administration from Oracle Identity Manager Self Service is governed by "menu item" permissions. When the user has access to Oracle Identity Manager Administration, the user is allowed to browse users, roles, and organizations.

Second level menus for edit, view, and delete actions on user and role entities are derived from the OES policies, such as create, update, delete on user and role respectively.

Similarly, second level menus to edit, view, and delete organizations is derived from "orgadmin role" and "data-object" permissions on organization entity type.

In Oracle Identity Manager 11*g* Release 1 (11.1.1), "delegated administration" permissions are managed by using Oracle Entitlements Server (OES) authorization policies. These OES policies for user management can be used to control:

> **See Also:** Chapter 15, "Managing Authorization Policies" for information about OES authorization policies

- Under which organizations you can create or modify users

- Data constraints can specify that you can change users in a set of organizations with or without hierarchy.

Together these capabilities give us the delegated administrative model.

To configure a delegated administrator for an organization:

1. Define a custom authorization policy to manage users and set organization constraints. Organization constraints can be hierarchy aware. See "Creating Custom Authorization Policies" on page 15-4 for information about creating custom authorization policies and setting data constraints.

2. Add the user to the role specified in the custom policy. See "Adding and Removing Roles" on page 11-25 for information about adding a user to a role.

3. To configure the role as organization administrator, first create a role. See "Creating Roles" on page 12-10.

   When you create the orgadmin role, the role detail page for this role is displayed.

4. Assign this orgadmin role "data object" permissions on the organization type. With this "data object" permission, the user (with this role), can create new organizations and manage them. See "Managing Administrative Roles" on

page 13-11 for information about assigning "create organization" permission to a role.

5. Select an organization and assign the orgadmin role as administrative role for the organization. This step would give the user the ability to manage the selected organization. Manage permissions include update, enable, disable, and delete. See "Managing Administrative Roles" on page 13-11 for information about assigning administrative roles to an organization.

14

Creating and Searching Requests

A User in Oracle Identity Manager can manage Requests by creating, searching, or performing other operations on requests from Oracle Identity Manager Advanced Administration if the user belongs to "REQUEST ADMINISTRATORS" group.

This chapter describes the request management feature in the following sections:

> **See Also:** "Managing Requests" on page 10-1 for information about request management concepts and tasks

- Creating Requests by Using Oracle Identity Manager Advanced Administration
- Searching and Tracking Requests

14.1 Creating Requests by Using Oracle Identity Manager Advanced Administration

You can log in to Oracle Identity Manager Advanced Administration and create requests for yourself and for others if your role has the appropriate privileges. You can also create requests by using Oracle Identity Manager Self Service.

Creating requests is described with the help of the following scenarios:

- Creating a Request To Create a User
- Creating a Request to Provision a Resource to Users
- Creating a Request to Deprovision Resources

14.1.1 Creating a Request To Create a User

To create a request to create a user:

1. In Oracle Identity Manager Advanced Administration, click the **Administration** tab, and then click **Requests**.

2. From the Actions menu on the left pane, select **Create Request**. Alternatively, you can also click the Create Request icon on the toolbar. The Select Request Template page of the Create Request wizard is displayed.

    > **Note:** The steps in the Create Request wizard are dynamically generated based on the selection of the request template in the first step.

3. From the Request Template list, select the request template based on which you want to create the request. The dropdown list shows all the default request templates as well as the custom templates that are created based on the request types. In this example, select **Create Contractor**, and then click **Next**.

Note:

- The Create Contractor request template is not a default request template and is available for selection when a request template with the same name is created based on the privileges you have. For the purpose of this scenario, this request template has been created based on the Create User request type for creating user accounts for contract employees. For information about creating this request template, see "Creating a Request Template Based on the Create User Request Type" on page 17-2".

- The Create Role, Modify Role, and Delete Role request templates are not available in the Request Templates list. This is because request creation by using any request template that are based on the Create Role, Modify Role, and Delete Role request types are supported from the APIs, but not in the UI. However, you can search for these request templates in the Request Templates tab. In addition, the Create Role, Modify Role, and Delete Role request types can be used to create approval policies and new request templates.

---

4. In the Enter Details page, specify values for the user attributes. The fields for the user attributes are displayed as defined in the Create Contractor request template. For example, the Middle Name attribute is not displayed if you have already specified a value for it at the template level. For the Organization attribute, an LOV is available, whose values are also defined at the template level. For details about specifying these values, see "Creating a Request Template Based on the Create User Request Type" on page 17-2.

   After specifying values for the user attributes, click **Next**.

5. In the Enter Additional Data page, enter the value of the attribute that is specified as additional data in the request template that you are using to create this request. In this example, Date of Birth is specified as an additional attribute in the request template. Enter a value in the Phone Number field, and then click **Next**.

Note: The Enter Additional Data page is displayed dynamically based on the additional data specified in the request template.

---

6. In the Confirm page, specify values for the Effective Date and Justifications fields. Effective date is the date from which the request will be active after approval. For example, after a create user request is approved, the user is created in Oracle Identity Manager on the date specified in the Effective Date field. The Justification field is a justification for creating the request that might help the approver in approving or rejecting the request.

   On clicking Finish, a request to create a user based on the Create Contractor request template is created.

14.1.2 Creating a Request to Provision a Resource to Users

To create a request to provision a resource to one or more users:

> **Note:** The following request types are similar in nature in terms of request creation and execution:
>
> - Provision Resource
> - Modify Provisioned Resource

1. In Oracle Identity Manager Advanced Administration, click the **Administration** tab, and then click the **Requests** tab.

2. From the Actions menu on the left pane, select **Create Request**. The Select Request Template page of the Create Request wizard is displayed. The steps in this wizard are dynamically generated based on the selection of the request template in the first step.

3. From the Request Template list, select the request type or request template based on which you want to create the request. In this example, select **Provision E-Business Resource**, and then click **Next**.

> **Note:** The Provision E-Business Resource request template is not a default request template and is available for selection when a request template with the same name is created based on the privileges you have. For the purpose of this scenario, this request template has been created based on the Provision Resource request type for provisioning an E-Business resource to a user. For information about creating this request template, see "Creating a Request Template Based on the Provisioning Resource Request Type" on page 17-6

4. In the Select Users page, specify a search criteria in the fields to search for the users that you want to provision the resource, and then click Search. A list of users that match the search criteria you specified is displayed in the Available Users list.

5. From the Available Users list, select one or more users to whom you want to provision the resource. You can select one or more users that are your direct reports. In other words, you can select one or more users for whom you are the manager as specified in the user's profiles.

   Click **Move** to include your selection in the Selected Users list, and then click **Next**.

> **Note:** In this page, available users list is shown based on the OES policies on user entities. The users cannot be restricted from the request template.

6. In the Select Resources page, search for the available resources. From the Available Resources list, select the resources that you want to provision, click **Move** or **Move All** to include the selected resources in the Selected Resources list. In this example, select **E-Business RO** as the resource to be provisioned, and then click **Next**.

> **Note:** Only the E-Business RO resource is displayed in the Selected Resources list because the Provision E-Business Resource request template is created only for provisioning the E-Business resource. The resources are displayed in the Selected Resources list based on the resource selection in the request template.

7. In the Resource Details page, specify values for the attributes of the resource.

   In this example, you can select the life span of the E-Business resource being provisioned to the selected user or users. In the Life Span Type lookup, select a life span type, such as Short term, Mid term, or Long term. In the Server lookup, select the name of the E-Business server to connect to. For the Oracle Apps User Responsibilities parent attribute, you can enter multiple sets of values for the Responsibility Start Date, Responsibility End Date, and Responsibility Name child attributes. To do so, select values in the fields, and then click **Add**. Repeat entering another set of values in the Responsibility Start Date, Responsibility End Date, and Responsibility Name fields, and then click **Add**. For information about defining parent and child attributes, see "Creating a Request Template Based on the Provisioning Resource Request Type" on page 17-6 and "Request Dataset" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

   Specify values for all other resource attributes, and then click **Next**.

   If you select multiple resources in the Select Resources page, then the Resource Details page for each selected resource is displayed one by one. For instance, in the Select Resources page, you select the E-Business and Active Directory resources. The Resource Details page for the E-Business resource is displayed. Enter values for all attributes of the E-Business resource, and click **Next**. Then, the Resource Details page for the Active Directory resource is displayed. Specify values for all attributes of the Active Directory resource, and click **Next**.

8. In the Justification page, you can specify values for the following fields, and then click **Finish** to submit the request.

   - **Effective Date:** Enter the date when you want the underlying operation of the request to be executed after approval. For example, if you specify September 15 as the effective date for provisioning a laptop to a user, then the laptop is not provisioned to the user before September 15 even if the request is approved. The resource is provisioned on September 15. If the request is approved after September 15, then the resource is provisioned with immediate effect.

   - **Justification:** Enter a justification for creating the request.

   If you have selected a user to provision the resource, then the request is available for approval. If you have selected multiple users to provision the resource, then the request is broken into multiple child requests for operation level approval, and each child request can be approved or rejected independently.

14.1.3 Creating a Request to Deprovision Resources

To create a request to deprovision one or more resources:

> **Note:** The following request types are similar in nature in terms of request creation and execution:
>
> - Enable Provisioned Resource
> - Disable Provisioned Resource
> - De-Provision Resource

1. In the Welcome page of Oracle Identity Manager Advanced Administration, under Administration, click **Requests**. Alternatively, you can click the **Administration** tab, and then click **Requests**.

2. From the Actions menu, select **Create Request**. Alternatively, you can click the create request icon on the toolbar. The Select Request Template page of the Create Request wizard is displayed. The steps in this wizard are dynamically generated based on the selection of the request template in the first step.

3. From the Request Template list, select **De-Provision Resource**. Then, click **Next**.

4. In the Select Users page, search for the users. Select one or more users from the Available Users list from whom you want to deprovision a resource. Click **Move** or **Move All** to move the users to the Selected Users list, and then click **Next**.

5. In the Select Resources page, search for the resources. Select one or more resources that you want to deprovision. Click **Move** or **Move All** to move the resources to the Selected Resources list. Then, click **Next**. The Justification page is displayed with summary information about the selected users and resources.

6. In the Effective Date field, specify a date on which you want the resource to be deprovisioned.

7. In the Justification field, enter a justification for the deprovisioning operation.

8. Click **Finish**. The request to deprovision one or more resources is created.

> **Note:** Resource search in Select Resources page lists all the resources provisioned to user selected in Select Users page. If multiple users are selected, then search shows common resources provisioned to all selected users.

14.2 Searching and Tracking Requests

You can login to Oracle Identity Manager Administration and search for requests to view a list of requests. You can perform simple search and advanced search for requests. You can also view the details of each request.

This section contains the following topics:

- Searching Requests
- Viewing Request Details

14.2.1 Searching Requests

To perform a simple search for requests:

1. Login to Oracle Identity Manager Advanced Administration.

2. In the Welcome page, under Administration, click **Requests**. Alternatively, you can click the **Requests** subtab under the **Administration** tab.

3. In the left pane, click the icon next to the Search field. A list of available requests are displayed in the search results table in the left pane with details such as request ID, request type, and request status. You can sort the requests based on the Request ID.

> **Note:**
>
> ■ Sorting on Request ID is string-based and not number-based.
>
> ■ For request search based on Requester/Beneficiary fields, enter requester/beneficiary user login id or display name only.

To perform an advanced search for requests:

1. In the left pane of the Requests section in Oracle Identity Manager Advanced Administration, click Advanced Search. The Advanced Search page is displayed.

2. Select any one of the following matching options:

   ■ **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

   ■ **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

3. Specify values in the fields as search criteria. For each field, select an operator, such as Equals, Contains, or Begins with.

4. To discard a field from your search, click the cross icon next to the field. To include a field in your search criteria, click **Add Fields**, and then select the field from the list.

5. Click **Search**. The search results table is displayed with details about request ID, request type, status, date requested, and requester, as shown in Figure 14 1. You can sort the requests based on the Request ID.

> **Note:** Sorting on Request ID is string-based and not number-based.

Figure 14 1   Advanced Search Results

14.2.2 Viewing Request Details

From the search results tables of the simple and advanced search, you can view the details of the requests for tracking. To do so, select a request in the search results table. From the Actions menu, select **Open Request Detail**. The Request Details page for the selected resource is displayed.

Figure 14 1 lists the fields in the Request Information section of the Request Details page:

Table 14 1   Fields in the Request Details page

Field	Description
Request ID	An ID to uniquely identify the request
Request Type	The type of request or the request type based on which the request is created
Status	The status in which the request is currently in
Date Requested	The date of creation of the request
Effective Date	The date from which the operation requested will be active
Requester	The user who created the request
Beneficiary	The user for whom the request is created
Justification	The reason for creating the request
Parent Request ID	The request ID of the parent request if the request whose details is displayed is a child request

Note: From the Request Details page, you can close the request by selecting **Close Request** from the Actions menu at the top of the page. For information about closing requests, see ""Closing Requests" on page 10-20".

The Request Details page displays the following tabs:

- The Resources or Users or Roles Tab
- The Request Comments Tab
- The Request History Tab
- The Approval Tasks Tab

14.2.2.1 The Resources or Users or Roles Tab

This tab is displayed in the Request Details page depending on the type of request. For example, the Resources tab is displayed in the Request Details page when the request type is Provision Resource. Similarly, the Users or Roles tabs are displayed when the request types are Create User or Assign Roles respectively.

Figure 14 2 shows the Resources tab:

Figure 14 2   The Resources Tab

In this tab, you can view the details of the resources associated with the request. The details include beneficiary, resource name, and resource details. To view resource details, click the **View Details** link for a particular resource. The Resource Details window is displayed, as shown in Figure 14 3:

Figure 14 3   The Resource Details Window

14.2.2.2 The Request Comments Tab

This tab displays any comments provided with the request that can help the approver take actions on the request. This tab also allows you to add a new comment to the request. To add a comment:

1. In the Request Comments tab, from the Actions list, select **New Comment**. The New Comment dialog box is displayed.

2. In the Comments field, enter the comment for the request.

3. Click **Save**. The comment is added and is displayed in the Request Comments tab, as shown in Figure 14 4:

Figure 14 4   The Request Comments Tab

14.2.2.3 The Request History Tab

This tab displays the history of the request, such as the request status, the date when the request is updated, and by whom the request is updated.

Figure 14 5 shows the Request History tab.

Figure 14 5   The Request History Tab

> **Note:**   If an approver is not specified for a request, then the Updated By column in the Request History tab displays *Internal User*. This is the OIMINTERNAL user, which is an Oracle Identity Manager system user. All the internal request status updates are performed as Internal User.

14.2.2.4 The Approval Tasks Tab

This tab shows the status of tasks that have been assigned to people in connection with the request.

Figure 14 6 shows the Approval Tasks tab. Two tasks are shown: Default Request Level Approval for Request ID 1, and Default Operation Level Approval for Request ID 1. Note that for tasks that are assigned to multiple approvers in a sequence (that is, Assignee 1, then Assignee 2), the Assignee column only shows the name of the person who currently has the task assigned (or, if the task sequence has been completed, it shows the name of the last person who worked on the task).

Figure 14 6   The Approval Tasks Tab

Part IV

Policy Administration

This part describes Oracle Identity Manager delegated administration functionalities by using the policy administration features.

It contains the following chapters:

- Chapter 15, "Managing Authorization Policies"
- Chapter 16, "Managing Access Policies"
- Chapter 17, "Managing Request Templates"
- Chapter 18, "Managing Approval Policies"
- Chapter 19, "Managing Attestation Processes"

15

Managing Authorization Policies

Oracle Identity Manager is a security product, and therefore, controls access to the application by the users to allow or prevent the users to perform various operations in the application. This is controlled by the authorization engine embedded in Oracle Identity Manager with the help of authorization policies. The authorization policies determine at runtime whether or not a particular action is allowed. You can define authorization policies that satisfy the authorization requirements within Oracle Identity Manager.

In earlier releases of Oracle Identity Manager, each Oracle Identity Manager feature defines and manages its own authorization policy UI and backend implementation. In Oracle Identity Manager 11*g* Release 1 (11.1.1), authorization policy management is centralized as an administrative feature. Oracle Identity Manager's authorization policy management and enforcement engine is now based on an embedded version of Oracle Entitlements Server (OES), Oracle's industry-leading fine-grained entitlements administration product. These authorization policies secure access control to the Oracle Identity Manager application, thereby defining "who can do what" inside the application. This centralized definition of authorization policies continues to provide context-sensitive authorizations for each feature as explained in the following sections:

- Authorization Policy
- Creating and Managing Authorization Policies
- Authorization Policies for Oracle Identity Manager Features

15.1 Authorization Policy

You can define and manage authorization policies in the Authorization Policies section of the Oracle Identity Administration. This section is available to users who have the Manage Authorization Policies privilege.

The following are the structural components of an authorization policy:

- **Identifying details:** Each authorization policy must have a name and description.
- **Oracle Identity Manager feature:** Each authorization policy is defined for a specific feature in Oracle Identity Manager. Features are well-defined components in Oracle Identity Manager such as user management and role management. The authorization requirements of multiple features cannot be covered by a single authorization policy.
- **Assignee:** This is the role or roles that a policy grants privileges to. You can grant privileges to one or more roles for each policy. All members of the role (direct or indirect through inheritance) are granted the privileges by the authorization policy. For the user management feature, a rule based on the manager relationship

is supported. Here, all the users that are in the management chain of the user being acted on are the assignees of the authorization policy.

> **Note:**
>
> - For information about inheritance of role membership, see Chapter 12, "Managing Roles".
>
> - Authorization policies cannot be assigned to a set of users that are defined by attribute filtering, which is defining a criteria on the attributes to select users. If such assignment is needed, a role must be defined for this set of users.

Assignee can include additional conditions that must be fulfilled by the assignee. This is a way of making the authorization policy context aware. For example, for the user management feature, a condition can state that for the assignee to have the privileges, the assignee must be a member of the same organization listed in the data security.

- **Functional security:** This section lists the privileges that the assignees are granted. The list of privileges is defined by the feature for which this policy is being defined. For example, the user management feature defines privileges such as Search for Users, View User Detail, and Modify User Profile. For a complete list of privileges for the user management feature, see "Privileges" on page 11-35.

  Some privileges also support fine-grained attribute-level controls that define which specific entity attributes of the feature are further granted to the assignee. For instance, for the View User Detail privilege, the policy can further define which of the attributes on the user entity can be viewed by the assignee at run time. Not all privileges support attribute-level details. For example, the Delete User privilege does not require or support any attribute-level details.

- **Data security:** This section lists the entities managed by the feature over which a privilege is granted to the assignee. This section is optional based on whether or not the feature for which the authorization policy is being defined supports data security. The data security is expressed in the form of an entity selection criteria or a search criteria that is used to determine the entities over which the privilege is granted. The data security can also be a list of specific entities. The data security capabilities depend on the feature. For instance, the criteria can specify that the assignee is granted privileges over the users belonging to a list of organizations. This criteria can provide additional security settings that apply to the data security. For example, in the user management feature, an instruction can be that the organization condition applies down the hierarchy so that users in the specified organization and all child organizations are in scope for this data security policy.

15.2 Creating and Managing Authorization Policies

Using the System Administrator's console, you can perform the following tasks related to authorization policies:

- Searching Authorization Policies

- Creating Custom Authorization Policies

- Creating Authorization Policies Based on Existing Policies

- Viewing and Modifying Authorization Policies

■   Deleting Authorization Policies

15.2.1 Searching Authorization Policies

You can perform simple or quick search and advanced search operations for existing authorization policies. These operations are described in the following sections:

■   Simple Search

■   Advanced Search

15.2.1.1 Simple Search

To perform simple search for authorization policies:

1. Login to the Administration console with credentials that have the Manage Authorization Policies privilege.

2. In the left pane, click **Authorization Policy** tab.

3. Verify that Policy is selected in the lookup.

4. In the text box, enter a search criteria for authorization policies.

5. Click the Search icon. You can include wildcard characters (*) in your search criterion. For performance reasons, initial (prefix) wildcards will be removed. However, a trailing (prefix) wildcard will be added to all searches.

> **Note:**   Authorization policy search is case sensitive, so you must ensure proper case while entering search criteria.

15.2.1.2 Advanced Search

To perform advanced search for authorization policies:

1. In the Welcome page, under Authorization Policies, click **Advanced Search - Authorization Policies**. Alternatively, you can click the **Authorization Policy** tab, and then click **Advanced Search** link on the left pane. The Advanced Search page is displayed.

2. Select any one of the following options:

    ■   **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

    ■   **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

3. In the Policy Name field, enter the authorization policy name that you want to search. To do so, select a search comparator in the list adjacent to the Policy Name field. The default search comparator is "Contains". Other comparators are available in the pulldown list as an alternative.

4. In the Role Name field, enter the name of the role to which the policies are assigned. You can use wildcard characters in your search criteria. Select a search condition in the list adjacent to the Role Name field.

5. In the Entity Type field, select the entity type for whom the authorization policies are defined.

6. Click **Search**. The search results are displayed in the search results table.

15.2.2 Creating Custom Authorization Policies

Oracle Identity Manager Administration allows you to create custom authorization policies for the following Oracle Identity Manager components:

- Role Management
- Authenticated Self Service User Management
- User Management

This section describes authorization policy creation for user management and role management features in the following topics:

- Creating an Authorization Policy for User Management
- Creating an Authorization Policy for Role Management

15.2.2.1 Creating an Authorization Policy for User Management

To create an authorization policy for user management:

1. Login to Oracle Identity Manager Administration console.

   > **Note:** You must be a member of the System Administrators role to create, modify, delete, search authorization policies.

2. On the Welcome page, under Authorization Policies, click **Authorization Policy**. Alternatively, you can you can click the Authorization Policy, and then click the Create New Policy icon on the toolbar. The Basic Policy Information page of the Authorization Policy wizard is displayed.

   > **Note:** In the Basic Policy Information page of the Create Policy wizard, only the Basic Policy Information, Policy Settings and Confirmation Nodes are shown at the top of the page. The other Nodes of the wizard are dynamically generated based on your selection in the Entity Name field.

3. In the Policy Name field, enter the name of the authorization policy.

4. In the Description field, enter a description of the authorization policy.

5. In the Entity name field, select the name of the feature for which you want to create the authorization policy. To create an authorization policy for user management, select **User Management**.

6. Click **Next**. The Permissions page is displayed. In this page, you can select permissions that you want to enable in the authorization policy.

7. In the Permissions table, select the check boxes in the Enable column. If you want to enable all permissions for the authorization policy, then select **Enable All Permissions** at the top of the table.

   To modify the permissions with attribute-level settings, you can click **Edit Attribute**.

8. Click **Next**. The Data Constraints page of the Authorization Policy wizard is displayed.

   In this page, options for the feature selected on the Entity Name field in step 1 are displayed.

9. Select one of the following:

   - **All Users:** Select this option to specify all the users in Oracle Identity Manager for which the authorization policy is created.

   - **Users that are members of selected Organizations:** Select this option to specify organizations for whose members you want to create the authorization policy.

10. If you select the **Users that are members of selected Organizations** option, then you must specify one or more organizations. To do so:

    a. Click **Add Organization**. The Add Organization dialog box is displayed.

    b. Click the Search icon to display the list of organizations in the Available Organizations list.

    c. From the Available Organizations list, select one or more organizations, and then click the **Move** or **Move All** buttons to move the selected organizations to the Organizations to Add list.

    d. Click **Save**. The selected organizations are added in the table in the Data Constraints page.

11. Under Organization Security Setting, select **Hierarchy Aware (include all child organizations)** to specify that the authorization policy is applicable to users who are members of all the child organizations of the selected organizations.

12. Click **Next**. The Assignment page of the Authorization Policy wizard is displayed.

13. Under Assign by Rule, select **Management Chain of User** to assign the direct and indirect managers of the user to the authorization policy.

14. To assign roles to the authorization policy:

    a. Click **Add**. The Assign Roles dialog box is displayed.

    b. Click the Search icon to display the list of roles in the Available Roles list.

    c. From the Available Roles list, select one or more roles, and then click the **Move** or **Move All** buttons to move the selected roles to the Organizations to Add list.

    d. Click **Save**. The selected roles are added to the table in the Assignment page.

    > **Note:** To remove a role from the table in the Assignment page, click **Remove**.

15. Under Assignment Security Setting, select **Assignee must be a member of the User's Organization** to specify that the authorization policy is to be applied only for the users that are members of the same organization in which the policy is applied.

16. Click **Next**. The Confirmation page of the Authorization Policy wizard is displayed with details specified in the steps of the wizard.

17. Click **Finish**. The authorization policy is created.

15.2.2.2 Creating an Authorization Policy for Role Management

To create an authorization policy for Oracle Identity Manager role management feature:

1. Login to Oracle Identity Manager Administration console.

2. On the Welcome page, under Authorization Policies, click **Create New Policy**. Alternatively, you can:

   - Click the **Authorization Policy** tab, and then click the **Authorization Policy** icon on the toolbar.

   - From the Actions menu, select **Create**.

   The Basic Policy Information page of the Authorization Policy wizard is displayed.

   > **Note:** In the Basic Policy Information page of the Create Policy wizard, only the Basic Policy Information, Policy Settings and Confirmation Nodes are shown at the top of the page. The other Nodes of the wizard are dynamically generated based on your selection in the Entity Name field.

3. In the Policy Name field, enter the name of the authorization policy.

4. In the Description field, enter a description of the authorization policy.

5. In the Entity Name field, select an entity name based on the authorization feature you want the assignee to have. To create an authorization policy for role management, select **Role Management**.

6. Click **Next**. The Permissions page is displayed.

7. Select the permissions that you want to enable for the authorization policy. To select all permissions, select **Enable All Permissions** at the top of the table.

8. Click **Next**. The Data Constraints page is displayed.

9. Select any one of the following options::

   - **All Roles:** To specify that the authorization policy is applicable to all roles in Oracle Identity Manager including all the child roles.

   - **Selected Roles:** To specify that the authorization policy is applicable to selected roles only.

   The roles selected in the Data constraint page are roles on which action is to be performed.

10. If you select the Selected Roles option, then you must select the roles for which the authorization policy is been created. To do so:

    a. Click **Add Role**. The Assign Roles dialog box is displayed.

    b. Click the Search icon to display all roles in the Available Roles list.

    c. Select the roles for which you want to apply the authorization policy.

    d. Click the **Move** or **Move All** buttons to move the roles to the Roles to Assign list.

    e. Click **Save**. The selected roles are added to the Data Constraints page of the Authorization Policy wizard.

11. To remove a selected role from the Data Constraints page:

    a. Select the role, and then click **Remove**. A message box is displayed asking for confirmation.

    b. Click **OK** to confirm.

12. In the Data Constraints page, under Role Security Setting, select **Hierarchy Aware (Include all Parent Roles)** to specify that the authorization policy is applicable to Roles, which are added as parent Roles.

13. Click **Next**. The Policy Assignment page is displayed. In this page, you can add and remove roles as described in steps 10 and 11.

Roles selected in the Policy Assignment page are roles whose direct and indirect members will perform the action based on the policy.

14. Click **Next**. The Confirmation page is displayed with Basic Policy Information and details about permissions, data constraints, and assignments.

15. Click **Finish**. The authorization policy is created.

15.2.3 Creating Authorization Policies Based on Existing Policies

You can create an authorization policy by using the general, permissions, data constraints, and assignment information from another authorization policy already existing in Oracle Identity Manager. To do so:

1. Search for the authorization policy from which you want to use information to create another policy.

2. Select the policy. From the Actions menu, select **Create Like**. The Authorization Policy wizard is displayed.

3. In the Basic Policy Information page, edit the Policy Name, Description, and Entity Name fields to specify new values.

4. Perform the steps to complete the wizard as described in "Creating Custom Authorization Policies" on page 15-4.

15.2.4 Viewing and Modifying Authorization Policies

You can view and modify authorization policies, and change the general information, permissions, data constraints, and assignments of the authorization policies. To do so:

> **Note:** The options for authorization policy modification changes dynamically based on the entity type selected for the policy. In this procedure, the example of an authorization policy for role management is used.

1. In the Authorization Policy tab of the Administration Console, in the left pane, search for authorization policies. The policies matching the search criteria are displayed in the search results table.

2. Click an authorization policy. Alternatively, you can select an authorization policy, and from the Actions menu, select **Open**. The page that allows you to view and modify authorization policy details is displayed. The General tab of the page is displayed by default, with details about the policy name, description, entity name, permissions, data constraints, and assignment.

3. Edit the Policy Name and Description fields to update the authorization policy name and description.

> **Note:** You cannot change the entity name of an authorization policy after the policy is created.

4. Click the **Permissions** tab. In this tab, you can check the permissions that you want to enable in this policy. To do so, select the permissions from the table, or select **Enable All Permissions** to enable all permissions.

   Some permissions have attribute-level settings. To modify the attribute-level settings, click **Edit Attributes**.

5. Click the **Data Constraints** tab. In this tab, you can modify the roles that the user must be a member of for this authorization policy.

6. Select any one of the following options:

   - **All Roles:** To specify that the authorization policy is applicable to all roles in Oracle Identity Manager including all the child roles.

   - **Selected Roles:** To specify that the authorization policy is applicable to selected roles only.

7. If you select the Selected Roles option, then you must select the roles for which the authorization policy is been created. This tab also allows you to remove selected roles. To add or remove roles, perform the steps described in steps 10 or 11 respectively of "Creating an Authorization Policy for Role Management" on page 15-5.

8. Select **Hierarchy Aware (include all Parent Roles)** to specify that all the parent roles of the selected roles must be selected for the authorization.

9. Click the **Assignment** tab. This tab displays the roles that are assigned to this policy.

   You can add or remove the assignment by performing steps 10 or 11 respectively of "Creating an Authorization Policy for Role Management" on page 15-5.

10. Click **Apply** to save changes.

    Alternatively, click **Revert** to refresh the page with old values.

    > **See Also:** "Disabling Access to Features Through the Authorization Policies" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about disabling or hiding features by using authorization policies

15.2.5 Deleting Authorization Policies

To delete an authorization policy:

1. In the Authorization Policy tab of the Administration Console, search for the authorization policy that you want to delete.

2. Select the policy. From the Actions menu, select **Delete**. A message box is displayed asking for confirmation.

3. Click **OK** to confirm deletion.

15.3 Authorization Policies for Oracle Identity Manager Features

This section describes the authorization policy components for the following Oracle Identity Management features:

- User Management

- Authenticated User Self Service

- Role Management

- Authorization Policy Management

- User Management Configuration

- Reconciliation Management

- Scheduler

- Request Creation By Using Request Templates

- Approval Policy Management

- Notification Management

- System Properties

- Diagnostic Dashboard

- Plug In

15.3.1 User Management

The components of the authorization policies defined for the user management feature and the default authorization policy are described in the following sections:

- Assignee

- Functional Security

- Data Security

- Default Authorization Policies

15.3.1.1 Assignee

The assignee of the policy can be a set of roles. The policy is assigned to each role in the set of policies. In addition, a rule for selecting the management chain of the user being managed as an assignee is supported. There is no ability to restrict this to just the direct manager of the user being managed.

The Assignee must be a member of security setting restricts the grant to the users who are also members of the organizations or roles being granted privileges over. If assignee belongs to multiple organization hierarchies, then a match to at least one organization hierarchy must provide the grant.

15.3.1.2 Functional Security

Multiple privileges are defined for the user management feature such as Search for Users and View User Detail. For a complete list of privileges for the user management feature, see "Privileges" on page 11-35.

The following privileges support the fine-grained attribute-level controls, in which the user is able to select the specific attributes applicable to that operation:

- View User Detail

- Modify User Profile

The list of attributes are based on the list of attributes defined for the user entity.

15.3.1.3 Data Security

For the user management feature, data security is defined as the list of organizations whose members the assignee has privileges over. The set of users being managed by the authorization policy cannot be specified by attribute filtering.

If the Hierarchy Aware option is selected, then the organization and role hierarchies are taken into account when determining the data security.

15.3.1.4 Default Authorization Policies

There are two default authorization policies for the user management feature. Users are not allowed to modify or delete these policies. Any User Management policy that provides the "Search User" permission should also provide the "View User Details" permission. The "View User Details" permission should include the User Login, Account Status, Identity Status, Full Name, and Display Name attributes. If these attributes are not provided, the user might not be fully viewable or editable.

The following table lists the default authorization policy details for user management:

Policy Name	Assignee	Functional Security	Data Security
User Management Administration Policy:	System Administrators and Identity User Administrators roles	The permissions include: Change User Password Create User Delete User Evaluate Access Policies Modify OIM Account Status Modify User Profile Modify User Proxy Profile Modify User Status Provision Resource to User Search User View User Details View User Requests Note: The Modify User Profile and View User Details have associated attribute settings. For both the permissions, the attribute setting is All Attributes.	All Users organization Assignee must be a member of the User's Organization: No Hierarchy Aware: Yes
User Management Search Policy: Allows Request Template and Approval Policy Administrators to search based on GUID and User Login	Request Template Administrators, Request Administrators, Approval Policy Administrators, and Reconciliation Administrators roles	The permissions are: Search Users View User Details: This has associated attribute settings. They are: Display Name, First Name, Full Name, GUID, Last Name, Organization, and User Login	All Organizations Assignee must be member of the User's Organization: No Hierarchy Aware: Yes

Policy Name	Assignee	Functional Security	Data Security
User Management All Users Policy	ALL Users role	The permission is:	All Organizations
		View User Details: This has associated attribute settings. They are:	Assignee must be member of the User's Organization: No
		Display Name, First Name, Full Name, GUID, Last Name, Organization, and User Login	Hierarchy Aware: Yes

15.3.2 Authenticated User Self Service

Authorization policies are used to control the following areas of authenticated self service:

- Authorization for Profile Attributes
- Authorization for Role Requests
- Authorization for Resource Requests
- Authorization for Proxies
- Default Authorization Policy

15.3.2.1 Authorization for Profile Attributes

The attributes displayed on the My Profile page of Oracle Identity Manager Self Service are controlled by using the VIEW_USER_DETAILS and MODIFY_USER_DETAILS privileges from the Self Service User Management OES authorization policies. If multiple policies are applicable, then the list of attributes on which the user has permissions is a union of the attributes determined by individual policies.

By default, the All Users and System Administrators roles have permissions to view and modify a set of attributes. The All users and System Administrators roles have permissions to view the following attributes:

Email, Display Name, First Name, Last Name, Locale, Middle Name, Telephone Number, Time Zone, User Login, Manager, Identity Status, and Account Status

The All users and System Administrators roles have permissions to modify the following attributes:

Email, Display Name, First Name, Last Name, Locale, Middle Name, Telephone Number, Time Zone, and User Login

If the user has view and modify privileges for an attribute, then the attribute is displayed as editable on the My Profile page. If the attribute has view permission only, then it is displayed as read-only. The request to modify self profile is submitted by using the Modify Self Profile request template. The request dataset for this request template is the same as that for the Modify User request template. This request template is configurable.

> **See Also:** Chapter 14, "Creating and Searching Requests" for detailed information about requests models, request templates, and request datasets

To display additional attributes on the user's profile:

1. Create a custom self service authorization policy with view and/or modify user profile permission having default or custom additional attributes. See "Creating Custom Authorization Policies" on page 15-4 for information about creating custom authorization policies.

2. Assign the custom authorization policy to the All Users and System Administrators roles because the administrator user does not have All Users role by default.

3. If the additional attribute is set to modify user profile permission in the policy, then update the request dataset for the Modify Self Profile, that is, ModifyUserDataset.xml to include the attribute. The entry in dataset is made for the attribute to be rendered on the Modify Self Profile page.

> **Note:** Ensure that the additional attribute has the visible property set.

15.3.2.2 Authorization for Role Requests

There is no permission defined for requesting and viewing roles as self service operations. However, while requesting for roles, only those request templates are displayed that the user is authorized to access. The request management feature controls this. While searching for roles during the request operation, the user is allowed to select from only those roles that the user is authorized to search and view. This is controlled by role management policies.

The user can request for all the roles for which the user has search permission. This is controlled by general authorization policy defined by role management. While creating a request for a role, the user must search and select the roles.

The roles available for the user in the list of roles on the Request Roles page are the result of intersection of the roles provided in the request template and roles that the user has search permission for. For example, if the request template has roles Role1, Role2, and Role3 and the user has search permission on Role2 and Role3, then Role2 and Role3 are displayed in the list of roles. Similarly, if the user has search permission over Role1, Role2, and Role3 and the request template has roles Role2 and Role3, then Role2 and Role3 are displayed in the list of roles.

15.3.2.3 Authorization for Resource Requests

There is no permission defined for requesting and viewing resources as self service operations. However, for requesting and viewing resources, the resource must be configured so that self requesting for that resource is allowed. This is done by selecting the **Self Request Allowed** option in the Resource Objects form in Oracle Identity Manager Design Console.

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about the Resource Objects form in Oracle Identity Manager Design Console

15.3.2.4 Authorization for Proxies

To add, modify, and remove proxy operations, authorization checks are required in the authenticated self service APIs along with a new MODIFY_SELF_USER_PROXY_PROFILE privilege in the default authorization policy for self service user management. The authenticated self service API first checks for this privilege. If the user is authorized to perform the proxy operation, then the authenticated self service API calls the corresponding APIs for user management.

> **See Also:** *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about Oracle Identity Manager APIs

The Modify Self User Proxy Profile permission is required to allow adding, modifying, and removing proxies.

15.3.2.5 Default Authorization Policy

The default authorization policy defined for the authenticated user self service feature is Self Service User Management All Users Policy, which allows users with the System Administrator role and All Users to access some of the self service user management operations. The policy has the following components:

:

- **Assignee:** The policy defines what privileges the assignee users have for managing their profile after logging into Oracle Identity Manager Self Service. However, roles-based assignee allows you to define different self-service policies for different roles, thereby restricting the self-service capabilities for these roles. For example, you define Policy1 that grants all self-service privileges to members of the Employee role.

- **Functional Security:** The authenticated user self service feature defines the following permissions:
    - View User Details
    - Modify User Profile
    - Modify Self User Proxy Profile

    The Modify User Profile and Modify Self User Proxy Profile permissions support fine-grained attribute level controls, in which the user is able to select the specific attributes that apply to that operation.

- **Data Security:** None

15.3.3 Role Management

The components of the authorization policies defined for the role management feature and the default authorization policy for this feature are described in the following sections:

- Assignee
- Functional Security
- Data Security
- Default Authorization Policies

15.3.3.1 Assignee

The assignee of the policy can be a role or a set of roles.

15.3.3.2 Functional Security

Multiple privileges are defined for the role management feature. The privileges do not support fine-grained attribute-level controls.

15.3.3.3 Data Security

For the role management feature, data security is defined as the list of roles the assignee will have privileges over.

The Assignee Must Be Member of condition restricts the grant to assignees that are also members of the role being granted privileges over.

The Hierarchy Aware setting takes the role hierarchies into account when determining the data security.

15.3.3.4 Default Authorization Policies

The default authorization policy defined for this feature cannot be modified or deleted by users. The policies are describes in the following table:

Policy Name	Assignee	Functional Security	Data Security
Role Management Administration Policy	System Administrators and ROLE ADMINISTRATORS roles	The permissions are: Create Role, Create Role Category, Delete Role, Delete Role Category, Modify Role, Modify Role Category, Modify Role Hierarchy, Modify Role Membership, Search for Role, Search for Role Categories, View Role Category Detail, View Role Detail, View Role Membership	All Roles
Role Management All Users Policy	ALL USERS role	The permissions are: Search for Role, Search for Role Categories, View Role Detail, View Role Category Detail	All Roles, in which the authorization is applied to users belonging to roles. Selected Roles, in which you can select the roles that the user must be a member of for this authorization
Role Management Role Owner Policy	ALL USERS role	The permissions are: Delete Role, Modify Role, Modify Role Hierarchy, Modify Role Membership, Search for Role, Search for Role Categories, View Role Category Detail, View Role Detail, View Role Membership	All Roles that the assignee is the owner of. When a user creates a role, the person with the role created will become the role owner.

Policy Name	Assignee	Functional Security	Data Security
Role Management Approval and Request Policy	APPROVAL POLICY ADMINISTRATORS, REQUEST TEMPLATE ADMINISTRATORS roles, and REQUEST ADMINISTRATORS roles	The permissions are: Search for Role Search for Role Categories View Role Category Detail View Role Detail	All Roles
Role Management Delegated Administration Policy	ROLE ADMINISTRATORS role	The permissions are: Modify Role Membership Search for Role Search for Role Categories View Role Category Detail View Role Detail View Role Membership	All Roles
Role Management Hierarchy Administration Policy	ROLE ADMINISTRATORS role	The permissions are: Modify Role Modify Role Hierarchy Search for Role Search for Role Categories View Role Category Detail View Role Detail View Role Membership	All Roles

15.3.4 Authorization Policy Management

Access to the authorization policy management feature is controlled by a default authorization policy. This policy grants the users who belong to the System Administrators role to perform authorization policy operations, such as searching authorization policies, and creating, modifying, and deleting custom authorization policies.

Note:

- The delete or disable action is controlled by feature specific UI code, which calls AuthorizationService API to find out whether the user is allowed to perform that action. If the user has the permission, then under Action list on the left pane of the UI, the user can see Delete or Disable options enabled.

- Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

The details of the default authorization policy for this feature is the following:

- **Policy Name:** Authorization Management Administration Policy

- **Assignee:** System Administrators role

- **Functional security:** The supported permissions are:

    - Create Authorization Policies

- – Delete Authorization Policies

- – Modify Authorization Policies

- – Search Authorization Policies

  These privileges do not support fine-grained attribute-level controls.

- **Data security:** This authorization policy does not support any data security. Anybody with the privileges to manage authorization policies can manage any and all authorization policies.

15.3.5 User Management Configuration

The default authorization policy for the user management configuration feature allows users with the System Administrators and USER CONFIGURATION ADMINISTRATORS roles to access all user management configuration operations. This policy has the following details:

- **Policy name:** User Management Configuration Administration Policy

- **Assignee:** System Administrators and USER CONFIGURATION ADMINISTRATORS roles

- **Functional security:** The permissions are:
  - – Add Category

  - – Add Derived Attributes

  - – Create Attribute

  - – Delete Attribute

  - – Delete Category

  - – Set Search Attributes

  - – Set Search Attributes

  - – Update Attribute

  - – Update Category

  These permissions do not support fine-grained attribute-level controls.

- **Data security:** None

> **Note:** Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.6 Reconciliation Management

The components of the authorization policies defined for the reconciliation management feature and the default authorization policy for this feature are described in the following sections:

- Assignee

- Functional Security

- Data Security

- Default Authorization Policy

15.3.6.1 Assignee

The assignee of the policy can be a role or a set of roles.

15.3.6.2 Functional Security

The reconciliation management feature defines multiple privileges from the authorization policy management area. These privileges do not support fine-grained attribute-level controls.

15.3.6.3 Data Security

This authorization policy does not support any data security. A user with the privileges to manage reconciliation events can manage all reconciliation events.

15.3.6.4 Default Authorization Policy

The following table lists the default authorization policies for the reconciliation management feature:

Policy Name	Assignee	Functional Security	Data Security
Reconciliation Management Administration Policy	SYSTEM ADMINISTRATORS and RECONCILIATION ADMINISTRATORS roles	The permissions include: Assign Bulk Action Create Act Create User Link Act Link User Search View Event Details These permissions do not support fine-grained attribute-level controls.	None
Reconciliation API Policy	SYSTEM ADMINISTRATORS and RECONCILIATION ADMINISTRATORS roles	The permissions are: Create Reconciliation Event Delete detected Accounts Get Missing Accounts Ignore Event Link Event to Resource for user Link Event to User Process Reconciliation Event These permissions do not support fine-grained attribute-level controls.	None

15.3.7 Scheduler

The default authorization policy for the scheduler feature allows users with the System Administrators and SCHEDULER ADMINISTRATOR roles to access all scheduler operations. This policy has the following details:

- **Policy Name:** Scheduler Administration Policy

- **Assignee:** System Administrators and SCHEDULER ADMINISTRATOR roles

- **Functional security:** The permissions are:
  - Job Create
  - Job Delete
  - Job Disable
  - Job Enable
  - Job Filter
  - Job Modify
  - Job pause
  - Job Resume
  - Job run now
  - Job Search
  - Job stop
  - Reset Status
  - Scheduler Search
  - Scheduler Start
  - Scheduler Stop
  - Trigger Create
  - Trigger Delete
  - Trigger Modify

  These permissions do not support fine-grained attribute-level controls.

- **Data security:** None

> **Note:** Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.8 Request Creation By Using Request Templates

For creating requests by using request templates, an authorization policy is created for each request template that is created. These authorization policies can be viewed but cannot be modified.

Each request template can be associated with a set of roles. Only the users that are members of any of these roles are able to create requests using that request template. Therefore, for each request template, Oracle Identity Manager generates a corresponding authorization policy. For each default request template, Oracle Identity Manager generates a corresponding authorization policy by default.

The default authorization policy for creating requests by using request template allows users with the REQUEST TEMPLATES ADMINISTRATORS role to access all operations related to request templates. The policy has the following details:

- **Policy name:** Request Template Administration Policy

- **Assignee:** REQUEST TEMPLATE ADMINISTRATORS role

- **Functional security:** The permissions are:

  - Create

  - Delete

  - Modify

  - Search

  These permissions do not support fine-grained attribute-level controls.

- **Data security:** None

Note: Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.9 Approval Policy Management

The default authorization policy for the approval policy management feature allows users with the APPROVAL POLICY ADMINISTRATORS role to access all approval policy management operations. This policy has the following details:

- **Policy name:** Approval Policy Management Policy

- **Assignee:** APPROVAL POLICY ADMINISTRATORS role

- **Functional security:** The permissions are:

  - Create

  - Delete

  - Modify

  - Search

  These permissions do not support fine-grained attribute-level controls.

- **Data security:** None

Note: Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.10 Notification Management

The default authorization policy for the notification management feature allows users with the NOTIFICATION TEMPLATE ADMINISTRATORS role to access all notification management operations. This policy has the following details:

- **Policy Name:** Notification Management Administration Policy

- **Assignee:** System Administrators and NOTIFICATION TEMPLATE ADMINISTRATORS roles

- **Functional security:** The permissions are:

  - Add Locale

  - Create

  - Delete

- Filter

- Lookup

- Modify

- Remove Locale

- Search

These permissions do not support fine-grained attribute-level controls.

- **Data security:** None

> **Note:**   Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.11 System Properties

The default authorization policy for the system properties feature allows users with the System Administrators and SYSTEM CONFIGURATION ADMINISTRATORS roles to access all operations related to system properties. This policy has the following details:

- **Policy name:** System Properties Administration Policy

- **Assignee:** System Administrators and SYSTEM CONFIGURATION ADMINISTRATORS roles

- **Functional security:** The permissions include:

  - Create

  - Delete

  - Filter

  - Lookup

  - Modify

  - Search

These permissions do not support fine-grained attribute-level controls.

- **Data Constraints:** None

> **Note:**   Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.12 Diagnostic Dashboard

The default authorization policy for the Diagnostic Dashboard feature allows users with the System Administrators role to access the diagnostic dashboard. This policy has the following details:

- **Policy name:** Diagnostic Dashboard Policy

- **Assignee:** System Administrators role

- **Functional security:** The Manage Failed Tasks permission without any fine-grained attribute-level controls

- **Data constraints:** None

> **Note:** Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

15.3.13 Plug In

The default authorization policy for the Plug In feature allows users with the PLUGIN ADMINISTRATOR role to register unregistered policies. This policy has the following details:

- **Policy name:** Plugin Administrator Policy
- **Assignee:** PLUGIN ADMINISTRATOR and SYSTEM ADMINISTRATOR role
- **Functional security:** The permissions are:
  - Register Plug In
  - Unregister Plug In

  These permissions do not support fine-grained attribute-level controls.
- **Data constraints:** None

> **Note:** Authorization policies are for Oracle Identity Manager account users. Other users can only view it on UI, but cannot modify.

16

Managing Access Policies

Access policies are a list of roles and the resources with which roles are to be provisioned or deprovisioned. Access policies are defined using Create Access Policy and Manage Access Policies menu items in Oracle Identity Manager Administrative and User Console.

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

This chapter discusses the following topics:

- Features of Access Policies
- Creating Access Policies
- Managing Access Policies

16.1 Features of Access Policies

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

Provisioning Options

Whenever an access policy is applied, the resources are directly provisioned to the user without the any request being generated.

Revoking the Policy

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

Denying a Resource

While creating an access policy, you can select resources to be denied along with resources to be provisioned for roles. If you first select a resource for provisioning and then select the same resource to be denied, then Oracle Identity Manager removes the resource from the list of resources to be provisioned. If two policies are defined for a role in which one is defined to provision a resource and the other is defined to deny the resource, then Oracle Identity Manager does not provision the resource irrespective of the priority of the policies.

Evaluating Policies

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

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

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

- If the retrofit flag is set for the policy

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

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

  – A role is added or removed from the policy definition. Policies are evaluated only for roles that is added or removed.

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

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

Access Policy Priority

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

- If the priority number entered is less than 1, then Oracle Identity Manager will change the value to 1 (highest priority).

- If the priority number entered is greater than M, in which M is the current lowest priority, then Oracle Identity Manager will specify the value as less than or equal to M+1.

- Two access policies cannot have the same priority number. Therefore, assigning an already existing priority number to an access policy will lower the priority by 1 for all policies of lesser priority.

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

Access Policy Data

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

1. Default values from the form definition

2. Organization defaults

3. Values obtained through data flow from data set to process form

4. Prepopulate adapters

5. Access policy data if resource is provisioned because of a policy

6. Data updated by Process Task or Entity Adapters

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

16.2 Creating Access Policies

You can define an access policy for provisioning resources to users who have roles defined in the policy by using the Access Policy Wizard.

To create an access policy:

1. To open the Create Access Policies page, in the left pane of Oracle Identity Manager Administrative and User Console, click **Create Access Policy**.

2. Click **Create**.

   The Create Access Policy page is displayed.

3. Enter information in the required fields indicated with an asterisk (*) and click **Next**.

4. Select **Retrofit Access Policy** to retrofit this access policy when it is created.

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

   If you do not select this option, then existing role memberships are not taken into consideration.

5. Click **Continue**.

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

6. Specify the resource to be provisioned for this access policy.

   Search for resources by using the filter search menu.

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

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

   - To unassign the selected resources, highlight the resource in the Selected list and click **Remove**.

7. Click **Continue**.

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

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

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

9. Click **Continue**.

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

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

    To select resources to be denied:

    a. Select the resources from the results table.

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

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

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

    c. Click **Continue**.

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

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

12. To associate a group with this access policy:

    ■ Select the group/role from the results table, and then click **Add**. You must select at least one group/role. The names of the selected group/roles appear in the Selected list.

    ■ You can delete the group name by clicking **Remove**.

13. Click **Continue.**

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

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

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

    > **Note:** When you create an access policy on a resource having a process form with Password field, the password policy is not evaluated. For information about password policies, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

16.3 Managing Access Policies

You can use Oracle Identity Manager Administrative and User Console to modify information in existing access policies.

To manage access policies:

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

   The Manage Access Policies page is displayed.

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

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

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

   The Access Policy Details page is displayed.

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

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

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

17

Managing Request Templates

A request template lets you customize a request type for a purpose. In other words, it allows you to control the attributes of the request by controlling the various capabilities in the UI. For instance, if you want to create requests for user creation for all contract employees and specify an attribute to have a particular value, then you can customize the Create User request type to create a request template that allows customization of the request. By creating the request template, you can specify that the middle name of all contract employees must be contract, or the user type must be specified as Part-time Employee.

Access to templates is based on the role assignment defined in the template. After creation of a request template, it is available only to the users with the roles that are assigned to the template.

A default template is shipped predefined for each of the request type. These predefined templates can not be deleted or renamed. Names of these predefined templates is same as corresponding models.

You can use a request template for the following purposes:

- **Adding template-level approval:** You can add an additional level of approval apart from request-level and operation-level while creating the template.

- **Adding restrictions:** This includes:

  - **Adding entity restrictions:** You can specify restrictions of the entity types or attributes that can be selected through the request templates. For example, a template for Provisioning Resource request type might specify a number of valid resources that can be selected by using this template. Limit the use of template to specific type of entities in case of generic requests. For example, the template defined on provisioning request type may specify that this template can only be used for Active Directory, Exchange, and UNIX resources.

    > **Note:** If no entity type is restricted in the template, then all the available entity types are shown to the requester while creating request using this template.

  - **Restricting data values for an attribute:** If you specify a value for attributes, then the default value of the attribute is set, and the attribute is not displayed in the UI. On specifying multiple such values, the values are available to the user as List of Values (LOV), from which the user can select a value.

- **Adding additional data collection attributes:** These attributes are not associated with any entity. Data collected by using such mechanism cannot be used during

request execution. However, it can be used for reporting purpose, validations on the request, and post submission data action handlers.

- **Assigning roles to template to restrict the use by end users:** Only the members of the appropriate roles assigned to the template can raise a request by using that template.

To summarize, the following are achieved by using the request template:

- The restricted entity types can be specified.

- The restricted attributes that are not required to be collected as a part of the request for the entity can be specified.

- The attribute can be restricted to one value or list of values. If only one value is specified, then the attribute is not shown to the requester while submitting the request. If a list of values is specified, then the requester has to select one value from the list of values.

The template management service internally uses Oracle Entitlements Server (OES) for determining who can perform what operations. The OES policy for request template authorization specifies that only users with the REQUEST TEMPLATE ADMINISTRATORS role are authorized to create or clone, search, modify, and delete request templates. See ""Request Creation By Using Request Templates" on page 15-18" for information about the authorization policy for request templates.

This section discusses the following topics:

- Creating Request Templates

- Searching and Modifying Request Templates

- Cloning Templates

- Deleting Templates

17.1 Creating Request Templates

As a user belonging to the REQUEST TEMPLATE ADMINISTRATORS role, you can create a request template by using the Create Request Template wizard in the UI for request management. Steps in the wizard are dynamically generated based on the selection of the request type in the first step and the selection of resource for resource-based request types.

Creation of request templates is described with the help of the following scenarios:

- Creating a Request Template Based on the Create User Request Type

- Creating a Request Template Based on the Provisioning Resource Request Type

17.1.1 Creating a Request Template Based on the Create User Request Type

To create a request template based on the Create User request type:

1. Log in to Oracle Identity Manager Administrative and User Console with credentials that have the permission to create a request template.

> **Note:** The user who is a member of the REQUEST TEMPLATE ADMINISTRATORS role is allowed to create a request template. If the appropriate role is not assigned to the user, then the required UI options for creating a request template will not be available to the user.

2. Click **Advanced** to open Oracle Identity Manager Advanced Administration.

3. Click the **Configuration** tab, and then click **Request Templates**. Alternatively, you click the **Search Request Templates** link under Configuration in the Welcome page.

4. On the left pane, from the Actions menu, select **Create**. Alternatively, you can click the **Create Request Template** icon on the toolbar. The Set request template details page of the Create Request Template wizard is displayed.

5. Enter values for the following fields, and then click **Next**.

   - **Request Template Name:** Enter the name of the template that you want to create, for example, Create Contractor.

   - **Request Type:** Specify the type of request for which you want to create the request template, for example, Create User. Click the icon next to the field to select from the list of model types.

   - **Description:** Enter a description for the request template that you are creating.

   - **Template Level Approval Process:** Specify the approval workflow name if you want to specify an approval process for the Create User request. This is a template-level approval in addition to the request-level and operation-level approvals. For creating users for contract employees, you can specify that the HR representative, who is responsible for the recruitment of all contract employees, must approve the user creation. For more information about approval-levels, see "Approval Levels" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

     See Also: "Chapter 25: Configuring Workflows" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about default approval processes

6. On the Select Attributes to Restrict page, select the attributes of the Create User type for which you want the user to enter values. This page displays the attributes based on the dataset for Create User request type. If a request is created by using the Create User request template, then you can specify values for all these default attributes. If you want to restrict some of these attributes and want the user to enter values for a few attributes, then you can select those attributes in this page. For example, you can select Middle Name because a value for this attribute must be specified. In this example, you can select the Middle Name, Organization, User Type, User Manager, and Country attributes.

Note:

- Even if a dataset attribute is configured with a PrePopulationAdapter, it can be restricted in a request template. In such case, pre-population will not happen and the values restricted in template will be shown in Request creation UI. Hence, if pre-population is required for an attribute, it should not be restricted in the template.

- As mentioned earlier in this section, the steps in the wizard are dynamically generated based on the request type and the resource selection for resource-based request types. The steps are indicated on the top of the tab.

7. On the Set Attribute Restrictions page, specify restrictions on the attributes that you selected in the Select Attributes to Restrict page. To specify restrictions:

Note: This step is generated only if there are any attributes specified in the corresponding request data set.

a. For the middle name attribute, select any one of the following:

- **Do not allow users to enter values for this attribute:** Select this option if you do not want the user to specify a value for the attribute. On selecting this option, the attribute will not be displayed in the UI when creating the user. This option is not displayed for a mandatory attribute because a value must be specified for this attribute.

- **Restrict this attribute to the following values:** Select this option if you want to specify one or more values for the attribute. For the middle name attribute, if you specify a value, such as Contractor, then the default value of the attribute is set to Contractor, and the attribute is not displayed in the UI when creating the user. You can also specify multiple values for the attribute by using the **+** (plus) icon. On specifying multiple values, the values are available to the user as List of Values (LOV) when creating the user, from which the user can select a value.

Tip: These options are displayed for the Middle Name attribute because the attribute is specified as a text box in the request dataset. For information about request datasets, see "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

b. Specify one or more values for the Organization attribute. To do so, click the search icon next to the Organization field, select one or more organization names from the Available Organizations list, and clicking the **Move** or **Move All** buttons.

> **Tip:** The Organization attribute is displayed as a field for which you must select a value by searching the existing organization names because this attribute is specified as an entity in the request dataset. This is a dynamic LOV because organizations can be created in Oracle Identity Manager. For information about request datasets, see "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

    c. Specify a value for the User Type attribute. To do so, select one or more values from the Available User Type list, and click the **Move** or **Move All** buttons.

> **Tip:** The User Type attribute is displayed as a static LOV because this attribute is specified as a static LOV in the request dataset. This is a static LOV because the user must select from the available user types and cannot create new user types. For information about request datasets, see "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

    d. Specify values for the User Manager and Country attributes, and click **Next**.

> **Note:** Steps 5, 6, and 7 are common for all request templates creation.

8. On the Set Additional Attributes page, you can specify additional information about attributes, which need to be collected based on the template that you are creating but are not used for the purpose of entity mapping. These additional attributes are specified for the purpose of request tracking.

> **Note:** The Additional Attribute Data is not used during request execution. This data is also not displayed to the approver.

In this example, specify date of birth as the additional attribute name. Select the Data Type as **Number** and Display Type as **Text Field**, and then click **Add**. You can specify multiple attributes by clicking the **Add** button. When finished, click **Next**.

> **See Also:** "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about the additional attributes that are not mapped to the underlying Oracle Identity Manager entity

9. On the Set Template User Roles page, you can select one or more roles, for example, AD Administrators, whose members are allowed to create requests by using the template that is being created. In this example, from the Available Roles list, select **IT RESOURCE ADMINISTRATORS** and **ATTESTATION CONFIGURATION ADMINISTRATORS**. Click **Move** to include the selected roles in the Selected Roles list, and then click **Next**.

> **Note:** Only members of the selected roles are allowed to create requests using the request template. This is governed by the authorization policy for creating requests by using request templates. See ""Request Creation By Using Request Templates" on page 15-18 for information about creating a request by using request templates.

10. On the Review Request Template Summary page, review the data that have been entered up to this point, and then click **Finish**.

11. Click **OK** to confirm the template creation.

In the Create Request Template wizard, the following steps are common irrespective of the request type that you select or the request dataset that you define:

- Request details to be specified in the Set request template details page. See step 5 in the create request templates.

- Setting additional attributes in the Set Additional Attributes page. See step 8.

- Setting roles for the template in the Set Template User Roles page. See step 9.

- Request summary information in the Review Request Template Summary page. See step 10.

17.1.2 Creating a Request Template Based on the Provisioning Resource Request Type

Provision Resource is the default request type or template for provisioning resources to users. But if you want to create a request template to provision a specific resource to users, then you can create a request template, which is based on the Provision Resource request type.

To create a request template based on the Provisioning Resource request type:

1. In Oracle Identity Manager Advanced Administration, click the **Configuration** tab, and then click the **Request Templates** tab. Alternatively, you click the **Search Request Templates** link under Configuration in the Welcome page.

> **Note:** The user who is a member of the REQUEST TEMPLATE ADMINISTRATORS role is allowed to create a request template. If the appropriate role is not assigned to the user, then the required UI options for creating a request template will not be available to the user.

2. On the left pane, from the Actions menu, select **Create**. Alternatively, you can click the **Create a Request Template** icon on the toolbar. The Set request template details page of the Create Request Template wizard is displayed.

3. In the Request Template Name field, enter the name of the request template, for example, Provision E-Business Resource.

4. In the Request Type field, search for a request type by clicking the search icon next to the field. Select **Provision Resource**, and click **Confirm**.

> **Note:** When you select the request type, the steps in the wizard are dynamically generated and are displayed on the top of the Create Request Template tab.

5. In the Approval Process field, enter the name of the approval workflow. For information about this field, see step 4 of "Creating a Request Template Based on the Create User Request Type" on page 17-2. Then, click **Next**.

6. In the Select Allowed Resources page, click **Search** to search for all the available resources.

7. From the Available Resources list, select one or more resources, and then click **Move** or **Move All** to include the selected resources in the Selected Resources list. In this example, select the **E-Business RO** resource, and then click **Next**.

    > **Note:**
    >
    > ■ When you create the request, only the resources that you select in this step are displayed. If you do not select a resource here, then all the resources in Oracle Identity Manager are displayed while creating the request.
    >
    > ■ If no entity type is restricted in the template, then all the available entity types are shown to the requester while creating request using this template.

8. In the Select Attributes to Restrict page, select the attributes associated with the E-Business resource that you want to restrict. These attributes are defined in the request dataset for provisioning the E-Business resource. See "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for more information about attributes.

    If you select multiple resources in the Select Allowed Resources page, then the attributes associated with all the resources are displayed in the Select Attributes to Restrict page. Select the attributes for all the resources that you want to restrict, and then click **Next**.

9. In the Set Attribute Restrictions page, specify values for the attributes whose values you want to restrict. For example, for the model attribute, select the **Do not allow users to enter values for this attribute** option if you do not want the user to specify a value for the attribute. Otherwise, select the **Restrict the attribute to the following values** option and specify one or more values for the model attribute. For information about these options and setting restrictions for attributes, see "Creating a Request Template Based on the Create User Request Type" on page 17-2.

    Note that the **Do not allow users to enter values for this attribute** option is not available for the Server and Life Span Type attributes. This is because these attributes are specified as required in the request dataset. For information about the required property, see "Request Dataset" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

    Select restriction values for all the attributes, and then click **Next**.

    > **Tip:** If you are creating a request template for a request to provision multiple resources to users, click the **Next Resource** and **Previous Resource** buttons to set attribute restrictions for all the resources.

    > **Note:** Attributes coming up as shuttle on attribute restrictions page will show upto 200 results at a time. You need to provide appropriate search pattern to get relevant search results.

10. Perform steps 8 through 10 of the procedure in "Creating a Request Template Based on the Create User Request Type" on page 17-2 to complete the wizard.

> **Note:** In the Create Request Template wizard, the steps to select resources and set attribute restrictions vary based on the request type. The rest of the steps are similar.

While creating a request template, if you select a resource that does not have a request dataset defined, then you are not allowed to restrict the attributes to collect from the user. This is because there is no information specified about the data that is to be collected from the user for the selected resource. As a result, the Step 2: Attributes and Step 3: Restrictions in the Create Request Template wizard are not applicable because the attributes in these steps are defined by the request dataset, in the absence of which, there is no data to restrict. However, when you select a resource that does not have a request dataset, the Service Account attribute is displayed in the Step 2: Attributes because this attribute is defined by the common request dataset. See "Common Request Dataset" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for information about common request dataset.

17.2 Searching and Modifying Request Templates

Oracle Identity Manager Administration allows you to perform simple and advanced search for request templates, if you have the privileges of the Template Administrator's role.

To perform a simple search for request templates:

1. Go to Oracle Identity Manager Advanced Administration.

2. In the left pane of the Request Templates section, enter a search criteria in the Search field. You can use the asterisk (*) wildcard character in the Search field.

> **Note:** In simple and advanced search for request templates, searching with translated request template name is not supported. Oracle Identity Manager supports only English string search for predefined request templates. For default request templates, you can search with English template names as stored in the database. However, if you create a request template by specifying its name in another language, then you can search it using the same string, and not in any other language.

3. Click the icon next to the Search field to display a list of default and nondefault request templates.

All the default request templates are blank templates without any customization on top of the request types. Table 17–1 lists the default request templates:

Table 17–1 Default Request Templates

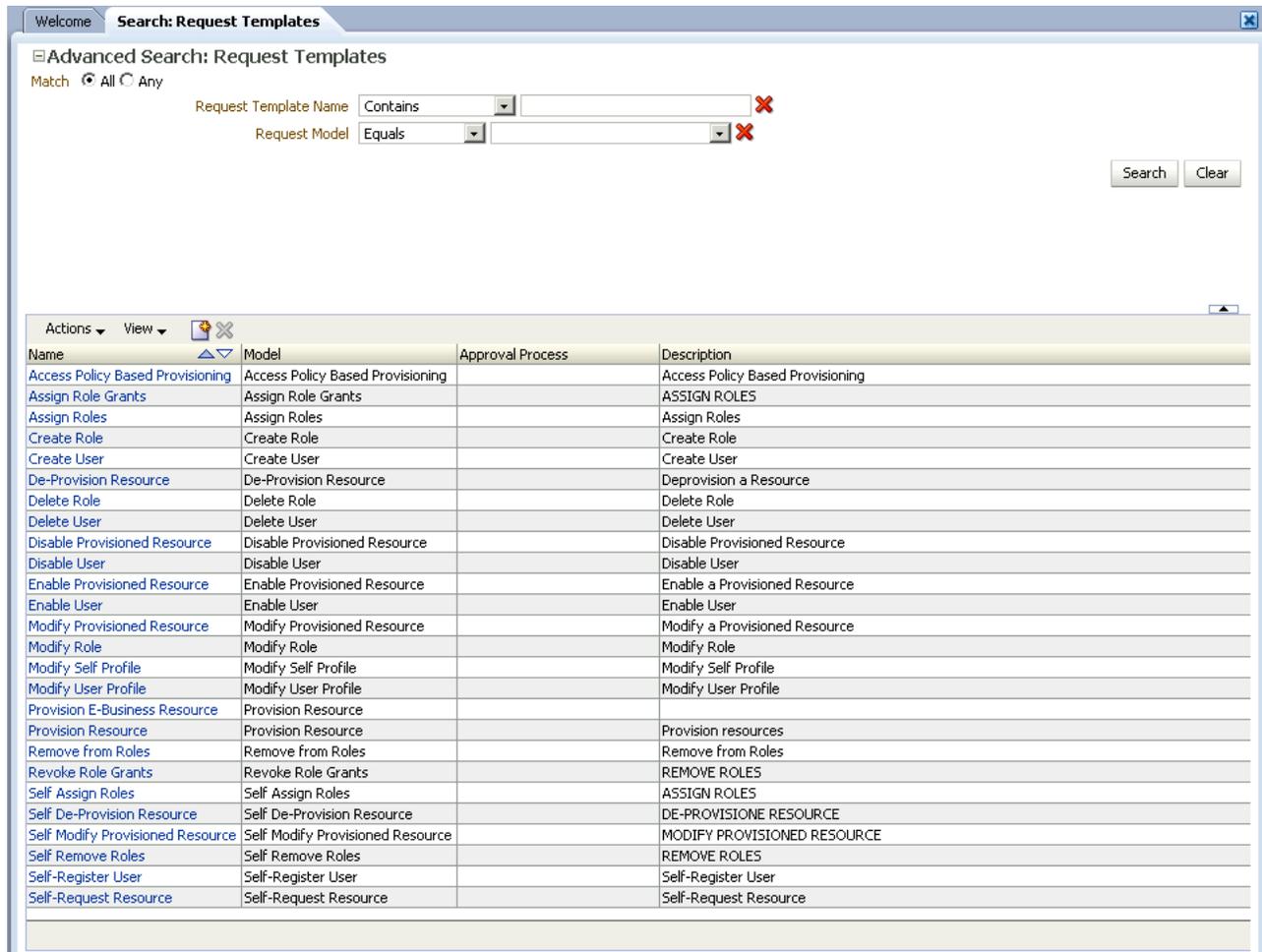| Request Template	Description
Assign Roles	Default template for assigning roles to users
Create User	Default template for creating users
De-Provision Resource	Default template for deprovisioning resources

Table 17–1   (Cont.) Default Request Templates

Request Template	Description
Delete User	Default template for deleting users
Disable Provisioned Resource	Default template for disabling provisioned resources
Disable User	Default template for disabling users
Enable Provisioned Resource	Default template for enabling provisioned resources
Enable User	Default template for enabling users
Modify Provisioned Resource	Default template for modifying provisioned resources
Modify Self Profile	Default template for modifying self profile
Modify User Profile	Default template for modifying user profiles
Provision Resource	Default template for provisioning resources
Remove from Roles	Default template for removing users from roles
Self-Register User	Default template for self registering users
Self-Request Resource	Default template for requesting resources for self

---

Note: Each request template mentioned in Table 17–1 has a default callback policy which are used by SPML webservice.

To perform an advanced search for request templates:

1. Go to Oracle Identity Manager Advanced Administration.

2. In the left pane of the Request Templates section, click **Advanced Search**. The Advanced Search: Request Templates page is displayed.

3. Select any one of the following matching options:

   ■ **All:** On selecting this option, the search is performed with the AND condition. This means that the search operation is successful only when all the search criteria specified are matched.

   ■ **Any:** On selecting this option, the search is performed with the OR condition. This means that the search operation is successful when any search criterion specified is matched.

4. Specify values in the fields as search criteria. For each field, select an operator, such as Equals, Contains, or Begins with.

5. To discard a field from your search, click the cross icon next to the field.

6. Click **Search**. The search results table is displayed with details about the request template name, request type, approval process, and description.

Figure 17–1   Advanced Search Result for Request Templates

To modify a request template:

1. Select a template name in the search results table. From the Actions menu, select **Open**. The Template Details page is displayed with the details about the template.

2. In the Template Details section, the details of the template are displayed in the fields, as shown in Table 17–2:

Table 17–2   Fields in the Template Details Section

Field	Description
Request Template Name	The name of the request template, for example, Create User
Request Type	The request type, for example, Create User
Template Level Approval Process	The additional approval process, which is invoked for requests that are created using this request template.
Description	The description for the request template

After you create a request template, and search for the request templates, the template that you created is also displayed in the search results table on the left pane. You can view the details of the template that you created. For example, if you create the Create Contractor request template and select **Open** from the Actions menu, then the Template Details page for the Create Contractor request template is displayed.

Note that the tabs that are displayed in the Request Details page correspond to the steps in the Create Template wizard. Similar to the steps in the wizard, the tabs in the Template Details page are dynamically generated, and each tab correspond to a step in the Create Template wizard. In general, the Template Details page has the following tabs:

- Allowed Resources or Allowed Roles

- Attribute Restrictions

- Additional Attributes

- Template User Roles

> **Note:** These tabs are dynamically generated based on the request type that is associated with the request template. In other words, each tab that is displayed in the Request Details page correspond a step in the Create Template wizard.

17.2.1 Allowed Resources or Allowed Roles

The Allowed Resources tab or the Allowed Roles tab is displayed only if the request type is associated with a resource or a role. Figure 17–2 shows the Allowed Resources tab:

Figure 17–2 The Allowed Resources Tab

The options available in this tab allows you to edit and delete resources or roles. To do so:

1. Open/Edit the Request Template that you want to modify in Oracle Identity Manager Advanced Administration.

2. In the Allowed Resources tab of the request template details page, select the resource of role that you want to edit.

3. From the Actions list, select **Edit**. The Allowed Resources dialog box is displayed.

4. Search for the resource or role that you want to edit.

5. From the Available Resources list, select a resources or multiple resources and click **Move** or **Move All** to include the resources in the Selected Resources list.

6. Click **Perform**. The resource is listed in the Allowed Resources tab.
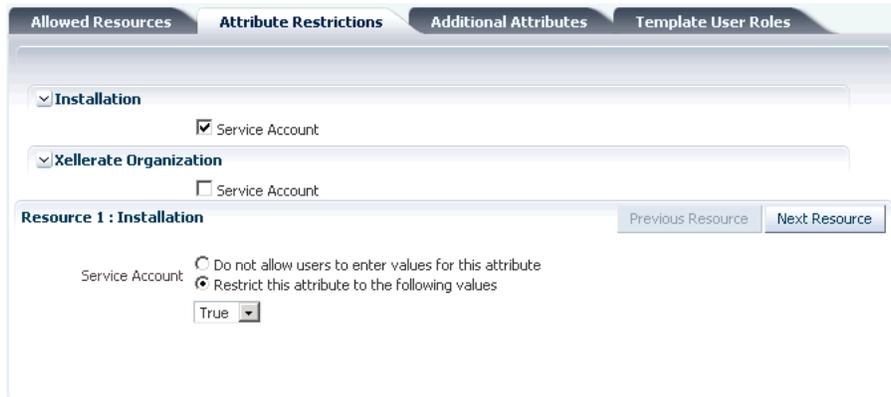
To delete a resource or role:

1. Select the resource or role that you want to delete.

2. From the Actions list, select **Delete**. A message box is displayed that confirms the deletion.

3. Click **OK**.

17.2.2 Attribute Restrictions

This tab contains the attribute restrictions, if any. Figure 17–3 shows the Attribute Restrictions tab:

Figure 17–3   The Attribute Restrictions Tab

Using this tab, you can put additional restrictions on the entity types that you can select if it is associated with a generic request type. To do so:

1. Go to Oracle Identity Manager Advanced Administration.

2. In the Selected Resources section of the Attribute Restrictions tab, select a resource whose attributes you want to restrict.

3. Specify the attributes that you want to specify in the lower part of the tab.

4. Click **Next Resource**. The attributes for the next resource are displayed.

5. Specify the attributes for the resource.

17.2.3 Additional Attributes

This tab is always displayed. Figure 17–4 shows the Additional Attributes tab:

Figure 17–4   The Additional Attributes Tab

Using this tab, you can specify additional attributes for data collection at the template level. These attributes are collected when the user creates a request. This data cannot

be used during request execution. Also, you can only add new template attributes or delete the existing template attributes

To specify additional attributes for data collection:

1. Open/Edit the Request Template that you want to modify in Oracle Identity Manager Advanced Administration.

2. In the Attribute Name field of the Additional Attributes tab, enter a name of the attribute.

3. From the Data Type list, select a value from String, Number, Date or Boolean.

4. From the Display Type list, select the type of field, such as text field, radio button, date field, check box, and date area, which you want to display for this attribute.

5. Click **Add**. The attribute is added to the Additional Attributes section.

To delete an additional attribute, select the attribute and select **Delete** from the Actions list.

17.2.4 Template User Roles

This tab allows you to select the roles that can be assigned to the request template. Only the users with the role are able to create requests by using the template. Figure 17–5 shows the Template User Roles tab:

Figure 17–5   The Template User Roles Tab
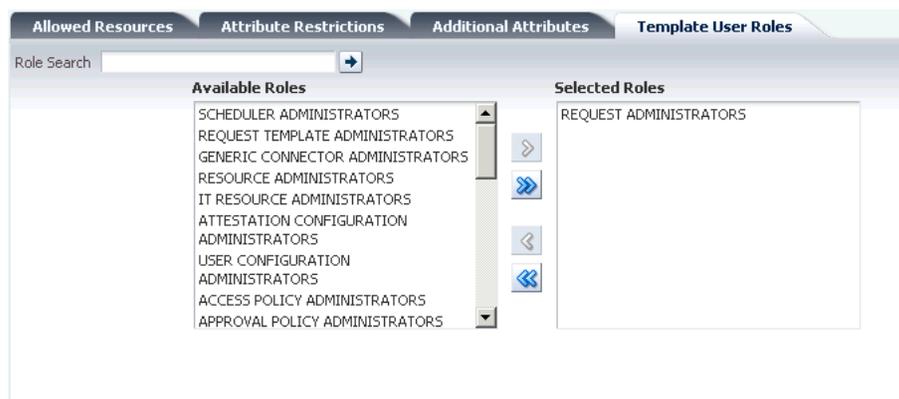
To select roles for assigning to the request template:

1. Open/Edit the Request Template that you want to modify in Oracle Identity Manager Advanced Administration.

2. From the Available Roles list of the Template User Roles tab, select the roles that you want to create requests by using this template.

3. Click **Move** or **Move All** to include the roles in the Selected Roles list.

17.3 Cloning Templates

Cloning a request template is the procedure to create a new request template by inheriting all the properties of an existing request template.

To clone a request template:

1. Go to Oracle Identity Manager Advanced Administration.

2. From the advanced search results in the Template Details page, select a request template that you want to clone.

3. From the Actions menu, select **Clone**. The Clone Template page is displayed with the details of the request template that you have selected for cloning.

4. Modify the required details of the request template for creating the new request template.

5. Click **Save** to create the new request template.

17.4 Deleting Templates

To delete a template as a member of the Templates Administrators role:

1. In the Request Templates tab in Oracle Identity Manager Advanced Administration, search for the existing request templates.

2. From the search results table, select the template that you want to delete.

3. From the Actions list, select **Delete**. A message box is displayed that asks for confirmation.

4. Click **OK** to confirm.

> **Note:** If the template to be deleted is referred by any existing requests, then it cannot be deleted.

18

Managing Approval Policies

Approval policy is a configurable entity of request management that helps associate various request types with approval processes defined in the request service only for request and operation level approvals. It associates approval workflows to be loaded at request or operation levels for a request type. You can use approval policies to associate various request types with various approval processes, which are the BPEL workflows. Approval policies control which approval process is to be invoked based on the request data evaluation.

You can define multiple approval policies for a request type. Each approval policy is associated with an approval process. When the request is submitted, in the approval initiation phase, all the approval processes associated with the request are picked up dynamically. Each approval policy decides on what process to invoke based on approval policy priority and approval policy rule.

Approval policy priorities are based on the following:

- For request level, request type + request level

- For operation level, request type + operation level + scope, which is the specific entity associated with the request

Each approval policy has a priority in the backend. When the request engine invokes the workflows, it picks up all the available approval policies in the order of priority. The approval policy with higher priority is called and its approval policy rule is evaluated. If the evaluation fails, then the approval policy rule of the approval policy with the next priority is evaluated. If the outcome of the evaluation is true, then the corresponding approval process associated with the approval policy is selected to be the workflow for that request. For information about creating approval policy rules, see "Creating Approval Policies" on page 18-4.

> **Note:** There is only one approval policy rule per approval policy. The rules can be complex, containing multiple conditions and other rules. The rules do not exist as independent entities and cannot be reused in any other approval policy. There is no default rule for an approval policy.

This chapter describes the following topics:

- Approval Selection Methodologies

- Creating Approval Policies

- Searching Approval Policies

- Modifying Approval Policies

- Modifying the Priority of an Approval Policy

- Deleting Approval Policies

> **Note:** Only the users that are members of the APPROVAL POLICY ADMINISTRATORS role are authorized to create, search, modify, and delete approval policies. See "Approval Policy Management" on page 13-18 for more information about authorization for approval policies.

18.1 Approval Selection Methodologies

Request types do not define approval. Models define the underlying methodology for approval only at the operation level. Every request goes through request level of approval, and therefore, do not require explicit configuration of methodology at the request type. The methodology picks the right approval to be used based on the approval policy configuration. An approval process selection methodology is an algorithm that selects the approval workflow to be initiated. Based on the request type, the request engine decides which methodology to be used and evaluates the approval process accordingly.

If no approvals are defined at the request level, it means that a default approval process is invoked. This default approval process is shipped with Oracle Identity Manager and is assigned to the administrator. If no approvals are defined at the operation level, it means that a default approval process is invoked. If no template-level approvals are defined, then it is assumed that no approvals are required at that level.

The following methodologies are supported:

- Request-Level Methodology

- Operation-Level Methodology: Organization-Based Selection

- Operation-Level Methodology: Resource-Based Selection

- Operation-Level Methodology: Role-Based Selection

18.1.1 Request-Level Methodology

The determination algorithm of the request-level selection methodology is as follows:

1. Search for all the approval policies configured for the request level and for the request type with which the request is associated in ascending order of approval policy priority. If the approval policies matching this criteria is found, then:

   a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating the approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval at the request level or operation level is specified, then the approval is by default.

   b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the request level.

2. If no approval workflow is determined, then the default request-level approval is selected.

18.1.2 Operation-Level Methodology: Organization-Based Selection

The determination algorithm for the organization-based selection methodology at operation level is as follows:

1. Search for the user's organization entity for which request is created.

2. Search for all the approval policies configured for the operation level, for the request type associated with the request, and for the user's organization entity in ascending order of the approval policy priority. If the approval policies matching this criteria is found, then:

   a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval at the request level or operation level is specified, then the approval is by default.

   b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the operation level for this organization.

3. If no approval workflow is configured for that organization entity, then follow the organization hierarchy till either the root node or the domain boundary, which is the root organization in the organization hierarchy. Repeat step 2 for each organization node.

4. If no approval workflow is determined, then the default operation-level approval is selected.

18.1.3 Operation-Level Methodology: Resource-Based Selection

The determination algorithm for the resource-based selection methodology at operation level is as follows:

1. Search for the resource entity being provisioned or deprovisioned to the user.

2. Search for all the approval policies configured for the operation level, for the request type associated with the request, and for the resource being provisioned or deprovisioned in ascending order of the approval policy priority. If the approval policies matching this criteria is found, then:

   a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval at the request level or operation level is specified, then the approval is by default.

   b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the operation level for this resource.

3. If no approval workflow is determined, then the default operation-level approval is selected.

18.1.4 Operation-Level Methodology: Role-Based Selection

The determination algorithm for the role-based selection methodology at operation level is as follows:

1. Search for the role entity being assigned to or removed from the user.

2. Search for all the approval policies configured for the operation level, for the request type associated with the request, and for the role being assigned or removed in ascending order of the approval policy priority. If the approval policies matching this criteria is found, then:

   a. Evaluate the approval policy rules associated with each approval policy to determine the approval workflow. When evaluating approval policy rules, for the first approval policy rule whose evaluation results in true, the corresponding approval workflow associated with that approval policy is selected. If automatic approval at the request level or operation level is specified, then the approval is by default.

   b. If none of the approval policy rules are satisfied, then it is considered that no approval workflow is configured at the operation level for this role.

3. If no approval workflow is determined, then the default operation-level approval is selected.

18.2 Creating Approval Policies

To create an approval policy:

1. Go to Oracle Identity Manager Advanced Administration.

2. In Oracle Identity Manager Advanced Administration, click the **Policies** tab, and then click **Approval Policies**. Alternatively, under Policies, you can click **Search Approval Policies**.

3. From the Actions menu on the left pane, select **Create**. You can also start the Create Approval Policy wizard by clicking the icon with the plus (+) sign on the toolbar. The Step 1. Set Approval Policy Details page of the Create Approval Policy wizard is displayed.

4. Enter values for the following fields, and then click **Next**:

   - **Policy Name**: Enter a name for the approval policy. This is a mandatory attribute.

   - **Description**: Enter the details about what this approval policy will do.

   - **Model Name**: Select the request model name by selecting from the LOV, for example, Assign Roles. This is a mandatory attribute.

   - **Level**: Select the approval level that you want to implement for this approval policy. This is a mandatory attribute. For more information about approval levels, see "Approval Levels" section in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

   - **Scope Type**: Select this option to the Scope Type associated with the approval policy, that is, the entity name based on the request type selected.

   - **All Scope**: Select this option to specify the approval policy associated with all entity for a particular entity type. An approval policy can be associated with All Scope based on the Scope Type.

   - **Scope**: Select this option to specify the approval policy associated with the specific entity for a particular entity type. An approval policy can be associated with a specific Scope based on the Scope Type.

   - **Auto Approval**: Select this option to specify automatic approval at the request level or operation level that you select in the Level field.

- **Approval Process**: Select the workflow that you want to associate with this approval policy. This is a mandatory attribute.

5. On the Step 2. Set Approval Rule and Component page, enter the name of the approval policy rule in the Rule Name field, for example, RuleTest1.

6. In the Rule Components section, you can define the parameters of the approval policy rule. To do so, click the icon next to the View list. The Add Simple Rule dialog box is displayed. In this dialog box, you must select values for the following fields, and then click **Add**.

   - **Entity**: Entity, such as Requester, Beneficiary, or Resource, with which the approval policy rule is associated. This varies based on the selected request type.

   - **Attribute**: Attribute of the above selected entity.

   - **Condition**: Condition of the approval policy rule, such as Equals, Not Equals, or Starts With.

   - **Value**: Value of the condition.

     > **Note:** If you use the User Login attribute in a rule expression, the corresponding User Login ID value must be entered in all uppercase letters, otherwise the expression will not evaluate to true.

   - **Parent Rule Container**: The rule container with which this approval policy rule needs to be associated with.

     > **Note:** When writing simple rule expressions, if an entity attribute has an encoded value, then create the expression by using the encoded value, not the lookup-code definition. For example, for the account status attribute, create the expression by using the encoded value 1 or 0, not the decoded value Locked or Unlocked.

7. To add a rule container for the approval policy rule, in the Rule Components section, from the Actions menu, select **Add Rule Container**. The Add Rule Container dialog box is displayed. In this dialog box, enter or select values for the following fields, and then click **Add**.

   - **Rule Container Nam**e: The name of the rule container.

   - **Parent Rule Container**: The name of the rule container under which you want to create this rule container. A rule container can hold either another rule container or rule elements with the AND or OR operators in a hierarchical order.

   - **Operator**: The operators are AND and OR.

8. When you click Perform on the Add Simple Rule dialog box, a simple approval policy rule is created and added in the Step 2. Set Approval Rule and Component page. Click **Next**.

9. On the Step 3. Review Approval Policy Summary page, verify the information that you have specified for the approval policy. You can click the Back button to modify any information if you want. Click **Finish** to create the approval policy.

10. A message is displayed confirming that the approval policy has been created. Click **OK**.

18.3 Searching Approval Policies

To search for approval policies:

1. Go to Oracle Identity Manager Advanced Administration.

2. On the left pane of the Approval Policies tab, in the Search field, enter a search criterion to search for approval policies. You can specify the asterisk (*) wildcard character to specify the search criterion.

> **Note:** In simple and advanced search for approval policies, searching with translated approval policy names is not supported. Oracle Identity Manager supports only English string search for approval policies. For default approval policies, you can search with English policy names as stored in the database. However, if you create an approval policy by specifying its name in another language, then you can search it by using the same string, and not in any other language.

3. Click the Search icon. A list of approval policies is displayed in a search results table, with the following fields:

   - **Policy Name**: The name of the approval policy

   - **Model Name**: The name of the request model associated with the approval policy

   - **Scope**: The associated resource, organization, or role name

   - **Level**: The approval level

   - **Rule Name**: The name of the approval policy rule

   - **Approval Process**: The approval process associated with the approval policy

   - **Priority**: Priority of the approval policy

   You can also use the Advanced Search option in the Approval Policies tab to search for approval policies based on advanced search criteria. To do so:

   1. On the left pane of the Approval Policies tab, click **Advanced Search**. The Advanced Search: Approval Policies page is displayed.

   2. Enter values in the fields to specify a search criteria. You can specify a combination of approval policy name, name of the request type associated with the approval policy, approval level, scope type such as resource, organization, or role, and scope to specify the search criteria.

   3. Click **Search**. The search result displays a list of approval policies with information about priority, policy name, model name, scope, level, rule name, and approval process.

18.4 Modifying Approval Policies

To modify approval policies:

1. On the search results table, select a policy.

2. From the Actions menu, select **Open**. The Approval Policy Details form is displayed.

3. In the Policy Details section, edit the fields to modify the approval policy.

> **Note:** You cannot modify the approval policy rule name and approval policy priority attribute.

4. In the Approval Rules section, modify approval policy rules, if required. To modify an approval policy rule, you can add a simple rule, add a rule container, modify rule components, or delete a rule component. For detailed information about adding approval policy rules and rule containers, see steps 6 through 8 in "Creating Approval Policies" on page 18-4.

5. To modify rule components:

   a. Select the approval policy rule.

   b. From the Actions menu, select **Modify Rule Components**. The Modify Rule Components dialog box is displayed.

   c. Edit the values in the fields provided, and click **Perform**.

6. To delete rule components:

   a. Select the approval policy rule that you want to delete.

   b. From the Actions menu, select **Delete Rule Components**. A message box is displayed asking for confirmation.

   c. Click **OK** to confirm the deletion.

7. Click **Save** to save the changes in the approval policy.

18.5 Modifying the Priority of an Approval Policy

To modify the priority of an approval policy:

1. From the approval policies search result, select a policy whose priority you want to modify.

2. From the Actions menu, select **Set Priority**. The Modify Approval Policy priority wizard is displayed.

3. In the Set Policy Details page, specify values in the fields as required. For information about the fields in this page, see step 4 in "Creating Approval Policies" on page 18-4. Then, click **Next**.

4. In the Set Policy Priorities page, enter a number to specify the priority of the approval policy. Then, click **Next**.

5. In the Review and Confirm page, the policy name and the priority that you set are displayed for your review. If you want to change the current priority, then click **Back**.

   Otherwise, click **Finish**. A message is displayed stating the approval policy priority has been changed successfully.

6. Click **OK**.

18.6 Deleting Approval Policies

To delete an approval policy:

1. Go to Oracle Identity Manager Advanced Administration.

2. In the search results table on the left pane or on the advanced search results, select the approval policy that you want to delete.

3. From the Actions menu, select **Delete**. A message box is displayed asking for confirmation.

4. Click **OK** to confirm the deletion.

19

Managing Attestation Processes

This chapter is divided into the following sections:

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

19.1 About Attestation

Attestation enables users designated as reviewers to be notified of reports they must review. These reports describe entitlements of other users. A reviewer can attest to the accuracy of these entitlements by providing a response. The attestation action, along with the response the reviewer provides, any associated comments, and an audit view of the data that the reviewer views and attests to, is tracked and audited to provide a complete trail of accountability. In Oracle Identity Manager, this process is known as an **attestation task**.

In Oracle Identity Manager, attestation is supported through the definition of scheduled attestation processes. An attestation process is not the same as an Oracle Identity Manager workflow. It is implemented as a configurable business process in Oracle Identity Manager, and it creates an attestation task for a user. The user acts as a reviewer, and must complete this process to provide correct audit information.

Tracking of attestation activity for a provisioned resource instance is done through tasks in the provisioning processes of resource objects. You can initiate workflow activity based on attestation actions. Additional activities to be started, and a workflow that can be modeled in the process definition form or workflow designer can be initiated, based on an initial attestation action. This is possible due to attestation subflows in the provisioning processes defined in Oracle Identity Manager.

Attestation activity can be initiated on a periodic basis or when required.

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

This section discusses the following topics:

- Definition of an Attestation Process
- Components of Attestation Tasks
- Attestation Request

- [Delegation](#)
- [Attestation Lifecycle Process](#)
- [Attestation Engine](#)
- [Attestation Scheduled Task](#)
- [Attestation-Driven Workflow Capability](#)
- [Attestation E-Mail](#)

19.1.1 Definition of an Attestation Process

An **attestation process** is the mechanism by which an attestation task is set up. Input that an attestation process requires includes information about how to define the components that constitute the attestation task and how to associate the attestation task with a schedule at which the task must be run. This definition is also the basis on which the attestation task can be initiated when required. An attestation process definition includes:

- **User Scope or Resource Scope**: This defines the algorithm by which the target user entitlements of the attestation process are determined.

- **Reviewer Setup**: This specifies the reviewer, who attests the entitlements of other users. An attestation process can specify a particular user as the reviewer, or can specify more abstractly how to select the reviewer. For example, the reviewer can be specified as the user's manager, as an administrator of the resource, as an authorizer of access to the resource, or as a member of the role that grants the entitlement.

- **Definition of Attestation Schedule**: This specifies the schedule for running the attestation process.

- **Process Owner**: This is a designated group of users that are responsible for monitoring activities related to the process.
  - They will be notified of any issues that occur when the process runs.
  - They will have permissions to view the process definition, but will not have administrative permissions by default.
  - They will be able to execute the process whenever required.

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.

19.1.1.1 Attestation Process Control

The following sections describe how you can control attestation processes.

19.1.1.1.1 Disabling Processes An attestation process can be disabled by the system administrator to prevent it from running at its preconfigured schedule. This gives an administrator better control over the environment. A system administrator attestation process can be enabled, but it cannot be enabled if its Next Run Time value is in the past. A user who enables an attestation process must set its next run time in the future.

19.1.1.1.2 Deleting Processes An attestation process can be deleted. This is called a soft-delete. It does not actually delete the records because the records must be maintained for audit purposes. Instead, the attestation process will be marked as deleted.

A deleted process is not displayed in Oracle Identity Manager Administrative and User Console. Because process names and codes are unique, a name once used is no longer available, and no new attestation process can be created with the same name.

19.1.2 Components of Attestation Tasks

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

- **A Reviewer**: This specifies the user who performs the attestation.

- **Task Source**: This specifies whether or not the attestation task is a result of a process or because of delegation by another reviewer. In the case of delegation, the task must track the reviewer who delegated the task, and which task is the source of the entitlements.

- **Attestation Data**: This is detailed data about user entitlements in the attestation scope. This data is from the process form of the provisioned resource instance.

- **Attestation Date**: This defines the date on which the attestation task is initiated.

- **Attestation Actions**: These are the actions that the reviewer can take on the attestation scope. The action is not at the level of attestation task overall, but rather against each entitlement in the attestation scope. The following are attestation actions:

  - **Certify**: The reviewer agrees that the user being reviewed is allowed to have the entitlement in its current form, including any specific data or fine-grained permissions.

  - **Reject**: The reviewer does not think that the user must have this entitlement in the form.

  - **Decline**: The reviewer does not want to accept the responsibility of attesting to the entitlement. This action is usually for cases in which processes have been configured incorrectly, and is useful in the early stages of a rollout.

    A reviewer declines a task when the reviewer wants someone else to act upon the task. When a task is declined, it gets assigned to a random user in the System Administrator role.

  - **Delegate**: The reviewer wants to reassign the attestation of this entitlement to another qualified person.

> **Note:** The attestation tasks are not workflow tasks in Oracle Identity Manager definition. They are not created as part of workflow. Attestation tasks do not support all the task management features that the workflow engine supports such as dynamic assignment, escalation, and proxy management.

19.1.2.1 Attestation Inbox

From the Attestation Inbox, a reviewer can view the details of each attestation task. Within an attestation task, the reviewer can provide responses or comments for individual entitlements.

19.1.3 Attestation Request

When an attestation process is executed, an attestation request is created and recorded in Oracle Identity Manager database. This request records for audit purposes, when an attestation process is executed. The attestation request record consists of basic identity and audit data and statistical data that is used in reports. The data includes the following items:

- A request ID: Each attestation request has a unique identifier. Each attestation task that Oracle Identity Manager creates as a result of a request, stores as part of its record, the request ID of the associated attestation request.

- Date and time of execution of the process.

- Date and time of completion of the process: The date and time of completion of the process is considered to be the date and time for that request.

- Total number of entitlements identified for attestation.

    The number of provisioned resources that matched the selection criteria (of the resource scope of the attestation process) during this particular execution of the attestation process.

- Number of entitlements certified.

- Number of entitlements rejected.

- Number of entitlements declined.

19.1.4 Delegation

The reviewer who is assigned to an attestation task may not be able to attest to all the entitlements in the task. There may be multiple reasons for this. For example:

- There may be too many entitlements covering too many users in the attestation task

- The reviewer is not sure about the reasons for which the entitlements were provisioned

In these cases, the reviewer may want to involve other people in the review. A reviewer can delegate attestation of certain entitlements in the task.

To delegate attestation, the reviewer selects a set of entitlements in the task and delegates them to another user. This creates a new attestation task that is assigned to the selected reviewer.

The new task contains only those entitlements that the original reviewer selected. The original reviewer is no longer responsible for providing an attestation response for those entitlements. The new attestation task assigned to the delegate would track who performed the delegation, which task it was created from, and some other information, for example, the request ID. The new attestation task is treated in the same manner as any other attestation task. It can even be delegated. Figure 19–1 shows delegate attestation page.

Figure 19–1   Delegate Attestation

19.1.5 Attestation Lifecycle Process

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

19.1.5.1 Stage 1: Creation of an Attestation Task

This stage starts when an attestation process is run. Figure 19–2 describes the workflow involved in this stage.

Figure 19–2   Creating an Attestation Task: Workflow
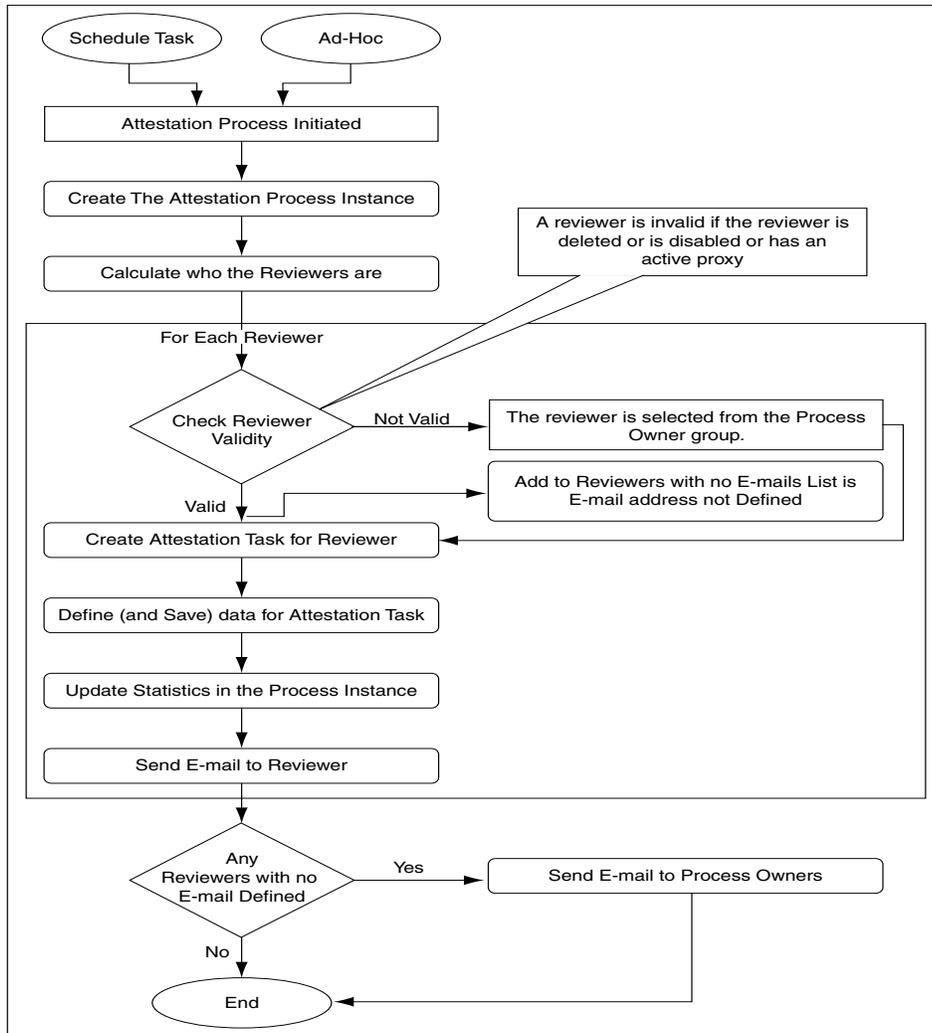
When the attestation process is run, it first creates a corresponding attestation process instance. It then identifies the reviewers for this run of the process. In most cases, there is only one reviewer. There can even be a set of reviewers.

Whenever an invalid reviewer is found, a new reviewer is fetched from the process owner group. Oracle Identity Manager will select, if possible, a member of the process owner group who has not yet been used as a reviewer for this attestation request. If this is not possible, then Oracle Identity Manager will select a member of the process owner group who has already been selected to act as a reviewer. If Oracle Identity Manager cannot find a member of the process owner group, then it will assign XELSYSADM as the reviewer for the attestation task.

For each valid reviewer, the process calculates all the user entitlements that the reviewer must attest to as part of that task, as determined by the attestation scope defined in the process. The process then adds a reference and any related information regarding those user entitlements to the attestation data of the task. It also adds the number of entitlements covered by that task to the statistical field for the total number of entitlements identified for attestation in the process instance. The process then sends an e-mail message to the reviewer. It also sends e-mail to process owners about the reviewers with no e-mail address defined.

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

19.1.5.2 Stage 2: Acting on an Attestation Task

When an attestation task is assigned to a reviewer, the reviewer receives an e-mail, and the task is displayed in the reviewer's attestation inbox. The reviewer views task details in this inbox.

From the task details page, the reviewer provides a response and, if required, a comment for each entitlement. This marks the attestation entitlement detail in the task as **Response Provided**.

If the reviewer's response includes delegating the attestation activity for a specific entitlement, then the reviewer must provide a delegated user. Optionally, the reviewer can provide comments explaining why the reviewer is delegating the attestation activity to that user.

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

Figure 19–3   Flow of Events When Reviewer Responds to Entitlement
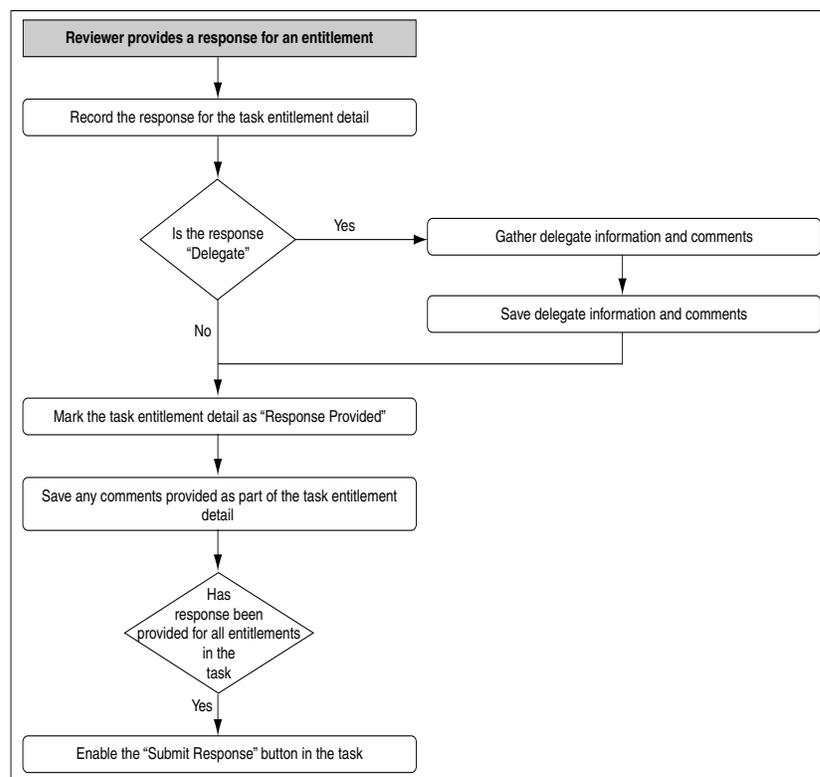
At this point, the next stage of the Attestation Business Process begins.

19.1.5.3 Stage 3: Processing a Submitted Attestation Task

The Attestation Task is marked as **Submitted**. At this point the attestation task is frozen, and cannot be acted on further. For each entitlement in the attestation task, the response is examined by the system. If the response is to either certify or reject, then the provisioned resource instance corresponding to that entitlement is updated accordingly. At the provisioned resource instance level, the last attestation result, the

time at which last attestation occurred, and who the reviewer was are recorded. If the response is to decline or delegate, then the attestation detail at the provisioned resource level is not changed.

The **User Attestation Event Occurred** task is inserted into the provisioning process of the resource instance. This starts any attestation-driven workflows that may have been defined. Any comments are saved to the notes field of the task.

The attestation entitlement detail in the task is marked as **Response Submitted**. Figure 19–4 shows the flow of events after the attestation task response is submitted.

Figure 19–4   Flow of Events After Attestation Task Response Is Submitted
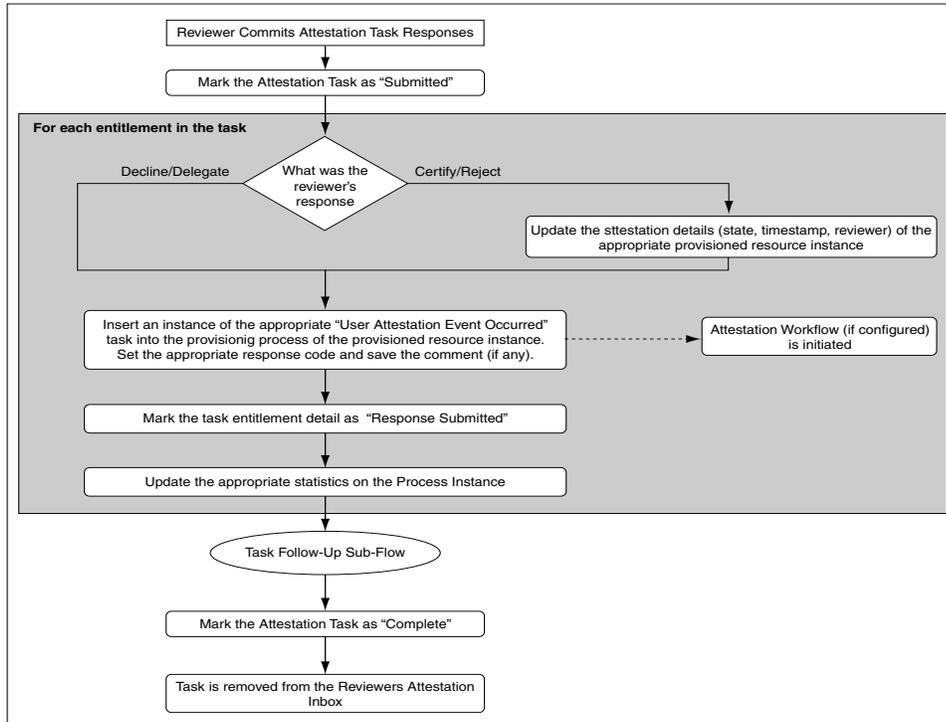
The following statistics are updated on the process instance:

- Number of entitlements certified
- Number of entitlements rejected
- Number of entitlements declined
- Number of entitlements delegated

After all entitlements are covered, a subflow for follow-up action is initiated. In this flow, the process examines if the response for any of the entitlements in the task was declined. If there were any such entitlements, then the process sends e-mail to the Process Owner outlining the details of the decline action.

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

After all the delegated attestation tasks are created, the subflow is completed and it merges back into the main flow. Figure 19–5 shows the flow of events of the follow-up action subflow.

Figure 19–5   Follow-Up Action Sub-Flow
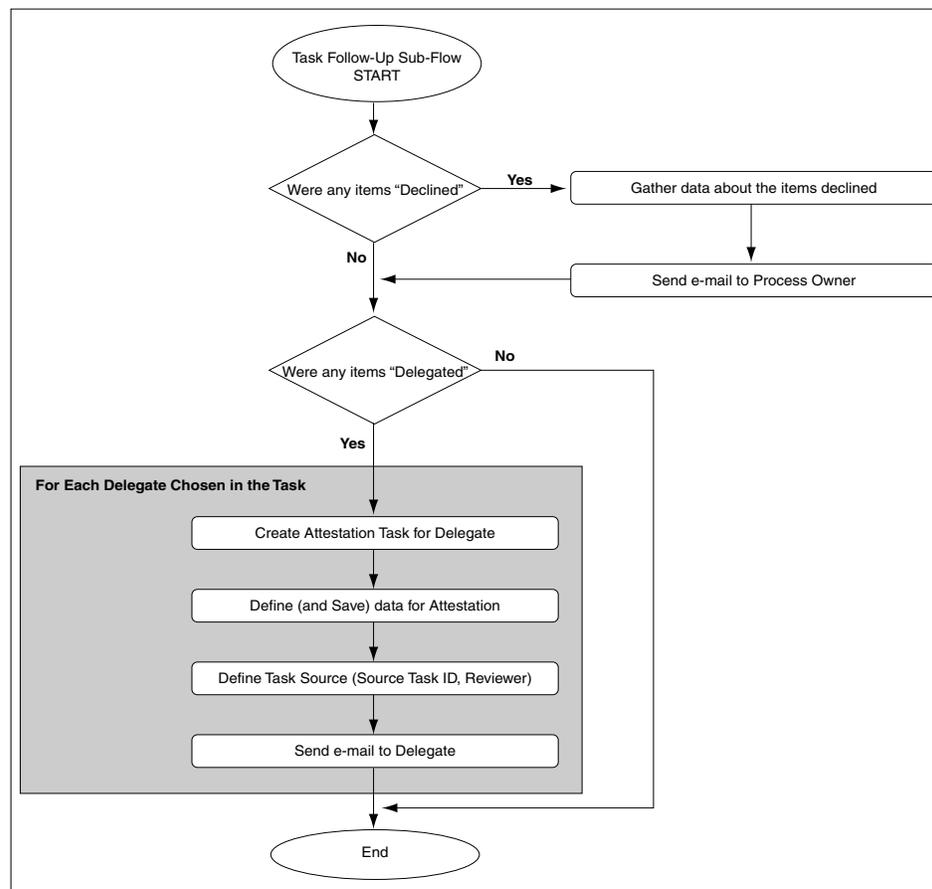
With the follow-up subflow complete, the attestation task is marked as **Complete**.

19.1.6 Attestation Engine

The attestation engine implements the attestation lifecycle. It is a service in Oracle Identity Manager architecture that exposes APIs to receive instructions to initiate a particular attestation process. The API is called from the attestation scheduled task as well as from the Run Now button on the Attestation Process Detail page to support on-demand execution. It supports both drivers for initiation of attestation processes.

The attestation engine uses the JMS messaging service to perform offline, queued processing. This ensures better performance.

> **Note:**   Attestation depends on the entry in the user profile audit data. If the audit entry is not generated for a user who is part of the attestation process, then the reviewer would not be able to see the user and process form information in attestation. To avoid such situations, ensure that the Issue Audit Messages Task scheduled task is run before performing the attestation run.

19.1.7 Attestation Scheduled Task

This new system scheduled task is responsible for examining the attestation processes defined in Oracle Identity Manager, and creating the necessary attestation tasks in the system.

Features of this scheduled task are:

- By default, this scheduled task is set to run every night. You can change the schedule according to your requirements.

- This scheduled task examines the attestation process definition table for all active (not system administrator) attestation processes

- If the scheduled task finds that the next scheduled start time of a process is in the past, then the task sends a call to the Attestation Engine to initiate the attestation process.

19.1.8 Attestation-Driven Workflow Capability

You can enhance the provisioning processes predefined in Oracle Identity Manager to listen to triggers coming from attestation activity. In this way, you can define custom workflows as part of the provisioning workflow that would respond to attestation taking place (or not taking place, in case of a refusal), and therefore be initiated when attestation takes place. This serves two purposes:

- The default attestation task in the flow, User Attestation Event Occurred, would provide the audit trail for the attestation history of the specific user entitlement.

  - There is one instance of this task for each time that resource instance is attested by the appropriate type of attestation process.

  - The response code set on the task indicates what the response provided by the reviewer is.

  - The user tagged as the person creating the task indicates who the reviewer is.

  - Any comment provided by the user is in the notes field for the task.

- Using response-generated tasks, the default task can start the workflow to respond to a particular attestation response received. Therefore, for a particular resource, you can specify that the Reject response must start the appropriate workflow tasks in the provisioning process for disabling the account, as an example.

19.1.9 Attestation E-Mail

As part of the attestation processes, the Attestation Engine sends out e-mail to various interested parties. To make the e-mail configurable with respect to the content, they are made available as e-mail templates of the General type in Oracle Identity Manager Email Definition store. For context-sensitivity, the e-mail contain a set of variables that can be replaced with the required values.

19.1.9.1 Notify Attestation Reviewer

This template is used to build the e-mail to send to the reviewer when an attestation task is assigned to the reviewer.

19.1.9.1.1 Variables The following are variables in the Notify Attestation Reviewer template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task was assigned

19.1.9.1.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Attestation Reviewer template:

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

19.1.9.1.3 Body The body of the e-mail message contains the following information:

```
The attestation task details are as follows
Process Name: Attestation Definition.Process Name
Process Code: Attestation Definition.Process Code
Data Type: Access Rights
Assigned Date: Attestation Task.Task Assigned Date
```

19.1.9.2 Notify Delegated Reviewers

This template is used to build the e-mail to send to a reviewer when an attestation task is delegated to the reviewer.

19.1.9.2.1 Variables The following are variables in the Notify Delegated Reviewers template:

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Definition.Process Code	Code for the attestation process
Attestation Task.Task Assigned Date	Date the attestation task is assigned
Attestation Task.Delegated By First Name	First name of the reviewer who performed the delegation
Attestation Task.Delegated By Last Name	Last name of the reviewer who performed the delegation
Attestation Task.Delegated By User Id	User ID of the reviewer who performed the delegation action

19.1.9.2.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Delegated Reviewers template:

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

19.1.9.2.3 Body The body of the message contains the following information:

```
The attestation task details are as follows
Process Name: Attestation Definition.Process Name
Process Code: Attestation Definition.Process Code
Data Type: Access Rights
Assigned Date: Attestation Task.Task Assigned Date
Delegated By: Attestation Task.Delegated By First Name Attestation Task.Delegated
By Last Name [Attestation Task.Delegated By User Id]
```

19.1.9.3 Notify Process Owner About Declined Attestation Entitlements

The Notify Declined Attestation Entitlements template is used to build the e-mail to send to process owners notifying them of any declined entitlement attestations.

19.1.9.3.1 Variables The following are variables in the Notify Process Owner about Declined Attestation Entitlements template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request
Attestation Definition.Process Name	Name of the attestation process
Attestation Task.Reviewer First Name	First name of the reviewer
Attestation Task.Reviewer Last Name	Last name of the reviewer
Attestation Task.Reviewer User Id	User ID of the reviewer
Attestation Data.Provisioned User First Name	First name of the user being attested
Attestation Data.Provisioned User Last Name	Last name of the user being attested
Attestation Data.Provisioned User Id	User ID of the user being attested
Attestation Data.Resource Name	Name of the resource being attested
Attestation Data.Entitlement Descriptive Data	Descriptive data of the entitlement being attested

19.1.9.3.2 Subject Line The following is the Subject line of e-mail messages defined by the Notify Process Owner About Declined Attestation Entitlements template:

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

19.1.9.3.3 Body The following is displayed in the body of the message:

```
Attestation of the following user access rights were declined by the reviewer.
Reviewer: Attestation Task.Reviewer First Name Attestation Task.Reviewer Last Name
[Attestation Task.Reviewer User Id]
Attestation Process: Attestation Definition.Process Name
Attestation Request ID: request Attestation Request.Request Id
Access Rights Data: Attestation Data.Provisioned User First Name Attestation
Data.Provisioned User Last Name [Attestation Data.Provisioned User User Id] -
Attestation Data.Resource Name - Attestation Data.Entitlement Descriptive Data
```

19.1.9.3.4 Special Comments Each entitlement data item will appear on a new line.

19.1.9.4 Notify Process Owner About Reviewers with No E-Mail Defined

The Attestation Reviewers With No Email Defined template is used to build the e-mail to send to process owners notifying them of reviewers for whom there is no e-mail address defined.

19.1.9.4.1 Variables The following are variables in the Notify Process Owner About Reviewers with No Email Defined template:

Variable	Description
Attestation Request.Request Id	ID of the attestation request

Variable	Description
Attestation Definition.Process Name	Name of the attestation process
Attestation Request.Request Creation Date	Date when the attestation request was created
Attestation Task.Reviewer First Name	First name of the reviewer that is invalid
Attestation Task.Reviewer Last Name	Last name of the reviewer that is invalid
Attestation Task.Reviewer User Id	User ID of the reviewer that is invalid

19.1.9.4.2 Subject Line The following is the Subject line for e-mail defined by the Notify Process Owner About Reviewers with No Email Defined template:

```
E-mail address is not defined for some of the reviewers in attestation process
Attestation Definition.Process Name, request Attestation Request.Request Id
```

19.1.9.4.3 Body The following is the body of the message:

```
The following attestation reviewers do not have e-mail addresses defined.
Attestation requests have been generated for these reviewers and can be accessed
by logging in to Oracle Identity Manager. However, notification e-mails were not
sent.
Attestation process: Attestation Definition.Process Name
Attestation Request ID: request Attestation Request.Request Id
Request date: Attestation Request.Request Creation Date
Reviewers Without Email: Attestation Task.Reviewer First Name Attestation
Task.Reviewer Last Name [Attestation Task.Reviewer User Id]
```

19.1.9.4.4 Special Comments Each reviewer detail appears on a new line.

19.2 Attestation Process Configuration

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

- Define new attestation processes.

- Manage existing processes.

- Initiate ad-hoc attestation processes.

19.2.1 Menu Structure

The top-level Attestation menu contains the following links in the Policies section of Oracle Identity Manager Advanced Administration:

- Create Attestation Process

- Manage Attestation Process

These menu items are governed by the same delegated administration permissions that govern all menu items in the Advanced Administration.

These menu items are defined but not assigned to any group in Oracle Identity Manager. They will be assigned to the System Administrators group in Oracle Identity Manager if audit compliance components are installed.

19.2.2 System Control

Attestation has the following dependencies:

- The User Profile Audit feature must be enabled.

- Historical data must be collected at least up to the Process Form level.

If the auditing level is set below the required levels, then clicking menu item links related to attestation generates the Attestation Feature Not Available page, and prevents the user from defining any attestation processes.

Audit levels are controlled by the system property called XL.UserProfileAuditDataCollection and the attestation feature expects this value to be set to at least Resource Form.

19.3 Creating Attestation Processes

> **Note:** Oracle Identity Manager Permission model applies to the procedure described in this section. This model restricts any list of targets (for example, users) to only those targets for which the logged-in user has read access.

To create an attestation process:

1. In the Welcome page of Oracle Identity Manager Advanced Administration, under Attestation Configuration list, select **Create**.

   The Step1: Define Process page is displayed.

2. Enter values for the fields described in the following table, and then click **Continue**:

Field	Description
Name	A unique name for the attestation process. The name must be unique across system administrator and deleted attestation processes.
Code	An identifying code (up to 32 characters) for the process. The code must be unique across system administrator and deleted attestation processes.
	Note: A code enhances the identification of the attestation process definition. However, if you do not specify a value in the Code field, then the attestation process is identified by the unique name.
Description	Detailed description of the attestation process.

3. On the Step 2: Define User Scope page:

   a. Select an attribute from the **Attribute** list. The Attribute list displays the user attributes given in the FormMetaData.xml file and the user-defined attributes from the user form. The attribute that you select is used to specify the criteria that must be met by users on whom the attestation process is applied.

   b. From the **Condition** list, select a condition. The Condition list of values will change based on the type of attribute selected. For example, if you select User ID in the Attribute field, then the conditions displayed are Contains, Does Not

Contain, Is Exactly, and Is Not Exactly. If you select the Start Date attribute, then the conditions displayed are Before, After, and Between.

c. In the **Value** field, enter a value for the user attribute.

d. Select the **Recursive** option. The Recursive check box is used for the entities for which you want to include the child entities while defining user scope. For example, if you select **Organization** in the user scope and then select **Recursive**, then the operation also includes all the suborganizations.

e. Click **Add** to add a new row to the user scope table, and click **Continue**. If you add multiple rows to the user scope table, then the attestation process will apply only to users who match all of the attribute conditions in the user scope.

4. On the Step 3: Define Resource Scope page, select a resource for the attestation process as follows:

a. From the **Attribute** list, select one of the resource attributes listed in the following table:

Attribute	Expression	Description
Name	Full text or wildcard	The name of the resource.
Type	Lookup values with the option to select all or a subset	The type of resource.
Resource Audit Objectives	Lookup values with the option to select all or a subset	The audit objectives assigned for a resource, which is provisioned. For example, whether or not the resource is financially significant.
		For more information about Resource Audit Objectives, see "Viewing Resource Details" on page 12-1.
Administrator User Groups	Lookup values with the option to select all or a subset	The user groups that have administrative permissions for a resource.
Authorized User Groups	Lookup values with the option to select all or a subset	The user groups that are authorizers or approvers for the resources.
Resource Status	Full text or wildcard	The status displayed when a resource is provisioned to a user, such as Certify, Reject, Open, or Closed.

b. From the **Condition** list, select a search condition.

c. In the **Value** field, enter a value for the resource attribute.

d. Click **Add** to add a new row to the resource scope table, and then click **Continue**. If you add multiple rows to the resource scope table, then the attestation process will apply only to resources that match all of the attribute conditions in the resource scope.

5. On the Step 4: Define Administration Details page, define the reviewer to attest data, the attestation process schedule, grace period, and the process owner by performing the following steps:

a. From the **Reviewer** list, select the type of reviewer for the attestation process, such as a single specific user, role member, or resource administrator. Then, select the reviewer from the adjoining lookup field.

When you select "Role Member" as the reviewer type, you must select a role for reviewing a particular attestation task. Once the attestation task has been created and run, it will be assigned to the role you selected based on the following conditions:

- All users who are not in Deleted and Disabled state will be assigned the attestation task.

- If the reviewer in that role happens to be the beneficiary as well, then that user will not be assigned the attestation task.

- If after the above checks, there is no eligible user in that role, then the task is assigned to all the users in the System Administrator role.

   b. Specify the attestation process schedule to run the attestation process once or repeatedly after a specific number of days, months, or years.

   c. Specify the grace period, the number of days in which each reviewer must respond to any attestation task that is generated by this attestation process.

   d. In the **Starting on** field, specify a start date for the attestation process.

   e. In the **Process owner group lookup** field, specify a group that is the process owner for the attestation process.

   f. If you want the process owner to be notified by e-mail if the reviewer refuses the attestation process, select **Email process owner if reviewer refuses attestation request**. Then, click **Continue**.

6. On the Step 5: Verify Info page, review the details of the attestation process, and then click **Create Process**.

You are redirected to a page with a message that you have successfully created an attestation process definition. Clicking the process name takes you to the Attestation Process Detail page. To create another attestation process, click **Create Another Attestation Process Definition**.

The Attestation Process Detail page is described in the "Managing Attestation Processes" section.

19.4 Managing Attestation Processes

To manage attestation processes:

1. In the Welcome page, click **Manage Attestation Process**, and then click **Manage.** The Manage Attestation Process page is displayed.

2. On the Manage Attestation Process page, enter the search criteria for the attestation process you want to manage. You can search by attestation process name, process code, reviewer type, or process owner. After you enter your search criteria, click **Search.** The Attestation Process Details page is displayed with the attestation processes that match your search criteria. The attestation processes displayed are the ones that the logged-in administrator is allowed to view based on permissions, or by virtue of being a member of the Process Owner group. This page does not show any deleted processes. The columns displayed on the page are listed in the following table:

Column	Description
Names	Specifies the name of the process.
Code	Specifies the attestation process code.

Column	Description
Description	Specifies a description for the process.
Status	Indicates whether the attestation process is active or system administrator.
Type	Specifies the type of resource.
User Scope	Specifies the scope of the user who will be a part of the attestation process.
Resource Scope	Specifies the resources that are within the scope of the attestation process.
Reviewer Type	Indicates the type of the reviewer.
Reviewer Name	Indicates the name of the reviewer.
Schedule	Indicates if the process is scheduled to run only once, or on a daily, monthly, or yearly basis.
Last Start	Specifies the last time an attestation process was run.
Next Start	Specifies when the process is scheduled to run next.
Process Owner Group	Indicates the process owner group. In addition, it specifies whether or not the process owner will be notified by e-mail if the reviewer refuses the attestation request.
Last Completion	Specifies the last time an instance of this process was completed.

The rest of this section discusses the following topics:

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

19.4.1 Editing Attestation Processes

To edit an attestation process:

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

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

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

19.4.2 Disabling Attestation Processes

To disable an active attestation process:

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

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

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

19.4.3 Enabling Attestation Processes

An attestation process can be enabled only if its next start time is in the future and if the process is disabled.

To enable an attestation process:

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

   Note that the Enable button is displayed only when the process is disabled.

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

19.4.4 Deleting Attestation Processes

You can edit, disable, or delete an attestation process only as a process administrator with the required permissions.

To delete an attestation process:

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

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

19.4.5 Running Attestation Processes

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

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

19.4.6 Managing Attestation Process Administrators

The tasks of adding, deleting, and updating administrative groups for attestation processes are similar to the tasks of adding, deleting, and updating administrative groups for users and organizations.

To manage the administrators of an attestation process, select **Administrators** from the Additional Details list on the Attestation Process Detail page. The Administrative Groups page is displayed. You can use this page to add and remove administrators for an attestation process and update administrator permissions.

The permission model for an attestation process definition is as follows:

- To view the attestation process definition, the user must be either of the following:
  - A member of a group that has the appropriate read permissions in the administrators group
  - A member of the group that is the process owner
- To edit the attestation process definition, the user must be a member of a group that has the required write permissions in the administrators group.
- To delete the attestation process definition, the user must be a member of a group that has the required delete permissions in the administrators group.

19.4.7 Viewing Attestation Process Execution History

To view the execution history of an attestation process, select **Execution History** from the Additional Details list on the Attestation Process Detail page. The Attestation Process Execution History page is displayed.

The following are the columns in the Attestation Process Execution History table:

Column	Description
Request ID	ID for the attestation process instance that was run
Reviewer	Name of the reviewer for the attestation process
Initiated On	Date and time when the request was started
Completed On	Date and time when the request was completed
	If the request is still pending, then it shows Not Completed.

On the Attestation Process Execution History page, click the request ID link to open the Request Detail page. On this page, you can filter the requests according to the certified, rejected, open, and closed state.

19.5 Using the Attestation Dashboard

You use the Attestation Dashboard to view the state of attestation processes that are owned by any group of which you are a member.

To use the Attestation Dashboard, in the Welcome page of the Advanced Administration, click **Launch Attestation Dashboard** under Event Management. Alternatively, click the Event Management tab, and from the Attestation list, select **Attestation Dashboard**. The Attestation Dashboard page displays a table listing the state of attestation processes that are owned by any group of which you are a member. The Attestation Dashboard table contains the columns listed in the following table:

Column	Description
Process Code	The attestation process code.
Process Name	The name of the process. The Attestation Process Detail page is displayed when the link for an attestation process name is clicked.
Last Completion	The date and time when the instance was run before the latest one was completed. If it does not exist, then the value must be None. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Request Date	The date and time when the last instance of this Process was run. If it has never been run, then the value is New. It is a link that takes the user to the Attestation Request Detail page for the required Attestation Request.
Current Completion	The date and time when the last instance run was completed. If it has not been completed, then the value is Pending.
Total Records	The total number of entitlements identified for attestation and covered by an attestation task as part of the last process instance.
Certified	The number of entitlements certified in the last attestation process instance.
Rejected	The number of entitlements rejected in the last attestation process instance.
Open	All the open records for which no responses have been provided by the reviewers.

19.5.1 Viewing Attestation Request Details

You can access the drill-down page from the Attestation Dashboard page. The drill-down page displays the attestation details of all entitlements covered by a particular run of the Attestation Process.

To view attestation request details:

1. Click the link for the Last Completion or Current Request Page fields listed in the table on the Attestation Dashboard page.

   The Attestation Request Detail page displays the request details for the selected attestation process, along with a table that contains the following columns:

Column	Description
User	User whose entitlement is being attested. The data is displayed as a link. When you click the link, the user profile page is displayed with the user details for the attestation date.
Resource	Resource that is the basis for the entitlement being attested. The data is displayed as a link. When you click the link, a page is displayed with the process form data of the entitlement for the attestation date.
Descriptive Data	Description of the provisioned resource instance.
Comments	Comment or status of the request. The value can be one of the following: ■ Certify ■ Reject ■ Open ■ Closed
Attestation Result	Last response that was provided for the attestation.
Reviewer	User who provided the response. The data is displayed as a link. When you click the link, the user profile page is displayed with the current user details.
Delegation Path	If the attestation of an entitlement goes through any delegation, then you can use the View link in this column to see the Delegation Path Detail page. If no delegation has taken place, then None is displayed.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

2. Any attestation requests that require delegation include a link in the Delegation Path column.

   Clicking the link displays a Delegation Path page that provides information about the delegation path of the attestation request.

   The Data Attested field shows details about the entitlement being attested. It constructs the value by putting together user information, the resource name, and descriptive data in the following format:

   User_First_Name User_Last_Name [User_ID] - Resource_Name - Descriptive_Data

   The table on the Delegation Path page contains the following fields:

Column	Description
Reviewer	The reviewer to whom the entitlement for attestation is assigned. The data is displayed as a link. When you click the link, the current user profile data is displayed.
Attestation Result	Action supplied by the reviewer. Except for the first record, the value is always Delegated.
Attestation Date	The date and time of the attestation response of the reviewer.
Comments	Reviewer comments. Long comments are truncated, and tooltips are used to show the full text of the comments.

19.5.2 E-Mail Notification

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

In the templates, the form user is defined as XELSYSADM. You can change it to a different user. You must ensure that the e-mail address is defined for the user selected to use these templates. Otherwise, the system may not be able to send out notifications.

The following e-mail notification templates are available:

- **Notify Attestation Reviewer:** Used for sending e-mail when an attestation task is assigned to a reviewer.

- **Notify Delegated Reviewers:** Used for sending e-mail to reviewers when an attestation task is delegated to them.

- **Notify Declined Attestation Entitlements:** Used for sending e-mail to users in the Process Owner group if a reviewer declines any entitlements.

- **Attestation Reviewers With No E-Mail Defined:** Used for sending e-mail to users in the Process Owner group if an e-mail address is not defined for any of the reviewers.

19.5.3 Attestation Grace Period Checker Scheduled Task

A system scheduled task called Attestation Grace Period Checker is used to examine the attestation processes defined in Oracle Identity Manager and to create the required attestation tasks.

The features of the Attestation Grace Period Checker scheduled task are:

- The scheduled task is set to run every 30 minutes by default. You can change this according to your requirement.

- The scheduled task examines all active attestation processes.

Part V

Reporting

This part describes Oracle Identity Manager delegated administration functionalities by using the reporting features in the following chapter:

- Chapter 20, "Using Reporting Features"

20

Using Reporting Features

This chapter includes the following sections:

- Reporting Features
- Starting Oracle Identity Management Reports
- Running Oracle Identity Management Reports
- Supported Output Formats
- Reports for Oracle Identity Manager
- Exception Reports
- Creating Reports Using Third-Party Software

> **Note:**
>
> - Oracle Identity Management Reports enables you to use Oracle BI Publisher as the reporting solution for Oracle Identity Management products.
>
> - Oracle Identity Management Reports are classified based on the functional areas. For instance, Access Policy Reports, Attestation, Request and Approval Reports, Password Policy Reports and so on. It is no longer named Operational and Historical.
>
> - Oracle Identity Management Reports provides a restricted-use license for Oracle BI Publisher and easy-to-use reporting packages for multiple Oracle Identity Management products.
>
> - For large-scale deployments, especially those taking advantage of the extensive auditing capabilities of Oracle Identity Manager, it is highly recommended that you deploy a dedicated enterprise-class reporting solution. A solution based on tools such as Oracle Business Intelligence Enterprise Edition can provide the flexibility, automation, and performance required for a large-scale organizations.

20.1 Reporting Features

The following are Oracle Identity Manager reporting features:

- Select and view reports from a predefined list in the BI Publisher.
- Filter report information.
- View reports on-screen in the desired format.

- Provide interactive reports.

20.2 Starting Oracle Identity Management Reports

To start BI Publisher:

1. Navigate to **Start**, **Oracle BI Publisher Desktop**, **Oracle - BIPHome10134**, and then click **Start BI Publisher**.

   The Oracle BI Publisher Home page appears.

2. Enter the user name and password.

3. Click **Sign In**.

20.3 Running Oracle Identity Management Reports

To run a report:

1. Start Oracle Identity Management Reports. See Section 20.2, "Starting Oracle Identity Management Reports" for more information.

2. Click the **more...** link under **Shared Folders**.

3. Do one of the following to access the reports.

   - Click **Oracle Identity Management Reports**.

   - Click the **more...** link under **Oracle Identity Management Reports**.

   The resulting page displays Oracle Identity Management Reports classified according to their functional areas.

4. Select a report by clicking its name.

   The resulting page displays all the reports with its description under the selected report role.

5. Do one of the following to view the report.

   - Select a report by clicking its name.

   - Click **View**.

   The Report Input Parameters page is displayed. This page displays the input parameters that must be provided to run a report. The report input parameters act as a filter criterion.

   In some cases, at least one or more parameter fields are required fields. Some reports do not require any input parameter. If this is not the case, then you must populate at least one of the fields to run a report.

   > **Note:** If you leave the input parameter field blank, and then click **View**, all the information associated with the report is displayed.

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

7. Click **View** to run the report.

   The report is displayed.

20.4 Supported Output Formats

BI Publisher supports multiple report output formats. All reports are generated in a native XML format which can be transformed into different other output formats. The following formats are supported:

- HTML

- PDF

- RTF

- MHTML

20.5 Reports for Oracle Identity Manager

All the reports containing Date type input parameters, have the following default date range in the date type input parameters:

Date Range is : Sysdate-30 To Sysdate.

If you want to run the reports for different date range, then please change the date type input parameters with your date ranges.

Oracle Identity Management Reports are now classified based on the functional areas. For instance, Access Policy Reports, Attestation, Request and Approval Reports, Password Policy Reports, and so on. It is no longer named Operational and Historical.

Oracle Identity Management Reports are classified into the following roles based on their functional areas:

- Access Policy Reports

- Attestation, Request, and Approval Reports

- Role and Organization Reports

- Password Reports

- Resource and Entitlement Reports

- User Reports

20.5.1 Access Policy Reports

Oracle Identity Management BI Publisher Reports provides the following access policy reports for Oracle Identity Manager:

- Access Policy Details

- Access Policy List by Role

20.5.1.1 Access Policy Details

It provides administrators or auditors the ability to view a current snapshot of all the policies defined in Oracle Identity Manager system, along with key information about each policy, and the number of instances in which each policy has been activated.

Input Parameters

The following table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Access Policy Name	Name of the Access Policy

Fields

The following table lists the fields of the report:

Report Field	Description
Description	Description of the policy
Approval Required	Approval required for the policy
Creation Date	Date when the policy is created
Retrofit Access Policy	Retrofit of the access policy
Created By	Name of the person who created the policy
Priority	Priority of the policy

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource

20.5.1.2 Access Policy List by Role

It lists all policies defined in Oracle Identity Manager system by role. This report can be used for operational and compliance purposes.

Input Parameters

The following table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role

Fields

The following table lists the fields of the report:

Report Field	Description
Description	Description of the policy
Approval Required	Approval required for the policy

Report Field	Description
Creation Date	Date when the policy is created
Retrofit Access Policy	Retrofit of the access policy
Created By	Name of the person who created the policy
Priority	Priority of the policy

Columns

The following table lists the columns of the report:

Report Column	Description
Role Name	Name of the role

20.5.2 Attestation, Request, and Approval Reports

Oracle Identity Management BI Publisher Reports provides the following attestation, request, and approval reports for Oracle Identity Manager:

- Approval Activity

- Attestation Process List

- Attestation Request Details

- Attestation Requests by Process

- Attestation Requests by Reviewer

- Request Details

- Request Summary

- Task Assignment History

20.5.2.1 Approval Activity

This report provides the administrators the ability to view the approval activity including requests that are approved, rejected, or pending.Z

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Approver's First Name	First name of the approver
Approver's Last Name	Last name of the approver
Approver's User ID	User ID of the approver
Organization	Name of the organization

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Approver's First Name	First name of the approver
Approver's Last Name	Last name of the approver
Approver's User ID	User ID of the approver
Organization	Organization of the approver
Approval Accepted	Count of the accepted approval
Approval Rejected	Count of the rejected approval
Approvals Pending	Count of the pending approval
Approval Requests Total	Total number of approval requests

20.5.2.2 Attestation Process List

This report displays details of all the attestation process. The security model is implemented in this report.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Process Owner	Owner of the attestation process

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Attestation Process Name	Name of the attestation process
Owner User ID	ID of the owner of attestation process

Report Column	Description
Date of Current Request	Data on which the request was made
Date of Last Completion	Data on which the request was completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined
Delegated	Attestation process delegated
Total	Sum of certified, rejected, and declined

20.5.2.3 Attestation Request Details

It lists details of selected Oracle Identity Manager attestation requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Request ID	ID of the attestation process
Request Initiation Date Range From	Start date of the attestation request
Request Initiation Date Range To	End date of the attestation request

Fields

The following table lists the fields of the report:

Report Field	Description
Attestation Process Name	Name of the attestation process
Attestation Request ID	ID of the attestation request
Request Initiation Date	Date on which the request is initiated
Completion	Date on which the request is completed
Certified	Attestation process certified

Report Field	Description
Rejected	Attestation process rejected
Delegated	Attestation process delegated
No Action	Number of attestation processes on which no action is taken

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user who initiated the attestation request
Last Name	Last name of the user who initiated the attestation request
User ID	ID of the user who initiated the attestation request
Resource	Name of the resource
Descriptive Data	Date on which the request is completed
Reviewer's First Name	First name of the reviewer
Reviewer's Last Name	Last name of the reviewer
Reviewer's User ID	ID of the reviewer
Action	Action taken by the reviewer

20.5.2.4 Attestation Requests by Process

This report displays details of all the attestation process and the request for each process, where the logged in user is a member of the administrator or the owner role of the attestation process.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Attestation Process Name	Name of the attestation process
Attestation Process Owner	Owner of the attestation process

Fields

The following table lists the fields of the report:

Report Field	Description
Attestation Owner	Name of the attestation process owner
Total Number of Requests	Total number of requests
Last Completion Date	Date by which attestation should be completed
Current Request Initiation Date	Date on which attestation is initiated

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	ID of the attestation request
Initiation Date	Date on which attestation is initiated
Completion Date	Date by which attestation should be completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined
Delegated	Attestation process delegated
Total Attested	Sum of certified records, rejected records and declined records

20.5.2.5 Attestation Requests by Reviewer

It displays list of attestation requests by reviewer. The report includes the number of requests associated with each reviewer and information about each request. In addition, it displays the time at which the request is created and completed.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Reviewer First Name	First name of the reviewer
Reviewer Last Name	Last name of the reviewer
Reviewer User ID	User ID of the reviewer

Fields

The following table lists the fields of the report:

Report Field	Description
Reviewer 's First Name	First name of the reviewer
Reviewer 's Last Name	Last name of the reviewer
Reviewer 's User ID	User ID of the reviewer
Total Number of Requests	Count of requests to review

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	ID of the attestation request
Process Name	Name of the process
Initiation Date	Date on which attestation is initiated
Completion Date	Date by which attestation should be completed
Certified	Attestation process certified
Rejected	Attestation process rejected
Declined	Attestation process declined
Delegated	Attestation process delegated
Total Attested	Count of requests to attest

20.5.2.6 Request Details

This report provides administrators the ability to view the details (requestor, current approver and so on) of all requests with the input current status. Additionally, this

report displays the details of all users (user name, organization, manager details, user status and so on) that will be provisioned as a result of the request approval. This helps administrators in planning and prioritizing operational activities so that they may expedite the closure of pending requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Requestor User First Name	First name of the requestor
Requestor User Last Name	Last name of the requestor
Request User ID	ID of the requestor
Request ID	Request ID
Request Parent ID	Parent ID of the request
Request Status	Status of the request
Request Type	Type of the request
Request Date From	Start date of the request
Request Date To	End date of the request
Beneficiary User First Name	First name of the beneficiary
Beneficiary User Last Name	Last name of the beneficiary
Beneficiary User ID	ID of the beneficiary

Fields

The following table lists the fields of the report:

Report Field	Description
Request ID	Request ID
Request Type	Type of the request
Requester User ID	ID of the requester
Request Date	Date on which request is initiated
Approver User ID	ID of the approver
Current Status	Status of the request
Parent Request ID	ID of the parent Requester

Columns

The following table lists the columns of the report, if a beneficiary is present:

Report Column	Description
First Name	First name of the beneficiary
Last Name	Last name of the beneficiary
User ID	ID of the beneficiary
User Type	Type of user
User Status	Status of the beneficiary
Organization	Organization of the beneficiary
Request Value	Request value of the resource

The following table lists the columns of the report, if a beneficiary is not present:

Report Column	Description
Request Name	Name of the request
Request Value	Value of the request

20.5.2.7 Request Summary

This report provides administrators the ability to view the current status of all requests raised in the specified time interval. This helps administrators in planning and prioritizing operational activities so that they may expedite the closure of pending requests.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Request Type	Type of request
Request Date From	Start date of the request
Request Date To	End date of the request
Organization	Details of the organization

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Request ID	Request ID

Report Column	Description
Parent Request ID	ID of the parent Requester
Request Type	Type of request
Request Status	Status of request
Requestor User ID	ID of the requestor
Beneficiary User ID	ID of the beneficiary
Request Details	Details of the request
Approver User ID	ID of the approver
Request Date	Date of request

20.5.2.8 Task Assignment History

It lists the history of all task assignments.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User ID	ID of the beneficiary
Assignee First Name	First name of the assignee
Assignee Last Name	Last name of the assignee
Assignee User ID	ID of the assignee
Assignee Role Name	Role name of the assignee
Assignee User Name	User name of the assignee

Report Column	Description
Employee Type	Type of employee

20.5.3 Role and Organization Reports

Oracle Identity Management BI Publisher Reports provides the following role and organization reports for Oracle Identity Manager:

- Role Membership History

- Role Membership Profile

- Role Membership

- Organization Details

- User Membership History

20.5.3.1 Role Membership History

This report displays membership history of all the roles. The report will not show indirect memberships.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role
Role Category	Category of the role
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Membership Status	Status of membership: Revoked, Active
Effective From	Role membership effective from date
Effective To	Role membership effective to date

Fields

The following table lists the fields of the report:

Report Field	Description
Created By	Name of the person who created the role

Report Field	Description
Creation Date	Date on which the role was created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of employee
Employee Status	Status of the employee
Membership Status	Membership date of the user
Effective From	Membership start date of the user
Effective To	Membership end date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager
Manager's User ID	ID of the manager

20.5.3.2 Role Membership Profile

This report shows number of users present for number of roles and the details of users belonging to count number of roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Organization	Organization of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Membership in Number of Roles	Number of members in number of roles
Number of Users	Number of users in the role

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

20.5.3.3 Role Membership

This report displays membership details of all roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Role Name	Name of the role
Role Category	Category of the role
Organization	Name of the organization
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date

Fields

The following table lists the fields of the report:

Report Field	Description
Created By	Name of the person who created the user
Creation Date	Date on which the user is created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of user
Employee Status	Status of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Member Since	Joining date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager
Manager's User ID	ID of the manager

20.5.3.4 Organization Details

It lists the hierarchical organization structure and details about users in the organization.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Organization Name	Name of the organization

Fields

The following table lists the fields of the report:

Report Field	Description
Parent Organization Name	Name of the parent organization

Columns

The following table lists the columns of the report:

Report Column	Description
Role	Name of Administrator User roles
First Name	First name of the user in the organization

Report Column	Description
Last Name	Last name of the user in the organization
User ID	ID of the user
User Status	Status of the user
User Type	Type of user
Start Date	Joining date of the user
End Date	Leaving date of the user

20.5.3.5 User Membership History

This report lists the logged in users with their membership history.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Last Name	First name of the user
First Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Organization	Organization of the user

Report Field	Description
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor

Columns

The following table lists the columns of the report:

Report Column	Description
User Role	Name of the user role
Membership Status	Status of membership
Effective From	Date from which the membership is effective

20.5.4 Password Reports

Oracle Identity Management BI Publisher Reports provides the following password reports for Oracle Identity Manager:

- Password Expiration Summary
- Password Reset Summary
- Resource Password Expiration

20.5.4.1 Password Expiration Summary

This report shows the list of all active users whose Oracle Identity Manager passwords are about to expire within a specified period.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Last Name	Last name of the user
First Name	First name of the user
User ID	ID of the user
Organization	Organization of the user
Expiration Date Range From	Start date of the expiration date
Expiration Date Range To	End date of the expiration date

Fields

N/A

Columns

The following table lists the columns of the report:

Report Field	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Employee Status	Status of the employee: Active, Disabled, Deleted, Disabled Until Start Date
Organization	Organization of the user
Password Expiration Date	Date on which the password expires

20.5.4.2 Password Reset Summary

This report provides the ability to view the aggregated metrics around password change attempts done by users themselves or on behalf of them. The metrics include all password change attempts, successful or failure outcome of password change attempt, users locked due to multiple concurrent unsuccessful password change attempts.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Aggregation Frequency	The frequency of the report generated
Date Range From	Start date of the report generated
Date Range To	End date of the report generated
Organization	Name of the organization

Fields

The following table lists the fields of the report:

Report Field	Description
Aggregation Frequency	The frequency of the report generated

Columns

The following table lists the columns of the report:

Report Column	Description
Time Period	Date and time of reset attempts performed
Reset Attempts	Number of reset attempts
Failed Reset Attempts	Number of failed reset attempts
Locked Users due to Failed Reset Attempts	Number of users locked due to a failed reset attempt
Resets by non-beneficiary	Number of resets by non-beneficiary

20.5.4.3 Resource Password Expiration

It lists users whose resource passwords will expire in a specified time period.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
User Status	Status of the user
Password Expiration Date From	The password expiry starting date
Password Expiration Date To	The password expiry ending date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Field	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of the user: Full-Time, Part-Time, Temp, Intern, Consultant, Contractor
Password Expiration Date	Date on which the password expires

20.5.5 Resource and Entitlement Reports

Oracle Identity Management BI Publisher Reports provides the following resource and entitlement reports for Oracle Identity Manager:

- Account Activity In Resource
- Delegated Admins and Permissions by Resource
- Delegated Admins by Resource
- Entitlement Access List
- Entitlement Access List History
- Financially Significant Resource Details
- Fine Grained Entitlement Exceptions By Resource
- Offline Resource Provisioning Messages
- Orphaned Account Summary
- Resource Access List History
- Resource Access List
- Resource Account Summary
- Resource Activity Summary
- Rogue Accounts By Resource
- User Resource Access History
- User Resource Access
- User Resource Entitlement
- User Resource Entitlement History

20.5.5.1 Account Activity In Resource

It lists all account activities in each resource. It also provides information on how each user is associated with a specific activity of that resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Date Range From	Date from which reports are displayed
Date Range To	Date to which reports are displayed

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Name	Name of the resource
Activity Type	The type of activity
Resource Authorizer User Role(s)	Name of the role which authorize the role
Resource Administrator User Role(s)	Name of the role which authorize the resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
Organization	Organization of the user
Manager's User ID	ID of the manager
Timestamp	Date when the report is created

20.5.5.2 Delegated Admins and Permissions by Resource

This report displays the list of user roles with write and delete access that are administrators of the resource.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Administrator Role Name	Name of the Administrator role
Administrator Role Information	Information about the Administrator role
Read Access	Indicates whether the resource has read access
Write Access	Indicates whether the resource has write access
Delete Access	Indicates whether the resource has delete access
Authorizer Role	Authorizer role name
Name Priority	Priority of the resource
Created By	Name of the person who created the resource
Creation Date	Resource creation date

20.5.5.3 Delegated Admins by Resource

The report displays the list of user roles that are the administrators or authorizers of the resource and members of those roles.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Report Parameter	Description
Resource Type	Type of resource
Resource Audit Objective	Objective to carry out the audit for the resource

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource
Target	Indicates whether the resource is a target for organization or user
Write Access	Indicates whether the resource has write access
Delete Access	Indicates whether the resource has delete access
Creation By	Resource creation source
Creation Date	Date on which resource is created

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
Member Since	Joining date of the user
Manager's First Name	First name of the manager
Manager's Last Name	Last name of the manager
Manager's User ID	ID of the manager

20.5.5.4 Entitlement Access List

This report provides administrators or auditors the ability to query all existing users, who have a specified entitlement. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Entitlement Code	Code of the entitlement
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of user
Provisioning Date From	Date from which the resource is provisioned to the user
Provisioning Date To	Date to which the resource is provisioned to the user

Fields

The following table lists the fields of the report:

Report Field	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Entitlement status	Status of the entitlement.
Resource Name	Name of the resource
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Id	ID of the user

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User Status	User Status
User Type	Type of the user
Organization	Organization of the user
Valid To Date	Entitlement valid from date
Valid From Date	Entitlement valid to date

20.5.5.5 Entitlement Access List History

This report provides administrators or auditors the ability to query all existing users provisioned to a entitlement over its lifecycle. This is a lifetime report showing entire history of resource's access list or entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Entitlement Code	Code of the entitlement
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user: Active, Disabled, Deleted, Disabled Until Start Date
User Type	Type of user
Effective From Date	Entitlement effective from date
Effective To Date	Entitlement effective to date

Fields

The following table lists the fields of the report:

Report Field	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Resource Name	Name of the resource

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Id	ID of the user
First Name	First name of the user
Last Name	Last name of the user
User Status	Status of the user
User Type	Type of user
Effective From	Entitlement effective from date
Effective To	Entitlement effective to date

20.5.5.6 Financially Significant Resource Details

This report provides Administrators to get a list of financially significant resources to prioritize various administrative and cleanup activities. It also helps Compliance or Privacy and Security officers assessing effectiveness of preventive and detective controls in financial significant resources and Auditors to understand the IT resources that host financial data.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
User Roles	Lists the resource administrator user roles

20.5.5.7 Fine Grained Entitlement Exceptions By Resource

This report enables administrators, signing officers, internal and external auditors to analyze discrepancies in various process forms and related child tables of various resources and mitigate material weaknesses in the resources through remediation activities.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Type	Type of the employee such as fulltime, part time
Organization Name	Name of the organization
Role Name	Name of the role

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Name	Name of the resource
User ID	ID of the user

Columns

The following table lists the columns of the report:

Report Column	Description
Form Name	Name of the form
Form Type	Type of the form

> **Note:** Before running this report, you must populate data for account audit and reconciliation exceptions.

To populate the data for account audit and reconciliation exceptions:

1. Set the value of the system property, XL.EnableExceptionReports, to True.

2. Provision an user to any target.

3. Modify any of the user's attribute in the target and reconcile the user.

4. Find data in UPA_UD_FORMFIELDS and UPA_UD_FORMS tables.

5. Go to Oracle Identity Manger server and run RefreshMaterializedViewScheduler Task.

6. Log in to BIP and view the report.

20.5.5.8 Offline Resource Provisioning Messages

Offline provisioning enhancement enables Oracle Identity Manager to do offline provisioning, enable, disable and revoke on resource instances that will improve the performance by parallel execution and also overcome transaction time-outs. This is achieved by submitting the JMS message when a specific action happens, the actual execution happens as a part of message processing. Such JMS message might be failed while processing due to some reasons. This report lists all the details of such failed off-line messages.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
User's First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Resource Name	Name of the resource
Action	Action taken by the resource
Date Range From	Start date
Date Range To	End date

Fields

The following table lists the fields of the report:

Report Field	Description
User's First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Resource Name	Name of the resource
Resource Description	Description of the resource
Action	Action taken by the resource
Request Key	Key of the request
Create Date	Provisioning creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Reason	Reason of the offline resource provisioning
Exception	Exception in the offline resource provisioning

20.5.5.9 Orphaned Account Summary

It lists the rogue accounts for the input resource for which a user existed in the target system, but the associated user to whom the account is provisioned never existed in Oracle Identity Manager.

Input Parameters

The table lists the report parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Reconciliation Date Range From	Start date of reconciliation
Reconciliation Date Range To	End date of reconciliation

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
Resource	Name of the resource
Account Information	Information of the orphaned account
Reconciliation Date	Date of reconciliation

20.5.5.10 Resource Access List History

This report provides administrators or auditors the ability to query all existing users provisioned to a resource over its lifecycle. This is a lifetime report showing entire history of resource's access list or entitlements.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user

Report Parameter	Description
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Snapshot Date From	Effective start date of resource access to the user
Snapshot Date To	Effective end date of resource access to the user
Changes Date From	Resource changed from date to user
Changes Date To	Resource changed to date to user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Resource Descriptive data	Description of the resource
User Status	Status of the user
Resource Status	Status of the resource
Effective From	Effective start date
Effective To	Effective end date

20.5.5.11 Resource Access List

This report provides administrators or auditors the ability to query all existing users provisioned to a specified resource. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Provisioning Date From	Resource provision start date
Provisioning Date To	Resource provision end date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
User Type	Type of the user
User Status	Status of the user
Organization	Organization of the user
Provisioning Date	Date on which the resource is provisioned

20.5.5.12 Resource Account Summary

This report lists the number of users for each status within each resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource

Report Parameter	Description
Resource Type	Type of resource
Account Status	Status of the account

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource
Total Number of Users	Total number of users associated with the account

Columns

The following table lists the columns of the report:

Report Column	Description
Account Status	Status of the account
Number of Users	Number of users with that account status

20.5.5.13 Resource Activity Summary

It lists the history of all provisioning and approval activities for a resource.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
Date Range From	Start date
Date Range To	End date

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
Accounts Provisioned	Number of accounts provisioned
Accounts De-Provisioned	Number of accounts de-provisioned
Approval Requests	Number of approval requests
Approval Accepted	Number of approved requests
Approval Rejected	Number of rejected requests

20.5.5.14 Rogue Accounts By Resource

This report includes all rogue accounts for the input resource. This report also includes the corresponding attestation data to analyze if the rogue accounts represent outstanding or accepted exceptions in the system. This enables administrators, signing officers, internal and external auditors to identify material weaknesses in the resources and plan their mitigation through remediation activities.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
Resource Name	Name of the resource
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization Name	Organization of the user
User Status	Status of the user
User Type	Type of the user

Fields

The following table lists the fields of the report:

Report Field	Description
Resource Type	Type of resource

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user

Report Column	Description
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Exception Type	Type of exception
Exception Approved in Attestation	Indicates whether the exception is approved or not
Reviewer First Name	First name of the reviewer
Reviewer Last Name	Last name of the reviewer
Reviewer User ID	User ID of the reviewer

20.5.5.15 User Resource Access History

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.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Status	Status of the user
Employee Type	Type of employee

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager

Report Field	Description
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource
Resource Descriptive Data	Description of the resource
Provisioned Date	Date on which the resource is provisioned
Provisioned By	Name of the person who provisioned the resource
Effective From	Effective start date of resource access to the user
Effective To	Effective end date of resource access to the user

20.5.5.16 User Resource Access

This report provides administrators or auditors the ability to query all existing users provisioned to a specified resource. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Resource Name	Name of the resource
Resource Descriptive Data	Description of the resource
Resource Status	Status of the resource
Provisioned Date	Date on which the resource is provisioned

20.5.5.17 User Resource Entitlement

This report provides administrators or auditors the ability to query all existing entitlements provisioned to specific users. This report can be used for operational and compliance purposes.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user
Email	Email of the user
Resource Name	Name of the resource
Organization	Organization of the user

Report Parameter	Description
Role Name	Name of the role
User Status	Status of the user
User Type	Type of the user

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
First Name	First name of the user
Middle Name	Middle name of the user
Last Name	Last name of the user
Email	Email of the user
Organization	Organization of the user
User Status	Status of the user
User Type	Type of the user
Manager First Name	First name of the manager
Manager Last Name	Last name of the manager
Start Date	Entitlement of resource start date
End Date	Entitlement of resource end date

Columns

The following table lists the columns of the report:

Report Column	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Entitlement Status	Status of the entitlement
Resource	Type of the resource
Provisioning Start	Date from which the resource is provisioned to the user

Report Column	Description
Valid From Date	Entitlement of resource valid start date

20.5.5.18 User Resource Entitlement History

This report provides administrators or auditors the ability to view user's resource entitlement 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.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user
Email	Email of the user
Resource Name	Name of the resource
Organization	Organization of the user
Role Name	Name of the role
User Status	Status of the user
User Type	Type of the user
Effective From Date	Resource entitlement effective start date
Effective To Date	Resource entitlement effective end date

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
First Name	First name of the user
Last Name	Last name of the user
User Status	Status of the user
User Type	Type of the user
Organization	Organization of the user
Email	Email of the user
Start Date	Start date of resource entitlement

Report Field	Description
End Date	End date of resource entitlement
Identity Creation Date	Date of identity creation
Manager First Name	First name of the manager
Manager Last Name	Last name of the manager

Columns

The following table lists the columns of the report:

Report Column	Description
Entitlement Code	Code of the entitlement
Entitlement Name	Name of the entitlement
Resource	Type of the resource
Effective From Date	Resource entitlement effective start date
Effective To Date	Resource entitlement effective end date

20.5.6 User Reports

Oracle Identity Management BI Publisher Reports provides the following user reports for Oracle Identity Manager:

- User Profile History
- User Summary
- Users Deleted
- Users Disabled
- Users Unlocked

20.5.6.1 User Profile History

This report shows all the users and their details based on the input parameters.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user

Report Parameter	Description
Role Name	Role of the user
Manager User ID	ID of the Manager to whom the user reports
Employee Status	Status of the user
Employee Type	Type of employee
Changes Date Range From	Effective start date of the changes
Changes Date Range To	Effective end date of the changes
Snapshot Date Range From	Effective start date of resource access to the user
Snapshot Date Range To	Effective end date of resource access to the user

Fields

The following table lists the fields of the report:

Report Field	Description
User ID	ID of the user
User First Name	First name of the user
User Last Name	Last name of the user
Manager User ID	ID of the reporting Manager
Manager First Name	First name of the reporting Manager
Manager Last Name	Last name of the reporting Manager
Organization	Organization of the user
Employee Status	Status of employee
Employee Type	Type of employee
Identity Creation Date	User creation date

Columns

The following table lists the columns of the report:

Report Column	Description
Profile Parameter	Name of user profile
Value	Value of user profile
Date Effective From	Effective from date
Time Effective From	Effective from time

20.5.6.2 User Summary

It lists all Oracle Identity Manager users created in a specified time period. In addition, it provides information on whether the users were created manually or through trusted reconciliation.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Employee Status	Status of the user
Employee Type	Type of employee
Creation Date From	Start date of user summary
Creation Date To	End date of user summary

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Creation Date	Date at which the user is created

20.5.6.3 Users Deleted

This report shows all the deleted users and their details based on input parameters.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Deletion Date From	Start date of summary of deleted users
Deletion Date To	End date of summary of deleted users

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Deletion Date	Date at which the user is deleted

20.5.6.4 Users Disabled

This report provides the ability to view the details of users whose accounts are disabled. The account may be disabled for various reasons. For example, rejection in attestation, unsuccessful login or password reset attempts failure and so on.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee

Report Parameter	Description
Disabled Date From	Start date of user disabled
Disabled Date To	End date of user disabled

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Current status of the employee
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Disabled Date	Date at which the user is disabled

20.5.6.5 Users Unlocked

This report provides the ability to view the details of users whose disabled accounts are unlocked by administrators. Delegated administrators of the organizations to whom the user belongs may enable the accounts.

Input Parameters

The table lists the report input parameters used to specify a criterion for subsetting data:

Report Parameter	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Type	Type of employee
Unlocked Date From	Start date of user unlocked
Unlocked Date To	End date of user unlocked

Fields

N/A

Columns

The following table lists the columns of the report:

Report Column	Description
First Name	First name of the user
Last Name	Last name of the user
User ID	ID of the user
Organization	Organization of the user
Employee Status	Status of the user
Employee Type	Type of employee
Manager ID	ID of the Manager to whom the user reports
Source	User creation source
Unlocked Date	Date at which the user is unlocked

20.6 Exception Reports

In Oracle Identity Manager, **exception** refers to the difference between accounts that a user is entitled to and the accounts that are actually assigned to a user. The user is assigned these accounts as a result of access policies, provisioning of resources, approval requests, and reconciliation events. Any difference of these accounts assigned to a user in the target system and the ones assigned to the user in Oracle Identity Manager comprises an exception.

The following exception reports have been introduced in this release:

■ **Rogue Accounts By Resource**

This report returns a list of all the rogue accounts existing in a resource. The following exceptions are reported:

– An account that exists in the target system, but is not provisioned to the corresponding user in Oracle Identity Manager

– An account that exists in the target system, but has been deprovisioned for the corresponding user in Oracle Identity Manager

– An account that exists in the target system, but the corresponding user to whom the account is provisioned has been deleted in Oracle Identity Manager

The following exception is not reported in spite of being a rogue account:

– An account that exists in the target system but the corresponding user to whom the account is provisioned has never existed in Oracle Identity Manager

■ **Fine Grained Entitlement Exceptions By Resource**

This report returns a list of all the accounts in a resource for which the process form data being reconciled is different from the expected values. It means that this report returns any account existing in the target system that is also provisioned to

the corresponding user in Oracle Identity Manager, but for which the process data does not match.

> **Note:**
>
> - After completion of initial target reconciliation, all account-related activities performed directly on a target resource are tracked as exception activity. Account-related activities include account creation, account modification, and entitlement assignment/revocation. The exception reports should be used only if the organization policies enforce that all account-related activities in target resources would always be initiated in Oracle Identity Manager. In addition, remember that exception detection and recording are an extension of account data reconciliation and, therefore, may result in a drop in performance during reconciliation.
>
> - Both the exception reports depend on reconciliation data. Therefore, these reports will not display any data if the corresponding reconciliation events are archived.

20.7 Creating Reports Using Third-Party Software

Oracle Identity Manager supports the creation of reports by using third-party tools such as Crystal Reports. You can use a third-party tool to create the reports listed in Section 20.5, "Reports for Oracle Identity Manager".

> **Note:** To learn how to create reports by using third-party software, see the third-party software documentation.

Index