

**Oracle® Role Manager**

User's Guide

Release 10g (10.1.4)

**E12027-02**

November 2008

Oracle Role Manager User's Guide, Release 10g (10.1.4)

E12027-02

Copyright © 2007, 2008, Oracle. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Author: Carla Fabrizio

Contributors: Ajeet Bansal, Miles Chaston, April Escamilla, Bennett Falk, Ashish Gupta, Madhup Kumar

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface</b> .....	xi
Audience.....	xi
Documentation Accessibility .....	xi
Related Documents .....	xii
Conventions .....	xii
<b>1 Introducing Oracle Role Manager</b>	
1.1 About Oracle Role Manager .....	1-1
1.2 Features of Oracle Role Manager.....	1-3
1.3 Types of Roles in Oracle Role Manager.....	1-5
1.3.1 Business Roles .....	1-6
1.3.1.1 Dynamic Business Roles .....	1-6
1.3.1.2 Static Business Roles .....	1-7
1.3.2 IT Roles.....	1-8
1.3.3 Approver Roles .....	1-12
1.3.4 System Roles.....	1-13
<b>2 Using Oracle Role Manager</b>	
2.1 Logging In to Oracle Role Manager .....	2-1
2.2 Working with the User Interface .....	2-2
2.2.1 First-Level Navigation Options: Home .....	2-3
2.2.2 First-Level Navigation Options: Organizations & People.....	2-5
2.2.2.1 Creating Cost Centers, Locations, and Reporting Organizations .....	2-6
2.2.2.2 Creating People.....	2-9
2.2.2.3 Modifying Cost Centers, Locations, People, and Reporting Organizations .....	2-15
2.2.2.4 Deleting Cost Centers, Locations, and Reporting Organizations.....	2-16
2.2.2.5 Deleting Persons .....	2-18
2.2.3 First-Level Navigation Options: Roles .....	2-18
2.2.4 First-Level Navigation Options: Administration.....	2-20
<b>3 Working with System Roles</b>	
3.1 Predefined System Roles.....	3-1
3.1.1 System Administrator .....	3-2

3.1.2	System Role Administrator .....	3-2
3.1.3	System Role Grant Administrator .....	3-2
3.1.4	Role Administrator .....	3-3
3.1.5	Role Grant Administrator .....	3-4
3.1.6	Reporting Organization Administrator .....	3-4
3.1.7	Cost Center Administrator .....	3-5
3.1.8	Location Administrator .....	3-6
3.1.9	User Administrator .....	3-6
3.1.10	Auditor .....	3-7
3.1.11	Role Delegation Administrator .....	3-7
3.2	Creating System Roles .....	3-8
3.3	Mapping and Unmapping System Privileges .....	3-10
3.4	Granting and Revoking System Roles .....	3-12
3.5	Deleting System Roles .....	3-13

## 4 Working with IT Privileges and IT Roles

4.1	IT Privileges .....	4-1
4.1.1	Creating IT Privileges .....	4-1
4.1.2	Modifying IT Privileges .....	4-2
4.1.3	Deleting IT Privileges .....	4-2
4.2	IT Roles .....	4-3
4.2.1	Creating IT Roles .....	4-3
4.2.2	Mapping and Unmapping IT Privileges .....	4-5
4.2.3	Granting and Revoking IT Roles .....	4-6
4.2.4	Delegating IT Roles .....	4-7
4.2.5	Deleting IT Roles .....	4-8

## 5 Working with Business Roles

5.1	Static Business Roles .....	5-1
5.1.1	Creating Static Business Roles .....	5-1
5.1.2	Granting and Revoking Static Business Roles .....	5-3
5.1.3	Delegating Static Business Roles .....	5-5
5.2	Dynamic Business Roles .....	5-6
5.2.1	Creating Dynamic Business Roles .....	5-6

## 6 Working with Approver Roles

6.1	Creating Approver Roles .....	6-1
6.2	Assigning Approvers to Approver Roles .....	6-2
6.3	Deleting Approver Roles .....	6-3

## 7 Building Membership and Eligibility Rules

7.1	Attribute Expressions .....	7-1
7.2	Hierarchy Expressions .....	7-3
7.3	Relative Object Expressions .....	7-5
7.4	Role Membership Expressions .....	7-7
7.5	Logical Expressions .....	7-8

## **A About the XML Schema Definition**

A.1	Attribute Expressions .....	A-2
A.2	Hierarchy Expressions .....	A-6
A.3	Relative Object Expressions.....	A-6
A.4	Role Membership Expressions.....	A-7

## **Index**

## List of Examples

7-1	Sample XML That Uses the Attribute Expression.....	7-2
7-2	Sample XML for Attribute Expression That Uses the null-constant Element.....	7-3
7-3	Sample XML That Uses the Hierarchy Expression .....	7-3
7-4	Sample XML That Uses the Relative Object Expression .....	7-5
7-5	Sample XML That Uses the Relative Object Expression and the Attribute Expression Element 7-6	
7-6	Sample XML That Uses the Relative Object Expression to Depict the Person-Organization Combination 7-6	
7-7	Sample XML That Uses the Role Membership Expression .....	7-7
7-8	Sample XML That Uses the Logical Expression .....	7-8



## List of Figures

1-1	Organization Structure Used for a Sample Dynamic Business Role Membership .....	1-6
1-2	Static Business Role with Sphere of Control .....	1-8
1-3	Sample Mapping of IT Role to Business Role: Scenario 1 .....	1-9
1-4	Sample Mapping of IT Role to Business Role: Scenario 2 .....	1-10
1-5	Sample Mapping of IT Role to Business Role: Scenario 3 .....	1-11
1-6	Sample Mapping of System Privileges to a System Role .....	1-14
1-7	Sample Scenario Depicting a System Role Grant with SOC .....	1-15
2-1	Layout of the People Page .....	2-2
2-2	Layout of the Locations Page .....	2-3
2-3	Oracle Role Manager First-Level Navigation Bar .....	2-3
2-4	Home: Second-Level Navigation Option .....	2-4
2-5	Outbox: Transactions Page .....	2-4
2-6	Organization & People: Second-Level Navigation Options .....	2-5
2-7	Shortcut Menu That Is Displayed When You Right-Click a Location Node.....	2-7
2-8	Dialog Box for Selecting the Cost Center Type.....	2-7
2-9	Attributes Tab for a New Location .....	2-8
2-10	Members Tab for a Reporting Organization.....	2-8
2-11	History Tab for a Cost Center .....	2-9
2-12	History Dialog Box for a Cost Center .....	2-9
2-13	Shortcut Menu That Is Displayed When You Right-Click a Reporting Organization Node .. 2-10	
2-14	Attributes Tab for a New Person Record .....	2-11
2-15	Memberships Tab for a New Person.....	2-12
2-16	Relationships Tab for an Existing Person.....	2-12
2-17	Business Roles Tab for a New Person .....	2-13
2-18	IT Roles Tab for a New Person.....	2-13
2-19	System Roles Tab for an Existing Person .....	2-14
2-20	History Tab for an Existing Person .....	2-14
2-21	History Dialog Box for an Existing Person.....	2-15
2-22	Search Results Displayed on the People Page .....	2-15
2-23	Reporting Organizations Page .....	2-17
2-24	Delete Confirmation Dialog Box.....	2-17
2-25	Roles: Second-Level Navigation Options.....	2-18
2-26	Administration: Second-Level Navigation Options .....	2-20



## List of Tables

2-1	Organizations & People: Shortcut Menu Options.....	2-5
2-2	Roles: Shortcut Menu Options .....	2-19
2-3	Administration: Shortcut Menu Options.....	2-20
7-1	Comparison Operator Used in the attribute-expression Element .....	7-2
A-1	Attribute Values for object-type and attribute-id.....	A-2
A-2	Attribute Values for relationship-path-id .....	A-6



---

---

# Preface

This guide provides an overview of the features of Oracle Role Manager. It explains the procedures to create and manage roles in your organization using Oracle Role Manager. It also explains how to build rules for roles using XML.

## Audience

This guide is intended for role administrators who want to perform the following tasks:

- Define roles.
- Create roles.
- Manage roles.
- Assign privileges to roles.
- Map privileges to roles.

## Documentation Accessibility

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

<http://www.oracle.com/accessibility/>

### Accessibility of Code Examples in Documentation

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

### Accessibility of Links to External Web Sites in Documentation

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

## TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

## Related Documents

For more information, see the following documents in the Oracle Role Manager release 10.1.4 documentation set:

- *Oracle Role Manager Release Notes*
- *Oracle Role Manager Installation Guide*
- *Oracle Role Manager Administrator's Guide*
- *Oracle Role Manager Developer's Guide*
- *Oracle Role Manager Integration Guide*
- *Oracle Role Manager Java API Reference*

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.
*_HOME	This convention represents the directory where an application is installed. The directory where you install Oracle Role Manager is referred to as <i>ORM_HOME</i> .

---

---

# Introducing Oracle Role Manager

Oracle Role Manager is an enterprise role management system that provides role lifecycle management capabilities to facilitate the management of business and organizational relationships, roles, and privileges.

Role management systems and provisioning systems are components of an identity management system, along with other components. A role management system, such as Oracle Role Manager, specifies the roles a user has, and a provisioning system ensures that the user has the required access and privileges on operational systems such as Oracle E-Business Suite, PeopleSoft, and Siebel.

This chapter provides an overview of Oracle Role Manager and includes the following topics:

- [Section 1.1, "About Oracle Role Manager"](#)
- [Section 1.2, "Features of Oracle Role Manager"](#)
- [Section 1.3, "Types of Roles in Oracle Role Manager"](#)

## 1.1 About Oracle Role Manager

A **role** is a collection of privileges that are granted to one or more users. Any user who is granted a role is known as a **role member**. A **privilege** is a combination of a single permission and a single resource. A **permission** is a right that enables a role member to perform an action (such as read, or write) on a specified resource (such as an FTP directory or a network printer). For example, if Folder X is a resource and Read is a permission, then Read Folder X is a privilege.

Roles are one of the means to address security risks and adhere to compliance regulations related to identity management.

Keeping information about roles and role assignments up to date across users, organizations, locations, and reporting structures can pose many challenges. By itself, a provisioning system cannot manage and maintain complex business data for multiple hierarchies such as location and reporting hierarchies. However, a role management system such as Oracle Role Manager provides you with the ability to handle complex data across multiple hierarchies, an ability that has traditionally not been offered by provisioning systems. Oracle Role Manager also provides comprehensive reporting features across the lifecycle of enterprise roles.

Oracle Role Manager offers a flexible predefined role model that allows users from the business to manage business policies (through role membership policies) and allows IT team members to manage privilege mappings to roles to ensure users get the appropriate IT access.

A role management system can be used in conjunction with a provisioning system. This is illustrated by the following example:

Suppose an individual joins the Sales team of an organization and the administrator wants to determine the privileges to be assigned to that individual. One approach would be to identify the set of privileges assigned to existing team members and use the provisioning system to individually assign these privileges to the new member. The drawbacks of this approach are:

- If the individual's role in the company changes, then the privilege assigned to the individual must be changed manually.
- It is difficult to ensure that other individuals hired into the same position are assigned the same set of privileges. This is because the individual was assigned privileges specific to the requirements of the Sales team. There are no designation or grade-level privileges that are common across teams.
- IT team members who assign privileges to individuals may not be aware of business policies that do not allow the assignment of privileges to individuals in certain contexts.

An alternative to manually assigning privileges to individuals is to use a role management system for creating roles that abstract these privileges. The role can then be grant to all members of the Sales team. In addition, the administrator can configure rules associated with the role so that when any individual leaves the team, the role management system recalculates the individual's role membership and the provisioning system revokes the privileges that the individual had as a member of the Sales team.

As illustrated by this example, a role management system extends the capabilities of a provisioning system by enabling you to determine privileges based on role memberships.

Oracle Role Manager provides a Web-based user interface for role lifecycle management. **Role lifecycle management** is a term that describes changes to roles from creation to deletion. It involves creating, modifying, and granting or revoking roles to or from users. Role lifecycle management also includes tracking of role-related information for audit and compliance purposes. Oracle Role Manager enables you to define role membership according to business policies, map roles to users and privileges, and change the state of roles (active state or inactive state) to control access. As mentioned earlier, a role is a set of privileges and all role members get the respective privileges. When business events cause changes in organizational relationships, role memberships are dynamically recalculated to ensure that user access and privileges are in line with business policies. Oracle Role Manager provides to provisioning systems, information about privileges a user belonging to a role must obtain. This is illustrated by the following example:

Suppose there are two departments, Mortgage and Escrow. Using Oracle Role Manager a role administrator creates the roles `Mortgage Team Member` and `Escrow Team Member`. All employees belonging to the Mortgage department are automatically granted the `Mortgage Team Member` role. Similarly, all employees belonging to the Escrow department are automatically granted the `Escrow Team Member` role.

In addition, the role administrator also configures rules associated with the roles, which enables role memberships to be recalculated whenever there are changes in a relevant organizational relationship. Now, suppose Jane Doe is currently working in the Mortgage department, due to which she is automatically granted the `Mortgage Team Member` role by Oracle Role Manager. If Jane Doe is transferred to the Escrow department, then Oracle Role Manager revokes the `Mortgage Team Member` role

(by automatically recalculating her role membership) and a provisioning system, such as Oracle Identity Manager, revokes the privileges associated with the `Mortgage Team Member` role of Jane Doe and then Oracle Role Manager grants Jane Doe the `Escrow Team Member` role.

Role memberships change as business relationships and policies change. Oracle Role Manager enables provisioning systems to provide users timely access to enterprise information systems by providing accurate role membership information. This ensures that such access is compliant with business regulations and policies.

Oracle Role Manager maintains audit information about roles and role memberships to capture *who should have access to what, when, and why*. However, a provisioning, system such as Oracle Identity Manager, captures *what access a person has*.

Oracle Role Manager is a role-based access control (RBAC) system. **RBAC** is a means of controlling user access to resources in an organization through roles (or role memberships). According to RBAC standards, users are granted access or permissions to resources based on their role grants. Similarly, revoking a role will revoke access or permissions to resources.

---



---

**Note:** A user can hold more than one role. In other words, a user can be granted memberships to multiple roles.

---



---

The following points describe the RBAC approach followed by Oracle Role Manager:

- Define roles in your organization.
- Map a group of privileges to roles.
- Grant users membership to roles.

Instead of assigning individual privileges to one user at a time, which can be a cumbersome task, you define a role, map privileges to it, and add users to the defined roles.

Typically, most enterprises have multiple organizational hierarchies such as reporting organization, cost center, and location. Oracle Role Manager manages the data for these multiple hierarchies in the organization. It also manages multiple relationships between hierarchies and users in an organization. Large enterprises require users to work with cross-organizational teams and groups, and this information needs to be captured. To provide an accurate representation of organizational relationships and to maintain data integrity among hierarchies, Oracle Role Manager provides a model known as **polyarchy** that maps the intersection of multiple, overlapping hierarchies. This feature enables organizations to model complex relationship paths across business structures such as reporting organization hierarchies and locations.

Oracle Role Manager enables organizations to address compliance regulatory requirements such as the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

## 1.2 Features of Oracle Role Manager

The features of Oracle Role Manager are as follows:

- [Context-Aware, Polyarchy-Enabled Role Engine](#)
- [Authoritative Role and Privilege Repository](#)
- [Configurable and Extensible Role and Relationship Model](#)

- [Role Delegation](#)
- [Integration with Provisioning Systems](#)
- [Comprehensive Compliance Reporting](#)

### **Context-Aware, Polyarchy-Enabled Role Engine**

Oracle Role Manager features a powerful role engine that uses your business policies and the relationships between users and organizations to determine accurate, real-time role membership. This contextually aware, polyarchy-enabled role engine resolves complex relationships across business organizations to ensure that access and privileges are aligned with corporate strategy.

For example, you can specify a cost center manager as a person who is in a Manager role within a cost center hierarchy in your organization. Similarly, you can specify a Europe-based account executive as a person who has a job code or team membership in the sales branch of the reporting hierarchy and who works from the European branch of the location hierarchy.

### **Authoritative Role and Privilege Repository**

Oracle Role Manager aggregates contextual business information, such as organizational relationships, to define role membership. These roles form a comprehensive role repository. Serving as the central source of information for roles, this role repository supplies authoritative privilege-related data to enterprise systems.

### **Configurable and Extensible Role and Relationship Model**

Businesses can have their own, custom-designed organization structures, relationships, and operational models. Oracle Role Manager makes it easy to model unique business structures and relationships by providing a customizable user interface, schema, business login, and so on.

As mentioned in one of the preceding sections, Oracle Role Manager has the reporting organization, cost center and location hierarchies that are predefined in the standard model of Oracle Role Manager. The **standard model** consists of objects that are required for the Web application of Oracle Role Manager to function as designed. In addition, you can load the **sample data** that contains sample roles and role definitions, persons, and organizations. See *Oracle Role Manager Installation Guide* for information about loading sample data.

You can customize the standard model by adding custom attributes and entities depending on the requirements of your business model. You can then add custom business logic to work with your custom objects. See *Oracle Role Manager Developer's Guide* for more information about customizing the standard data model.

### **Role Delegation**

Some business scenarios may require users to delegate access and privileges to other users to distribute role administration across users in an enterprise. By providing features for delegation of role administration, Oracle Role Manager enables users to easily delegate access and privileges without violating business policy. Delegated administration provides business users the ability to manage access and privileges, a function normally performed by IT departments.

For example, a Senior Project Manager who is a business user may choose to delegate role administration of his team to a Project Manager. This enables the Project Manager to manage the access rights and privileges of all team members on behalf of the Senior Project Manager.



### Integration with Provisioning Systems

Oracle Role Manager provides an Oracle Role Manager Integration Library (Integration Library) that integrates Oracle Role Manager with provisioning systems such as Oracle Identity Manager. This integration can be used to initiate provisioning events in response to changes in role membership, and business role and IT role mappings.

After integration, whenever a user is created or deleted in Oracle Identity Manager, a corresponding person is created in or deleted from Oracle Role Manager. Similarly whenever a role is created or a role membership is changed in Oracle Role Manager, a corresponding user group is created or the user group membership is changed in Oracle Identity Manager.

Integrating Oracle Role Manager with a provisioning system such as Oracle Identity Manager ensures the following:

- Provisioning events occur when role memberships change.
- Provisioning events occur when business role and IT role mappings change.
- Business events, such as a new hire or transfer, cause role membership to change, which in turn initiates provisioning events.

See *Oracle Role Manager Integration Guide* for more information about the Integration Library.

### Comprehensive Compliance Reporting

Oracle Role Manager captures audit data related to role configuration and role memberships. This data can be manually exported to an audit platform such as Oracle GRC Manager and can be used as evidence of compliance.

## 1.3 Types of Roles in Oracle Role Manager

By default, every role in Oracle Role Manager is attached to a reporting organization. This means that every role must belong to a reporting organization. The reporting organization to which a role belongs does not limit the scope of role resolution. Oracle Role Manager enables you to set a reporting organization to which the role belongs. This reporting organization states the organization which will be responsible for administering the role definition and role membership.

In other words, setting an organization for a role only states who should administer the role, but does not affect who can be granted this role.

Any role in Oracle Role Manager can be in one of the following statuses:

- Inactive
 

If a role is inactive, then the Integration Library does not send role membership information to a provisioning system, such as Oracle Identity Manager. You can create and modify role definitions and role memberships without initiating any provisioning events.
- Active
 

If a role is active, then the Integration Library sends information about creation and modification of role definitions and role memberships to a provisioning system such as Oracle Identity Manager.

Oracle Role Manager supports the following types of roles:

- [Section 1.3.1, "Business Roles"](#)

- [Section 1.3.2, "IT Roles"](#)
- [Section 1.3.3, "Approver Roles"](#)
- [Section 1.3.4, "System Roles"](#)

## 1.3.1 Business Roles

A **business role** is a named collection of business duties or responsibilities that can be granted to users. A business role can be either of a static role type or a dynamic role type. After the role type of a role is defined, the role type cannot be altered.

Business roles are created and managed by business users, such as managers and team leaders. For example, a Regional Manager in the Sales organizational unit can create the `Account Executive` business role to be granted to employees whose responsibility is to manage new accounts.

Role memberships constantly change in an organization. These changes occur when an employee joins the organization, receives promotion, joins new projects, joins another team, receives a transfer, and so on. With a large number of users and roles, it may be difficult to ensure that users have the right roles at the right time to fulfill their work responsibilities. To address this challenge, Oracle Role Manager provides a feature called dynamic business roles.

The following business roles are discussed in this section:

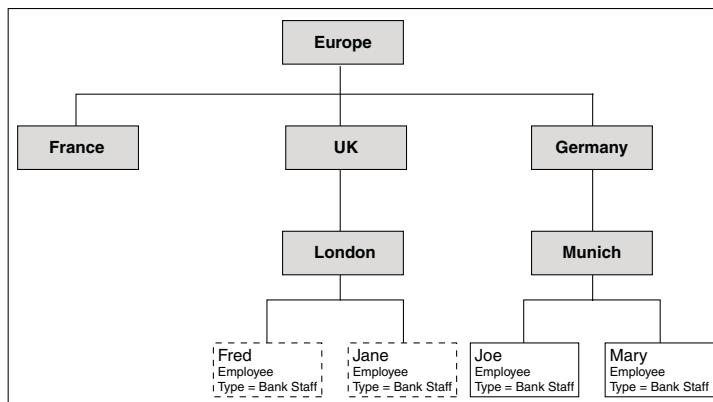
- [Dynamic Business Roles](#)
- [Static Business Roles](#)

### 1.3.1.1 Dynamic Business Roles

Dynamic business roles depend on rules (membership rules) to determine role memberships. **Membership rules** define who must be granted a particular role under what circumstances. For example, a business user can create a membership rule to grant the `Senior Accountant` business role to all users in the Accounting reporting hierarchy whose job title is Manager. All users in the Accounting reporting organization who meet the condition described by this membership rule are automatically added to the membership list of the Senior Accountant role. A **membership list** for a role is a set of all users who have been granted that particular role.

[Figure 1–1](#) illustrates another example of a dynamic business role.

**Figure 1–1 Organization Structure Used for a Sample Dynamic Business Role Membership**



Consider the `Bank_Teller_UK` dynamic business role. This role uses the membership rule that states that all users whose office location is within the UK office hierarchy and employee type is Bank Staff will automatically be granted the `Bank_Teller_UK` role.

As shown in [Figure 1–1](#), Fred and Jane are granted this role because they meet the criterion specified in the preceding paragraph. However, Joe and Mary, whose employee type is Bank Staff, are not granted this role because they do not belong to the UK office hierarchy. In addition, if Jane's employee type changes to IT Staff, then the `Bank_Teller_UK` role is automatically revoked because she no longer satisfies the membership rule criterion.

As illustrated by this example, dynamic business roles help maintain role membership accuracy because memberships to these roles are automatically determined in response to business events, such as promotion or change in office location. In addition, if the membership rule of a dynamic business role is modified, then the membership list of this role will be recalculated using the modified membership rule.

### 1.3.1.2 Static Business Roles

Static business roles determine role membership through manual role grants. Unlike dynamic business roles, which use membership rules, static business roles must be granted manually to one user at a time. They do not depend on rules that define who must be granted a particular role.

For example, consider the static business role `Accounting Clerk`. If John, an Accounting Manager decides to grant this role to his team member David, then John must manually grant this role to David. Similarly, when David moves to a different team or a role, John must manually revoke this role from David.

A static business role may also be associated with an eligibility rule. An **eligibility rule** enables you to filter the list of users to whom you want to manually grant roles. In other words, an eligibility rule shortlists all the users who are eligible to be granted a static business role. For example, consider the `Payroll Analyst` static business role with the `View and Edit Payroll` privilege, which is a special privilege. To closely monitor access to this privilege, you can choose to grant this role manually. In addition, you can create an eligibility rule that states that the `Payroll Analyst` static business role can only be granted to users who belong to the payroll team. When someone tries to grant the `Payroll Analyst` static business role to a person who does not belong to the payroll team, the grant fails. In other words, the eligibility rule does not allow this role to be granted to users who are not members of the payroll team.

---

---

**Note:** An eligibility rule will prevent a role grant whenever the person being granted the role does not meet the requirements of the rule. Also note that eligibility rules do not automate role memberships.

---

---

An eligibility rule is enforced only at the time of grant. For example, suppose Max has been granted the `Project_Manager_Europe` static business role. This role is associated with the `MS_Access_UK` privilege, which translates into an account on the Microsoft Access installation in Manchester, UK. The eligibility rule associated with this privilege is that the individual to whom the privilege is assigned must be a manager in any of the European offices of the organization. Now, suppose Max is transferred to the San Francisco office. The `Project_Manager_Europe` role is not automatically revoked from Max in response to this business event. In other words,

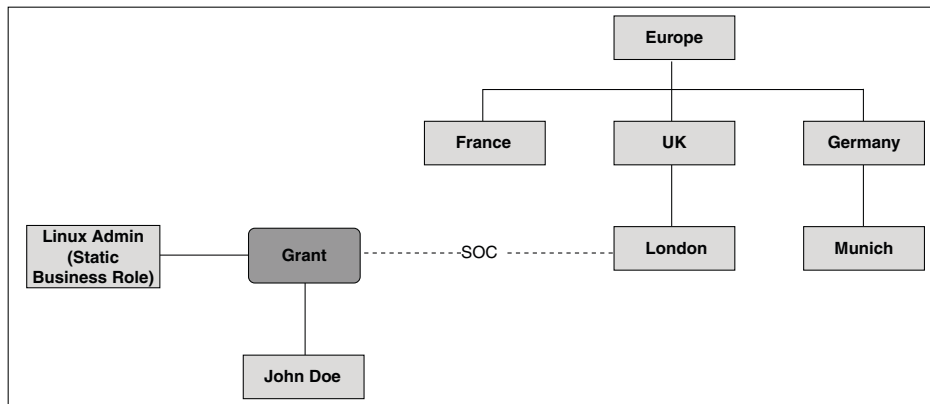
Max's eligibility to be granted the `Project_Manager_Europe` role is checked only before he is granted the role, and not at any other time.

You can create static business roles with a **sphere of control (SOC)**, which is a relationship between a grant and a node within a hierarchy such as reporting, cost center, and location. In other words, SOC specifies the organizational scope (hierarchy or a node within a hierarchy) within which a grantee can exercise a role. A **grantee** is a person to whom a role has been granted.

SOC is a means of limiting the validity of a grant within a hierarchy.

Figure 1–2 illustrates a location hierarchy along with the `Linux Admin` static business role that is granted to John Doe.

**Figure 1–2 Static Business Role with Sphere of Control**



The `Linux Admin` static business role is granted to John with the SOC set to the London office (which is a node) in the Location hierarchy. This means that John has this role only when he is in the London office. This role is not valid if John moves to the Munich office.

Static business roles enable you to handle special and high-value privileges and ensure that the system does not automatically grant access to such privileges.

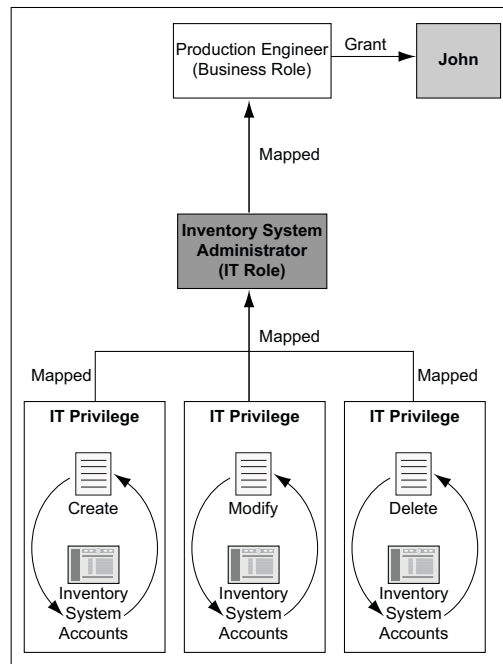
You can choose to grant static business roles if you are in a situation where no appropriate rule has been (or can be) defined, yet there is a need for grouping users according to a single business context.

## 1.3.2 IT Roles

An **IT role** is a named collection of IT privileges that can be granted to users. Any privilege for an external application that associates itself with an IT resource is known as an **IT privilege**. For example, if a router is an IT resource and `Configure` is a permission, then `Configure Router` is an IT privilege.

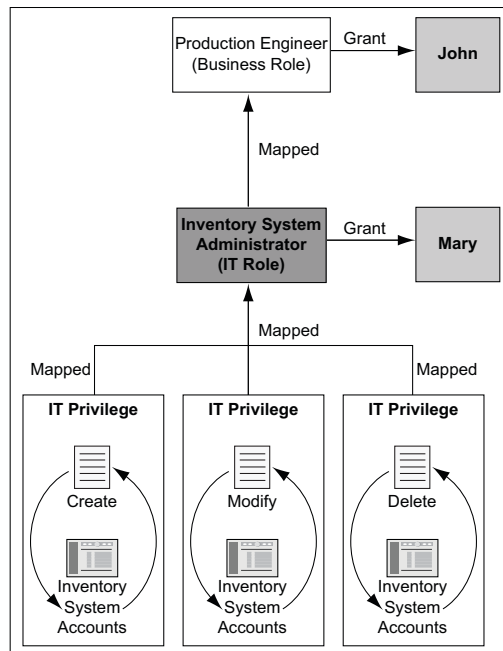
You can map IT roles to business roles in order to grant users a set of privileges.

Figure 1–3 illustrates an example of an IT role mapped to a business role.

**Figure 1-3 Sample Mapping of IT Role to Business Role: Scenario 1**

As illustrated in [Figure 1-3](#), the Inventory System Administrator IT role is a collection of IT privileges: Create Inventory System Accounts, Modify Inventory System Accounts, and Delete Inventory System Accounts. This IT role is mapped to the business role Production Engineer, which is granted to John. Because John is a member of the business role Production Engineer, he is also automatically a member of the related Inventory System Administrator IT role. Therefore, John gets all the privileges that are mapped to the Inventory System Administrator IT role.

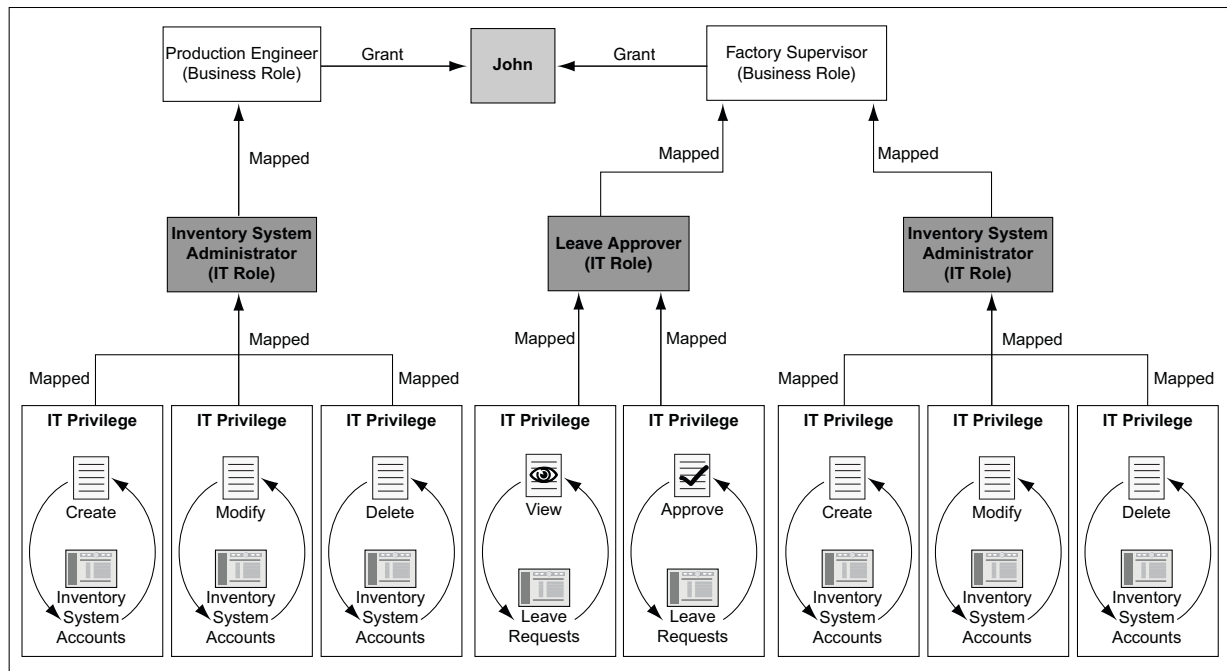
In addition to mapping IT roles to a business role for granting users a set of IT privileges, you can directly grant an IT role to a user. [Figure 1-4](#) extends the scenario described in [Figure 1-3](#).

**Figure 1–4 Sample Mapping of IT Role to Business Role: Scenario 2**

As illustrated in [Figure 1–4](#), John is granted the Production Engineer business role. This business role has the Inventory System Administrator IT role, which is a collection of the Create Inventory System Accounts, Modify Inventory System Accounts, and Delete Inventory System Accounts IT privileges. This implies that John automatically has membership to the Inventory System Administrator IT role. Therefore, John gets all the privileges that are mapped to the Inventory System Administrator IT role.

Mary, who is another user, also has membership to the Inventory System Administrator IT role though she is not a member of the Production Engineer business role. This is because Mary is directly granted the Inventory System Administrator IT role.

If a user is no longer a member of a particular business role, then that user will automatically lose membership to related IT roles. However, it is possible that a user may have two business roles, both of which are mapped to the same IT role. In such a scenario, the user will not lose membership of the IT role unless the user loses membership of both business roles. [Figure 1–5](#) illustrates this scenario.

**Figure 1–5 Sample Mapping of IT Role to Business Role: Scenario 3**

As shown in [Figure 1–5](#), John has been granted another business role, *Factory Supervisor*, which is mapped to the *Leave Approver* and *Inventory System Administrator* IT roles as illustrated in [Figure 1–5](#). The *Leave Approver* IT role has the *View Leave Requests* and *Approve Leave Requests* IT privileges on the HR system. The *Inventory System Administrator* IT role has the *Create Inventory System Accounts*, *Modify Inventory System Accounts*, and *Delete Inventory System Accounts* IT privileges. Therefore, mapping of the *Leave Approver* and *Inventory System Administrator* IT roles to the *Factory Supervisor* business role results in the IT privileges of all IT roles (mapped to the business role) being applied to John, who is a member of the *Factory Supervisor* business role.

Now, suppose John loses the *Production Engineer* business role. However, John does not automatically lose the related *Inventory System Administrator* IT role. This is because John is granted the *Factory Supervisor* business role that has the *Inventory System Administrator* IT role as one of its IT roles. John will not lose the membership to the *Inventory System Administrator* IT role unless he loses memberships to both the business roles granted to him.

Typically, IT roles are managed by IT teams. It is recommended that IT team members provide descriptive data about the IT role because the IT privilege names (from external systems) may be cryptic. This may give no indication to the business user about the kind of access being granted to a user.

Providing descriptive information about an IT role enables business users to decide if the IT role should be mapped to a business role. For example, an IT team member can enter the following description for the *Inventory System Administrator* IT Role:

This role will give users the ability to create, edit, and modify inventory system accounts.

Therefore, IT roles can be understood at a high level by business users also.

IT roles often group all privileges from a single resource. For example, consider the IT role `Outlook E-mail Access`, which contains privileges such as `Create E-mail`, `Send E-mail`, `Delete E-mail`, and `Create Calendar Entry`. These privileges belong to a single resource, which is the Outlook e-mail server.

---

**Note:** Although it is possible to group privileges from multiple resources into a single IT role, Oracle recommends grouping privileges only from a single resource in an IT role. This is because it is easier to manage an IT role containing privileges from a single resource.

---

You can map an IT role to one or more business roles. For example, the `E-mail Access` IT role can be mapped to business roles such as `Sales Manager`, `Accounts Manager`, and `HR Manager`. However, it is recommended to directly grant an IT role to a user than to grant a business role with a single IT role.

### 1.3.3 Approver Roles

An **approver** is a person who is responsible for authorizing a workflow request or even a single step within a multiple-step workflow request, in a system other than Oracle Role Manager. An approver role is a collection of approvers. In other words, an approver role is a container that holds approvers.

Approver roles are dynamic in nature. Therefore, they use membership rules similar to dynamic business roles.

For example, you can create a membership rule to determine the person who approves the CRM application access request for a person John Doe. When you run this rule, John Doe (the subject of the rule) is found along with the person who has a Manager relationship with John Doe.

Identifying the approvers for workflow routing (which is done by an external application) is complex because it requires more organizational data than a provisioning system can typically store and manage. Approver roles are a unique concept of Oracle Role Manager, to leverage the polyarchy data for use with external workflow systems.

Provisioning and access management products include the names of the approvers in their approval workflow itself. This way, you need multiple workflows for the same privilege because you must include different approvers for different organizational units and functional groups within the approval workflow. Because approvers are directly included in workflows, the workflows lack business context and become out of date whenever an approver leaves or the approval rule changes.

Oracle Role Manager enables you to define membership rules and to determine approvers by navigating various organizational and relationship hierarchies.

### 1.3.4 System Roles

A **system role** is a named collection of system privileges related to your current installation of Oracle Role Manager. A **system privilege** is a combination of a single object and one or more system permissions. A **system permission** is a right that enables access to an object (or a system resource). For example, if a business role is an object and `Manage` is a permission, then `Manage Business Role objects` is a system privilege.



System privileges are created during Oracle Role Manager installation. You cannot add, modify, or delete system privileges. System privileges are mapped to system roles to represent that the members of that system role have system permissions with respect to objects or the system resource (in this case, Oracle Role Manager).

A system role defines the kind of access to Oracle Role Manager a user has. A system role also determines if you have the privileges required to modify other system roles.

System roles are containers for system privileges. Objects (such as Business Role objects, IT privilege objects, Country objects, and Person objects) can have `Audit`, `Delegate`, `Grant`, and `Manage` as system permissions. For example, the `Role Administrator` system role can have the `Manage Approver Role` objects, `All for IT Role` objects, and `Delegate Business Role` objects system privileges.

---

**Note:** By default, every user in Oracle Role Manager has read permission on all objects.

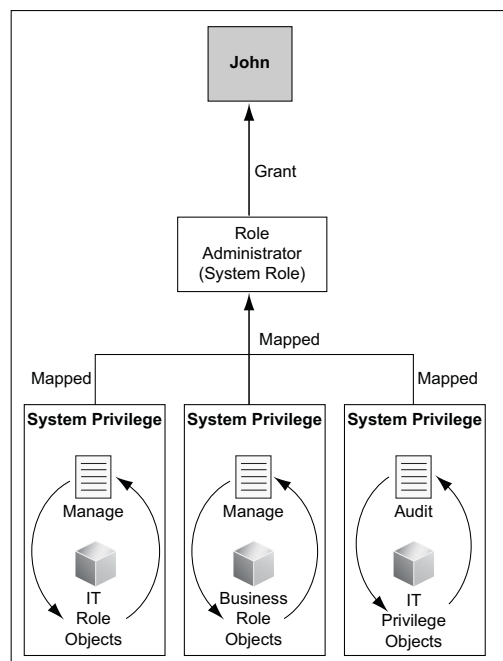
---

System roles are static in nature. System roles can be granted to persons or system identities. **System Identities** are system user objects that are created in order to access the Oracle Role Manager system. System Identities normally represent external systems, such as a user provisioning system that accesses Oracle Role Manager for role resolution, workflows, or access provisioning.

You must individually grant system roles to users of Oracle Role Manager or system identities. For example, you can define users who must have `delegate` access for certain objects in the Oracle Role Manager user interface, and `grant` access for some other objects of the user interface. System roles are the means for enforcing internal security for Oracle Role Manager.

Figure 1–6 illustrates an example of system privileges mapped to a system role that is granted to a user John.

**Figure 1–6 Sample Mapping of System Privileges to a System Role**

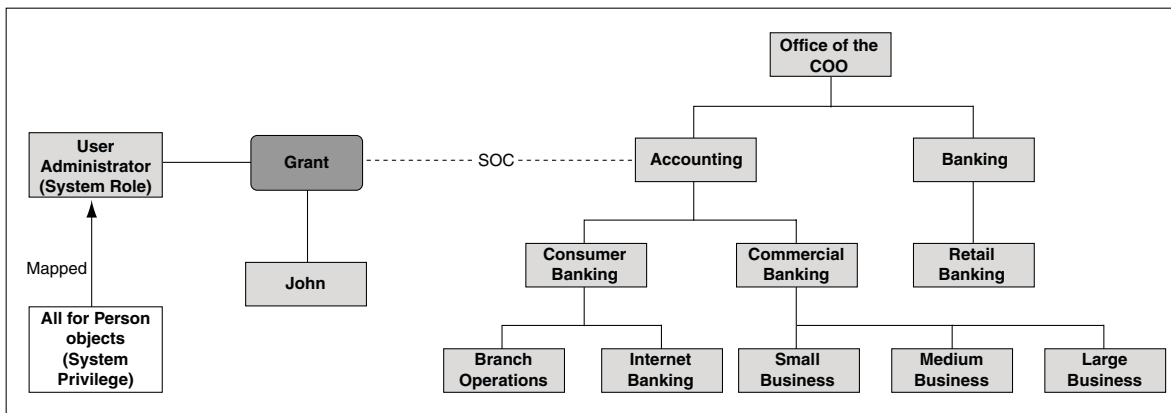


As illustrated in [Figure 1-6](#), the `Role Administrator` system role is a collection of the `Manage IT Role` objects, `Manage Business Role` objects, and `Audit IT Privilege` objects system privileges. The `Role Administrator` system role is granted to John. Therefore, with the `manage` system permission for IT role and business role objects, John can create, update, and delete IT roles and business roles. With the `Audit IT Privilege` objects system role, John can read all information related to IT privileges.

System roles support the concept of sphere of control (similar to static business roles) by defining the hierarchy within which the role is valid. You can grant system roles to Oracle Role Manager users with SOC.

[Figure 1-7](#) illustrates an example of a system role granted to John with SOC.

**Figure 1-7 Sample Scenario Depicting a System Role Grant with SOC**



Suppose John belongs to the Accounting reporting organization. As illustrated in [Figure 1-7](#), John is granted the `User Administrator` system role with an SOC set on the Accounting reporting organization. The `All for Person` objects system privilege is mapped to the `User Administrator` system role. This means that, John can create, update, and delete person records that belong to the Accounting reporting organization and all its child organizations.

Now, suppose John is moved from the Accounting reporting organization to the Office of the COO organization. John will still be able to create, update, and delete person records that belong to the Accounting reporting organization and all its child organizations such as the Consumer Banking, Commercial Banking and Branch Operation reporting organizations. This is because, John has been granted the `User Administration` system role with SOC set on the Accounting reporting organization. The organization to which a person belongs is orthogonal to the organizations over which the person is granted SOC.

System privileges and the System Administrator system role are defined during Oracle Role Manager installation. In addition, system roles can be created, modified, or deleted according to your requirements. See "[Predefined System Roles](#)" on page 3-1 for information about predefined system roles that are available in addition to the system roles that are available as part of the sample data.

---

---

## Using Oracle Role Manager

This chapter discusses the procedure to access Oracle Role Manager and will help you to familiarize yourself with the Oracle Role Manager application. This will enable you to quickly start using Oracle Role Manager. This chapter discusses the following topics:

---

---

**Note:** The topics discussed in this section assume that you have installed Oracle Role Manager and loaded the sample data.

---

---

- [Section 2.1, "Logging In to Oracle Role Manager"](#)
- [Section 2.2, "Working with the User Interface"](#)

### 2.1 Logging In to Oracle Role Manager

To log in to Oracle Role Manager:

1. Browse to the following URL by using a Web browser:

```
http://hostname:port/webui
```

In this URL, *hostname* represents the name of the computer hosting the application server and *port* refers to the port on which the server is listening. The default port number for JBoss Application Server is 8080.

---

---

**Note:** The application name, *webui*, is case-sensitive.

---

---

For example:

```
http://localhost:8080/webui/
```

2. After the Oracle Role Manager login page is displayed, log in with your user name and password.

---

---

**Note:** While logging in to Oracle Role Manager, if you enter *n* number of incorrect passwords, then your account will be locked. Here, *n* is the **account lockout threshold** or the number of attempts to log in before the account is locked. Account lockout threshold is set by the system administrator. By default, the value of *n* is set to 5.

---

---

## 2.2 Working with the User Interface

Each page in the Oracle Role Manager user interface is divided into two panes. The left pane consists of a navigation tree that enables you to navigate through various nodes. The right pane consists of a Search For field, using which you can search for one or more records in Oracle Role Manager.

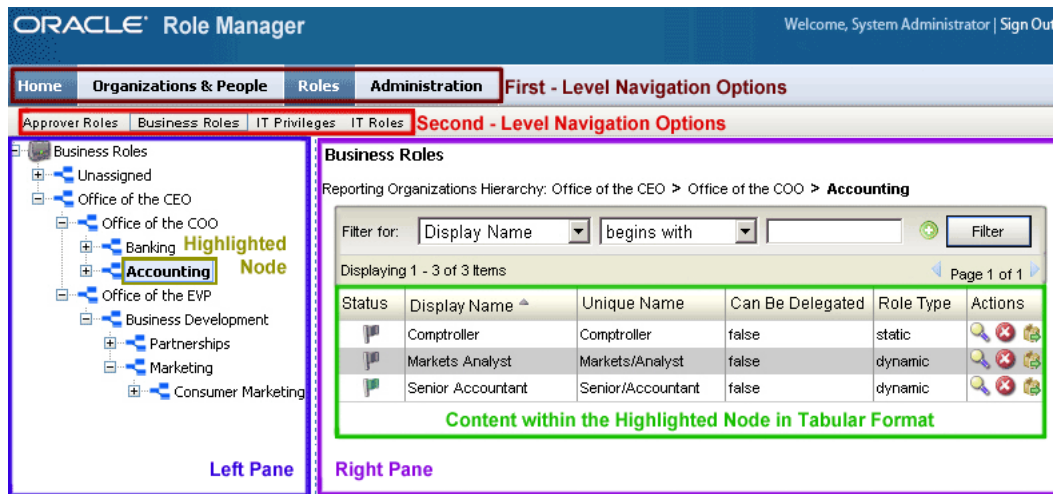
---

**Note:** You can use the percent sign (%) as the wildcard character to perform search operations.

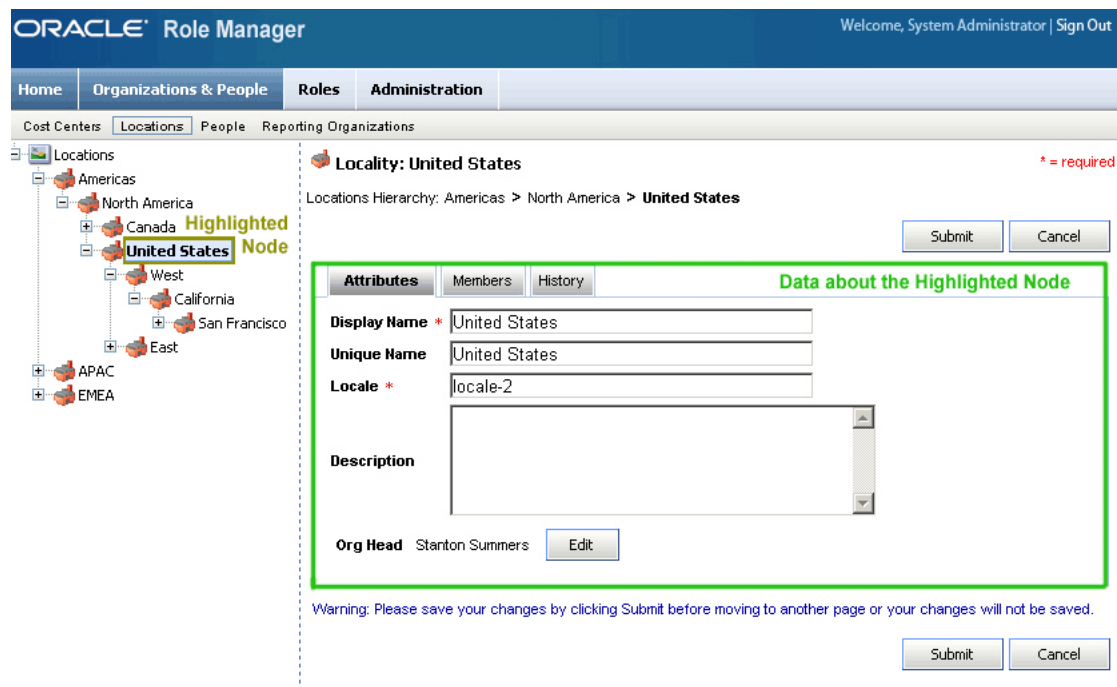
---

Depending on the navigation options that you select, the contents displayed on the left and right panes vary. [Figure 2–1](#) shows a sample page, and the layout of most pages in Oracle Role Manager is similar to the user interface layout on this page.

**Figure 2–1** Layout of the People Page



There are some pages in the Oracle Role Manager user interface that have a layout different than the one shown in [Figure 2–1](#). [Figure 2–2](#) shows one such page.

**Figure 2–2** Layout of the Locations Page

The Oracle Role Manager user interface contains the first-level navigation bar that consists of the following options:

- [First-Level Navigation Options: Home](#)
- [First-Level Navigation Options: Organizations & People](#)
- [First-Level Navigation Options: Roles](#)
- [First-Level Navigation Options: Administration](#)

Figure 2–3 shows the first-level navigation bar in Oracle Role Manager.

**Figure 2–3** Oracle Role Manager First-Level Navigation Bar

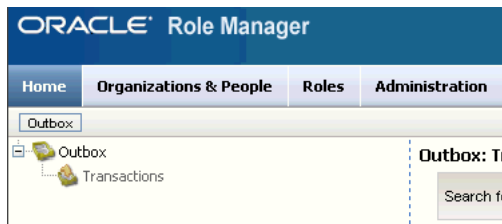
## 2.2.1 First-Level Navigation Options: Home

Home is the first option on the first-level navigation bar. It contains Outbox, which is a second-level navigation option. On the left pane, the Outbox node consists of the Transactions child node.

You can use the Outbox node to search for and view details of all transactions performed using the interface.

Figure 2–4 shows the Outbox node by using which you search for transactions. You must right-click the Transactions node to search for transactions.

**Figure 2–4 Home: Second-Level Navigation Option**



A **transaction** in Oracle Role Manager, is a sequence of actions (performed in the UI) that can be updated and stored multiple times before it can be submitted to the database. For example, the sequence of steps performed to create a role is a transaction. Another example is, updating and submitting a role.

A transaction can be in any one of the following statuses:

- Pending
- Finalized
- Canceled

The status of a transaction is pending if the transaction is not complete. For example, if you perform a sequence of actions to update the details of an IT role but do not submit the details, then the Update IT Role transaction is said to be in the pending status.

Figure 2–5 shows the status of the Update IT Role transaction.

The status of a transaction is finalized if the transaction is complete and the changes are submitted to the database. For example, if you perform a sequence of actions to enter the details to create a business role and then submit the details, then the Create Business Role transaction is said to be in the finalized status. Figure 2–5 shows the status of the Create Business Role transaction.

The status of a transaction is canceled if the transaction is not complete and the sequence of actions performed are canceled. For example, if you perform a sequence of actions to update the details of a person and then cancel the details, then the Update Person transaction is said to be in the canceled status. Figure 2–5 shows the status of the Update Person transaction.

**Figure 2–5 Outbox: Transactions Page**

**Outbox: Transactions**

Search for:

Displaying 1 - 15 of 387 Items Page 1 of 26

Status	Transaction	Submission Date	Actions
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	
finalized	Create Role to Privilege Mapping	21 October 2008 6:52 PM IST	

## 2.2.2 First-Level Navigation Options: Organizations & People

You can create, update, delete, and search cost centers, location, people, and reporting organizations by using the second-level navigation options available under Organizations & People, as shown in [Figure 2–6](#).

**Figure 2–6 Organization & People: Second-Level Navigation Options**



The first-level navigation option Organizations & People contains the following second-level navigation options:

- Cost Centers
- Locations
- People
- Reporting Organizations

---

**Note:** In this document, entities created under each of the hierarchies (such as Cost Centers, Locations, and Reporting Organizations) are called **nodes**.

For example, Operations is a node under the Cost Centers hierarchy.

---

Right-clicking a node on the left pane of the Organizations & People page will display the menu options listed in [Table 2–1](#). You can perform the actions listed in this table depending on the privileges you have been granted. For example, the New option is grayed out if you do not have the appropriate system privilege to create a reporting organization.

**Table 2–1 Organizations & People: Shortcut Menu Options**

Menu Item	Action
View Details	Displays details of the node.
New	Creates a node.
Search	Searches for nodes within the current node and all its child nodes.
Move	Moves the node to another location within the node-navigation tree. <b>Note:</b> This option is not available in the People view.
Collapse	Changes the display of the current node to show only the parent node and hide all child nodes.
Expand	Changes the display of the current node to show all its child nodes.
Refresh	Refreshes the view of the node.
Delete	Deletes the node. If the node has child nodes, then this option is grayed out. <b>Note:</b> This option is not available in the People view.

You can create, modify, and delete cost centers, locations, people, and reporting organizations. To perform these procedures, you must be a member of a system role that contains the All or Manage privileges for each of the objects. See "[Working with System Roles](#)" on page 3-1 for more information about system roles.

For example, if you want to create person records, then you must be a member of a system role that contains one of the following system privileges:

- All for Person objects
- Manage Person objects

Similarly, if you want to modify a reporting organization of the type country, then you must be a member of a system role that contains one of the following system privileges:

- All for Country objects
- Manage Country objects

This section discusses the following procedures:

- [Creating Cost Centers, Locations, and Reporting Organizations](#)
- [Creating People](#)
- [Modifying Cost Centers, Locations, People, and Reporting Organizations](#)
- [Deleting Cost Centers, Locations, and Reporting Organizations](#)
- [Deleting Persons](#)

### 2.2.2.1 Creating Cost Centers, Locations, and Reporting Organizations

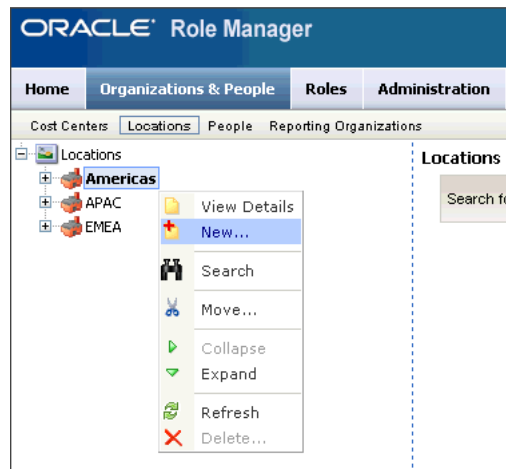
To create a cost center, location, or reporting organization:

1. On the first-level navigation bar, click **Organizations & People**.
2. Depending on the node that you want to create, on the second-level navigation bar, select one of the following:
  - Cost Centers
  - Locations
  - Reporting Organizations
3. On the left pane, right-click the node within which you want to create a node and then click **New**.

For example, if you want to create the `South America` location, then you right-click the `Americas` location.

[Figure 2-7](#) shows the menu that is displayed when you right-click the `Americas` location.



**Figure 2–7** Shortcut Menu That Is Displayed When You Right-Click a Location Node

4. In the dialog box that appears, select the type of node that you want to create and then click **Submit**.

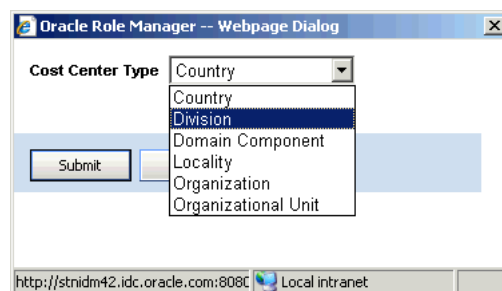
---

**Note:** The list in the dialog box displays only list items for which you have the Manage or All system privilege. For example, if you have the Manage system privilege for the Country and Locality objects, then you can view only the nodes of type Country and Locality in the list displaying node types.

---

For example, in the Cost Center Type box, select Division and then click **Submit**.

Figure 2–8 shows the dialog box containing the Cost center Type box.

**Figure 2–8** Dialog Box for Selecting the Cost Center Type

5. On the Attributes tab of the New page, enter appropriate values in the fields.

---

**Note:** You can successfully create two or more nodes with the same display name because there are no uniqueness constraints on the **Display Name** field. Enter a value in the **Unique Name** field to uniquely identify a node in Oracle Role Manager.

---

Figure 2–9 shows the Attributes tab on which sample values have been specified for creating a location of the type country.

**Figure 2–9 Attributes Tab for a New Location**

**New: Country**  
 Locations Hierarchy: EMEA > Europe

Attributes Members

Display Name \* France

Unique Name France

Description

Country Code FR

Org Head Lamont Teague

- You cannot perform any action on the Members tab while creating a node. However, while you modify a node, the Members tab displays a list of all persons who are members of the node.

Figure 2–10 shows the list of all persons who belong to the Consumer Marketing reporting organization.

**Figure 2–10 Members Tab for a Reporting Organization**

Organization: Consumer Marketing \* = required

Reporting Organizations Hierarchy: Office of the CEO > Office of the EVP > Business Development > Marketing > Consumer Marketing

Attributes **Members** History

Filter for: First Name begins with

Displaying 1 - 7 of 7 Items Page 1 of 1

Status	First Name	Last Name	Display Name	Unique Name	Email	Actions
	Barney	Heffner	Barney Heffner	Heffner/Barney-53	Heffner.Barney@samplebank.orn	
	Christa	Picard	Christa Picard	Picard/Christa-49	Picard.Christa@samplebank.orn	
	Elden	Grimes	Elden Grimes	Grimes/Elden-52	Grimes.Elden@samplebank.orn	
	Jack	Parra	Jack Parra	Parra/Jack-50	Parra.Jack@samplebank.orn	
	Ken	Christianson	Ken Christianson	Christianson/Ken-51	Christianson.Ken@samplebank.orn	
	Luvenia	Acker	Luvenia Acker	Acker/Luvenia-48	Acker.Luvenia@samplebank.orn	
	Sheree	Polk	Sheree Polk	Polk/Sheree-54	Polk.Sheree@samplebank.orn	

Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

- You cannot perform any action on the History tab while creating a node. However, while you modify a node, the History tab displays a list of events for the corresponding node.

For example, if you update the telephone number of the Risk Management cost center, then this event is stored and displayed on the History tab. Figure 2–11 shows the History tab for the Risk Management cost center.

**Figure 2–11 History Tab for a Cost Center**

**Organization: Risk Management** \* = required

Cost Center Hierarchy: Operations > Banking > Investment Banking > **Risk Management**

Submit Cancel

Attributes Members **History**

Displaying 1 - 3 of 3 items Page 1 of 1

Transaction Time	Transaction ID	User	Reason	View
21 October 2008 7:23 PM IST	919	System Administrator	Organization 'Risk Management' was updated.	
21 October 2008 6:51 PM IST	638	System Administrator	Assigned Cone/Leonardo-23 as the head of organization named org29	
21 October 2008 6:49 PM IST	41	System Administrator	Organization was created.	

Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

Submit Cancel

In addition, by clicking the View icon in the row for an event, you can view details of the event such as the time at which the event occurred, the name of the attribute that has been modified, its original value, and its new value.

Figure 2–12 shows a dialog box that displays details of an event.

**Figure 2–12 History Dialog Box for a Cost Center**

Oracle Role Manager -- Webpage Dialog

History Details

**Operation: Update Organization**

**Object Changed:** organization : Risk Management

**User :** System Administrator

**Event Timestamp :** 19 September 2008 3:50 PM IST

Attribute Changed	Original Value	New Value
Telephone Number	(510) 555-4511	(510) 555-4512

OK

http://stnidm42.idc.oracle.com:8080/webui/pages/components/history\_info.jsf Local intranet

## 8. Click Submit.

A message indicating that the node was created successfully is displayed.

### 2.2.2.2 Creating People

---

**Note:** Do not perform the procedure described in this section, if the Integration Library is installed. Creating people must be performed in provisioning systems.

A provisioning system, such as Oracle Identity Manager, is the authoritative source for people data, and this data is imported into Oracle Role Manager by using the Integration Library.

---

#### To create a person:

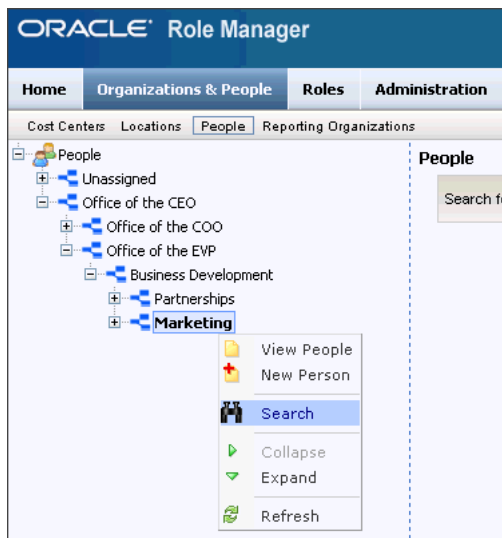
1. On the first-level navigation bar, click **Organizations & People**.
2. On the second-level navigation bar, click **People**.

- On the left pane, right-click the node within which you want to create a person and then click **New Person**.

For example, if you want to create a person belonging to the `Marketing` organization, then right-click the `Marketing` organization and then click **New Person**.

Figure 2–13 shows the menu that is displayed when you right-click the `Marketing` organization.

**Figure 2–13** *Shortcut Menu That Is Displayed When You Right-Click a Reporting Organization Node*



- On the Attributes tab of the New Person page, enter the appropriate values in the fields.

---



---

**Note:** You can successfully create two or more persons with the same display name because there are no uniqueness constraints on the **Display Name** field. Enter a value in the **Unique Name** field to uniquely identify a person in Oracle Role Manager.


---



---

Figure 2–14 shows the Attributes tab on which sample values have been specified.

**Figure 2–14 Attributes Tab for a New Person Record**

 **New Person**

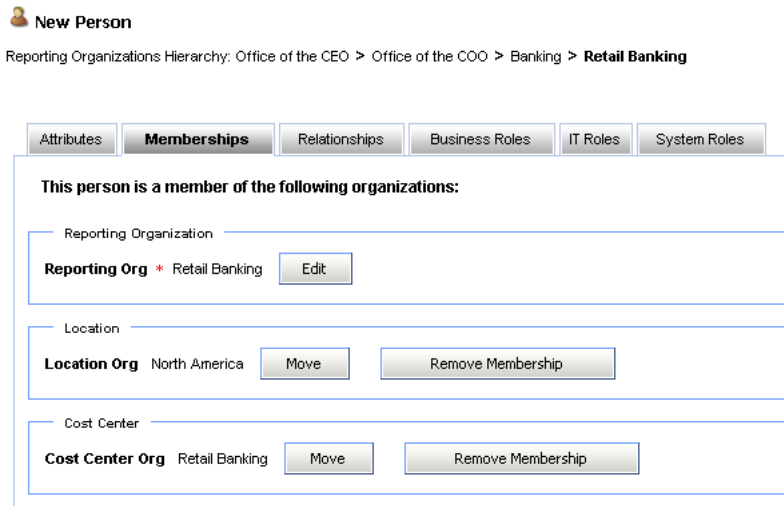
Reporting Organizations Hierarchy: Office of the CEO > Office of the COO > Banking > **Retail Banking**

Attributes	Memberships	Relationships	Business Roles	IT Roles	System Roles
<b>First Name *</b>	<input type="text" value="John"/>				
<b>Last Name *</b>	<input type="text" value="Doe"/>				
<b>Display Name *</b>	<input type="text" value="John Doe"/>				
<b>Unique Name</b>	<input type="text" value="Doe/John-23"/>				
<b>User ID</b>	<input type="text" value="Doe.John"/>				
<b>Password</b>	<input type="password" value="••••••••"/>				
<b>Confirm Password</b>	<input type="password" value="••••••••"/>				
<b>Employee Number</b>	<input type="text" value="549"/>				
<b>Employee Type</b>	<input type="text" value="Facilities"/>				
<b>Fax</b>	<input type="text" value="(213) 555-1248"/>				
<b>Home Phone</b>	<input type="text" value="(415) 555-2387"/>				
<b>Home Address</b>	<input type="text" value="1234-4321 ABC Park"/>				
<b>Job Title</b>	<input type="text" value="Facilities Architect"/>				
<b>Email</b>	<input type="text" value="Doe.John@samplebank.com"/>				
<b>Manager</b> None Selected	<input type="button" value="Edit"/>				
<b>Mobile Phone</b>	<input type="text" value="(715) 555-9876"/>				
<b>Pager</b>	<input type="text" value="(715) 555-1111"/>				
<b>Preferred Mailing Address</b>	<input type="text" value="345 Union Street"/>				
<b>Preferred Language</b>	<input type="text" value="English"/>				
<b>Main Phone</b>	<input type="text" value="(555) 555-1234"/>				
<b>Status *</b>	<input type="text" value="Active"/>				

5. Optionally, on the Memberships tab of the New Person page, you can:
  - Change the reporting organization to which a person belongs, by using **Edit** to search for and select a new reporting organization.
  - Set the location to which a person belongs, by using **Move** to search for and select a new location.
  - Set the cost center to which a person belongs, by using **Move** to search for and select a new cost center.

[Figure 2–15](#) shows the Memberships tab on which sample values have been specified.

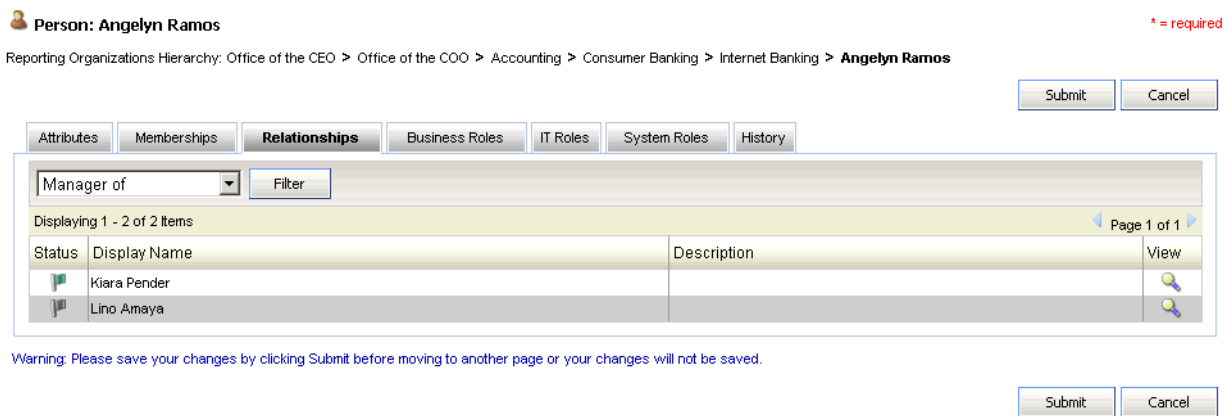
**Figure 2–15 Memberships Tab for a New Person**



6. You cannot perform any action on the Relationships tab while creating a person. However, while you modify a person node on the Relationships tab:
  - To view the list of people a person is managing, select **Manager of** and click **Filter**.
  - To view the list of organizations the person is heading, select **Head of Organization of** and click **Filter**.
  - To view the list of roles the person owns, select **Owner of** and click **Filter**.

Figure 2–16 shows the Relationships tab for a person node.

**Figure 2–16 Relationships Tab for an Existing Person**



7. Optionally, on the Business Roles tab, you can:
  - Grant static business roles by using **Grant Role**. See "[Granting and Revoking Static Business Roles](#)" on page 5-3 for information about granting static business roles.
  - View details of business roles granted to the person by clicking the View icon in the row for the business role.

- Delegate static business roles by using the Delegate icon. See "[Delegating Static Business Roles](#)" on page 5-5 for more information about delegating static business roles.
- Filter business roles (for reference or verification) by providing a criterion for filtering business roles and then clicking **Filter**.

Figure 2–17 shows the Business Roles tab.

**Figure 2–17 Business Roles Tab for a New Person**

**New Person** \* = required

Reporting Organizations Hierarchy: Office of the CEO > Office of the COO > Banking > **Retail Banking**

Submit Cancel

Attributes Memberships Relationships **Business Roles** IT Roles System Roles

Filter for: Business Role Name begins with  Filter

Displaying 1 - 1 of 1 items Page 1 of 1

Status	Business Role Name	Grant Type	Sphere Of Control	Actions
	Compliance Officer	static	Banking	

Grant Role

Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

Submit Cancel

8. Optionally, on the IT Roles tab, you can:

- Grant IT roles by using **Grant Role**. See "[Granting and Revoking IT Roles](#)" on page 4-6 for information about granting IT roles.
- View details of IT roles granted to the person by clicking the View icon in the row for the IT role.
- Delete IT roles mapped to a person by using the Delete icon. See "[Deleting IT Roles](#)" on page 4-8 for more information about deleting IT role mappings.
- Delegate IT roles by using the Delegate icon. See "[Delegating IT Roles](#)" on page 4-7 for more information about delegating IT roles.
- Filter IT roles (for reference or verification) by providing a criterion for filtering IT roles and then clicking **Filter**.

Figure 2–18 shows the IT Roles tab.

**Figure 2–18 IT Roles Tab for a New Person**

**New Person** \* = required

IT Role 'Telecom Provisioner' granted to 'John Doe'.

Reporting Organizations Hierarchy: Office of the CEO > Office of the COO > Banking > **Retail Banking**

Submit Cancel

Attributes Memberships Relationships Business Roles **IT Roles** System Roles

Filter for: IT Role Name begins with  Filter

Displaying 1 - 4 of 4 items Page 1 of 1

Status	IT Role Name	Actions
	Job Scheduler	
	Machine Installer	
	Restart Server Applications	
	Telecom Provisioner	

Grant Role

Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

Submit Cancel

- You cannot perform any action on the System Roles tab while creating a person. However, while you modify a person node, the System Roles tab displays a list of system roles that have been granted to the person.

**Note:** Unless the person has been granted a system role, you will not be able to view any system roles on the System Roles tab.

Figure 2–19 shows the System Roles tab for a person node.

**Figure 2–19 System Roles Tab for an Existing Person**

**Person: Francesco Fajardo** \* = required

Reporting Organizations Hierarchy: Office of the CEO > Office of the COO > Accounting > Commercial Banking > Large Business > Francesco Fajardo

Submit Cancel

Attributes Memberships Relationships Business Roles IT Roles **System Roles** History

Filter for: System Role Name begins with  Filter

Displaying 1 - 2 of 2 items Page 1 of 1

Status	System Role Name	Sphere Of Control	Actions
	Database Administrator	Banking	
	Operating System Administrator	Accounting	

Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

Submit Cancel

- You cannot perform any action on the History tab while creating a person record. However, while you modify a person record, the History tab displays a list of events for the person records.

For example, if you grant an IT role to a person, then this event is stored and displayed on the History tab. Figure 2–20 shows the History tab for a person record.

**Figure 2–20 History Tab for an Existing Person**

**Person: Ellis Arevalo** \* = required

Reporting Organizations Hierarchy: Office of the CEO > Office of the COO > Accounting > Commercial Banking > Ellis Arevalo

Submit Cancel

Attributes Memberships Relationships Business Roles IT Roles System Roles **History**

Displaying 1 - 4 of 4 items Page 1 of 1

Transaction Time	Transaction ID	User	Reason	View
22 October 2008 4:03 PM IST	929	System Administrator	Person 'Ellis Arevalo' was updated.	
22 October 2008 4:00 PM IST	926	System Administrator	Granted Storage Technician role to Ellis Arevalo with Sphere of Control.	
21 October 2008 6:50 PM IST	388	System Administrator	Person was updated.	
21 October 2008 6:50 PM IST	163	System Administrator	Person was created.	

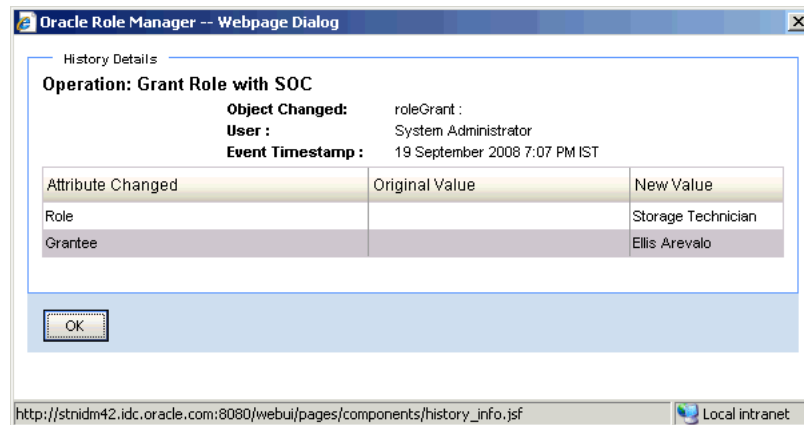
Warning: Please save your changes by clicking Submit before moving to another page or your changes will not be saved.

Submit Cancel

In addition, by clicking the View icon in the row for an event, you can view details of the event, such as the time at which the event occurred, the name of the attribute that has been modified, its original value, and its new value.

Figure 2–21 shows a dialog box that displays details of an event.



**Figure 2–21 History Dialog Box for an Existing Person****11. Click Submit.**

A message indicating that the person was created successfully is displayed.

**2.2.2.3 Modifying Cost Centers, Locations, People, and Reporting Organizations**

To modify a cost center, location, person, or reporting organization:

1. On the first-level navigation bar, click **Organizations & People**.
2. Depending on the node that you want to modify, on the second-level navigation bar, select one of the following:
  - Cost Centers
  - Locations
  - People
  - Reporting Organizations
3. On the left pane, right-click the node within which you want to search the node that has to be modified, and then click **Search**.
4. On the right pane, specify the search criterion for the node that you want to modify.

A list of all nodes that meet the search criterion is displayed.

Figure 2–22 shows the list of people who meet the sample search criterion.

**Figure 2–22 Search Results Displayed on the People Page**

People

Search for:

Displaying 1 - 4 of 4 items Page 1 of 1

Status	First Name	Last Name	Display Name	Unique Name	Email	Actions
	Alva	Weinberg	Alva Weinberg	Weinberg/Alva-20	Weinberg.Alva@samplebank.orn	
	Alverta	Rowell	Alverta Rowell	Rowell/Alverta-72	Rowell.Alverta@samplebank.orn	
	Angelyn	Ramos	Angelyn Ramos	Ramos/Angelyn-45	Ramos.Angelyn@samplebank.orn	
	Asa	Caudill	Asa Caudill	Caudill/Asa-37	Caudill.Asa@samplebank.orn	

5. To display the details of the node that you want to modify, click the View/Edit icon in the row for the node.

6. Depending on the node that you want to modify, select one of the following:
  - If you want to modify a node under cost center, location, or reporting organization, then perform Step 5 of "[Creating Cost Centers, Locations, and Reporting Organizations](#)" on page 2-6.
  - If you want to modify a person account, then perform Steps 4 through 8 of "[Creating People](#)" on page 2-9.

---

---

**Note:** If there are person records in the Unassigned node, then you must perform this procedure. See "[Unassigned Node](#)" on page 2-16 for information about the Unassigned node.

---

---

7. Click **Submit**.

A message indicating that the node was updated successfully is displayed.

### **Unassigned Node**

Person records can be loaded from external systems into Oracle Role Manager. If the organization to which a person belongs was not specified on the external system, then the person is created under the Unassigned node during the loading operation.

For example, consider the following person records that are loaded into Oracle Role Manager:

- John Doe, Accounting, San Jose  
Because the Accounting reporting organization exists in Oracle Role Manager, this person record is created in Oracle Role Manager.
- Jane Doe, Engineering, San Francisco  
The record is not created in Oracle Role Manager because, the Engineering reporting organization does not exist in Oracle Role Manager.
- Richard Roe, , Oakland  
This record is created in the Unassigned node of Oracle Role Manager because no reporting organization has been specified for the person record.

---

---

**Note:** You cannot modify the Unassigned node. For example, you cannot change the display name of the Unassigned node. Similarly, you cannot delete the Unassigned node.

---

---

### **2.2.2.4 Deleting Cost Centers, Locations, and Reporting Organizations**

**To delete a cost center, location, or a reporting organization:**

1. On the first-level navigation bar, click **Organizations & People**.
2. Depending on the node that you want to delete, on the second-level navigation bar, select one of the following:
  - Cost Centers
  - Locations
  - Reporting Organizations
3. Select one of the following:

---

**Note:** You can delete a node *only* if it does not have a child node and associated memberships. For example, you cannot delete an organization that contains persons. Similarly, you cannot delete a locality that contains a building.

---

- a. Right-click the node that you want to delete and click **Delete**. Then, proceed to Step 6.  
A dialog box prompting you to confirm if you want to delete the node is displayed.
  - b. Right-click the reporting organization within which you want to search the node that you want to delete, and then click **Search**.
4. On the right pane, specify the search criterion for the node that you want to delete.  
A list of all nodes that meet the search criterion is displayed.

Figure 2–23 shows the list of reporting organizations that meet the sample search criterion.

**Figure 2–23 Reporting Organizations Page**

Reporting Organizations

Search for:  contains

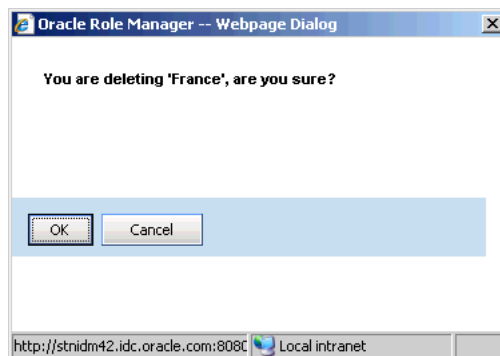
Displaying 1 - 6 of 6 Items Page 1 of 1

Display Name ^	Unique Name	Actions
Banking	org7	
Commercial Banking	org12	
Consumer Banking	org11	
Internet Banking	org19	
Merchant Banking	ou21	
Retail Banking	org10	

5. Click the Delete icon in the row for the node that you want to delete.  
A dialog box prompting you to confirm if you want to delete the node is displayed.

Figure 2–24 shows the dialog box that is displayed when you delete the France location node.

**Figure 2–24 Delete Confirmation Dialog Box**



6. Click **OK**.

A message indicating that the node was deleted successfully is displayed.

### 2.2.2.5 Deleting Persons

---



---

**Note:** Do not perform the procedure described in this section, if the Integration Library is installed. Deleting persons must be performed in a provisioning system.

A provisioning system, such as Oracle Identity Manager, is the authoritative source for people data, and this data is imported into Oracle Role Manager by using the Integration Library.

---



---

**To delete a person:**

1. On the first-level navigation bar, click **Organizations & People**.
2. On the second-level navigation bar, click **People**.
3. On the left pane, perform one of the following:
  - Right-click **People** and then click **Search**.
  - Right-click the reporting organization within which you want to search the person that you want to delete, and then click **Search**.
4. Perform Steps 4 through 6 of "[Deleting Cost Centers, Locations, and Reporting Organizations](#)" on page 2-16.

## 2.2.3 First-Level Navigation Options: Roles

You can create, update, delete, and search approver roles, business roles, IT roles, and IT privileges by using the second-level navigation options available under Roles, as shown in [Figure 2-25](#):

**Figure 2-25 Roles: Second-Level Navigation Options**



Roles is a first-level navigation option. It contains the following second-level navigation options:

- Approver Roles
- Business Roles
- IT Roles
- IT Privileges

Right-clicking a node for any role or IT privilege on the left pane of the Roles page displays the menu options listed in [Table 2-2](#). You can perform the actions listed in this table depending on the privileges that you have been granted. For example, the New option is grayed out if you do not have the appropriate system privilege to create a business role.

**Table 2–2 Roles: Shortcut Menu Options**

Menu Item	Action
View <Role Type> In this menu item, <Role Type> can take values such as Approver Roles, Business Role, or IT roles.	Displays a list of roles within the selected reporting organization. For example, you can right-click Office of the CEO reporting organization under the IT Roles node, and then click <b>View IT Roles</b> to view the list of IT roles within the Office of the CEO reporting organization. <b>Note:</b> This option is not available for the IT Privilege node.
New <Role Type> In this menu item, <Role Type> can take the values such as Approver Roles, Business Role, or IT roles <b>Note:</b> The New menu item is also available for the IT Privilege node.	Creates a role or an IT privilege.
Search	Searches for roles or IT privileges within the current node and all its child nodes.
Collapse	Changes the display of the current node to show only the parent node and hide all child nodes.
Expand	Changes the display of the current node to show all its child nodes.
Refresh	Refreshes the view of the node

For information about creating, modifying, and deleting approver roles, business role, IT roles, and IT privileges see [Working with IT Privileges and IT Roles](#), [Working with Business Roles](#), and [Working with Approver Roles](#).

### Unassigned Node

Roles can be loaded into Oracle Role Manager by using a command line script or the Oracle Role Manager administrative console. If the organization to which a role belongs was not specified on the external system, then the role is created under the Unassigned node during the loading operation.

For example, consider the following roles that are loaded into Oracle Role Manager:

- Risk Manager, Marketing, Active  
Because the Marketing reporting organization exists in Oracle Role Manager, this role is created in Oracle Role Manager.
- Compliance Officer, Financial Banking, Inactive  
The role is not created in Oracle Role Manager because the Financial Banking reporting organization does not exist in Oracle Role Manager.
- Sales Representative, , Active  
This role is created in the Unassigned node of Oracle Role Manager because no reporting organization has been specified for the role.

---

**Note:** You cannot modify the Unassigned node. For example, you cannot change the display name of the Unassigned node. Similarly, you cannot delete the Unassigned node.

---

## 2.2.4 First-Level Navigation Options: Administration

You can create, update, delete, and search system roles by using the second-level navigation option available under Administration, as shown in [Figure 2–26](#):

**Figure 2–26 Administration: Second-Level Navigation Options**



Administration is a first-level navigation option. It contains System Roles, which is the second-level navigation option.

Right-clicking the system roles node on the left pane of the Administration page displays the menu options listed in [Table 2–3](#). You can perform the actions listed in this table depending on the privileges that you have been granted. For example, the New option is grayed out if you do not have the appropriate system privilege to create a system role.

**Table 2–3 Administration: Shortcut Menu Options**

Menu Item	Action
View	Displays a list of system roles within the selected reporting organization.  For example, if you right-click the Office of the COO reporting organization under the System Roles node and then click <b>View System Roles</b> , then you can view the list of system roles within the Office of the COO reporting organization.
New	Creates a system role.
Search	Searches for system roles within the current node and all its child nodes.
Collapse	Changes the display of the current node to show only the parent node and hide all child nodes.
Expand	Changes the display of the current node to show all its child nodes.
Refresh	Refreshes the view of the node.

For information about creating, modifying, and deleting system roles see [Working with System Roles](#).

---

---

## Working with System Roles

This chapter discusses the predefined system roles in Oracle Role Manager. This chapter also discusses the procedure to create and manage system roles. It contains the following sections:

- [Predefined System Roles](#)
- [Creating System Roles](#)
- [Mapping and Unmapping System Privileges](#)
- [Granting and Revoking System Roles](#)
- [Deleting System Roles](#)

### 3.1 Predefined System Roles

Oracle Role Manager provides predefined system roles in the sample data. In addition, Oracle Role Manager provides the following predefined system roles (including the System Administrator system role):

---

---

**Note:** See *Oracle Role Manager Installation Guide* for information about loading the standard\_roles.dar file containing predefined system roles.

---

---

- [System Administrator](#)
- [System Role Administrator](#)
- [System Role Grant Administrator](#)
- [Role Administrator](#)
- [Role Grant Administrator](#)
- [Reporting Organization Administrator](#)
- [Cost Center Administrator](#)
- [Location Administrator](#)
- [User Administrator](#)
- [Auditor](#)
- [Role Delegation Administrator](#)

### 3.1.1 System Administrator

The `System Administrator` system role enables complete access to the Oracle Role Manager system. This system role is granted to persons.

A person who is granted this system role can perform all transactions in the system without regard to sphere of control (SOC).

The following are the privileges that are mapped to the `System Administrator` system role:

- All for Approver Role objects
- All for Business Role objects
- All for Cost Center Hierarchy Root objects
- All for IT Privilege objects
- All for IT Role objects
- All for Location Hierarchy Root objects
- All for Person objects
- All for Reporting Hierarchy Root objects
- All for System Identity objects
- All for System Role objects
- All for all organization objects

### 3.1.2 System Role Administrator

The responsibilities of the `System Role Administrator` system role are as follows:

- Creating system roles
- Updating system roles
- Deleting system roles
- Reading audit data related to system roles
- Mapping and unmapping system privileges to and from system roles

The `System Role Administrator` system role is granted to persons.

A person with the `System Role Administrator` system role can perform all the actions listed in the preceding list without regard to SOC.

The following are the system privileges that are mapped to the `System Role Administrator` system role:

- Audit System Role objects
- Manage System Role objects

### 3.1.3 System Role Grant Administrator

The responsibilities of the `System Role Grant Administrator` system role are as follows:

- Granting system roles
- Revoking system roles

The `System Role Grant Administrator` system role is granted to persons.



System role grant administrators can grant and revoke roles to and from users without regard to SOC.

The following are the system privileges that are mapped to the `System Role Grant Administrator` system role:

- Grant Person objects
- Grant System Identity objects
- Grant System Role objects

### 3.1.4 Role Administrator

The responsibilities of the `Role Administrator` system role are as follows:

- Creating roles and privileges (except system roles and system privileges)

---



---

**Note:** Creating a role includes creating rules (membership and eligibility rules) for role grants.

---



---

- Updating roles and privileges (except system roles and system privileges)
- Moving roles (except system roles)
- Deleting roles and privileges (except system roles and system privileges)
- Reading audit data related to approver, business, and IT roles
- Managing privilege mappings between business roles and IT roles
- Managing privilege mappings between IT roles and IT privileges

The `Role Administrator` system role is granted to persons

This system role can be granted with SOC. The SOC for this system role is defined relative to the reporting organization hierarchy.

For example, if John Doe is granted the `Role Administrator` system role with SOC over Accounting organization, then:

- John can create, update, move, and delete roles in the Accounting organization and any of its child organizations.
- John can create rules for role grants, however he does not have the ability to grant roles.
- If the Operations Director business role belongs to the Accounting organization, then John can map the Network Engineer IT role to the Operations Director business role. This is regardless of whether or not the reporting organization of the Network Engineer IT role is the Accounting organization or any of its child organizations.

Similarly, John can delete the mapping between the Network Engineer IT role and the Operations Director business role based on the criterion described in the preceding paragraph.

The following are the system privileges that are mapped to the `Role Administrator` system role:

- Audit Approver Role objects
- Audit Business Role objects

- Audit IT Privilege objects
- Audit IT Role objects
- Manage Approver Role objects
- Manage Business Role objects
- Manage IT Privilege objects
- Manage IT Role objects

### 3.1.5 Role Grant Administrator

The responsibilities of the `Role Grant Administrator` system role are as follows:

- Granting roles (except system roles)
- Revoking roles (except system roles)

The `Role Grant Administrator` system role is granted to persons

This system role can be granted with SOC. The SOC for this system role is defined relative to the reporting organization hierarchy.

For example, if John Doe is granted the `Role Grant Administrator` system role with SOC over Accounting organization, then:

- John can grant roles that belong to the Accounting organization, its parent organization, or any of its child organizations.
- John can grant roles *only* to people who belong to the Accounting organization or any of its child organizations.

Similarly, John Doe can revoke roles based on the criterion described in the preceding paragraph.

---

---

**Note:** Role Grant Administrators cannot create or edit the rules for approver, static, and dynamic business role grants.

---

---

The following are the system privileges that are mapped to the `Role Grant Administrator` system role:

- Grant Business Role objects
- Grant IT Role objects
- Grant Person objects

### 3.1.6 Reporting Organization Administrator

The responsibilities of the `Reporting Organization Administrator` system role are as follows:

- Creating organizations
- Updating organizations
- Moving organizations
- Deleting organizations
- Reading organization-related audit data

The `Reporting Organization Administrator` system role can be granted to persons or system identities (through integrations. For example, the Oracle Role Manager and the Oracle Identity Manager integration) .

This system role can be granted with SOC. The SOC for this system role is defined relative to the reporting organization hierarchy.

For example, if John Doe is granted the `Reporting Organization Administrator` system role with SOC over the Commercial Banking organization, then he can perform the following actions:

- Create organizations within the Commercial Banking organization and any of its child organizations.
- Update the Commercial Banking organization and any of its child organizations.
- Move the child organizations of the Commercial Banking organization to any of its child organizations.
- Delete the Commercial Banking organization and any of its child organizations.
- Read organization-related audit data of the Commercial Banking organization and any of its child organizations.

The following are the system privileges that are mapped to the `Reporting Organization Administrator` system role:

- Audit all organization objects
- Manage all organization objects

### 3.1.7 Cost Center Administrator

The responsibilities of the `Cost Center Administrator` system role are as follows:

- Creating cost center hierarchies
- Updating cost center hierarchies
- Moving cost center hierarchies
- Deleting cost center hierarchies
- Reading cost center-related audit data

The `Cost Center Administrator` system role can be granted to persons or system identities.

This system role can be granted with SOC. The SOC for this system role is defined relative to the cost center hierarchy.

For example, if John Doe is granted the `Cost Center Administrator` system role with SOC over the Retail Banking cost center, then he can perform the following actions:

- Create cost centers within the Retail Banking cost center and any of its child cost centers.
- Update the Retail Banking cost center and any of its child cost centers.
- Move the child cost centers of the Retail Banking cost center to any of its child cost centers.
- Delete the Retail Banking cost center and any of its child cost centers.
- Read cost center-related audit data of the Retail Banking cost center and any of its child cost centers.

The following are the system privileges that are mapped to the `Cost_Center Administrator` system role:

- Audit all organization objects
- Manage all organization objects

### 3.1.8 Location Administrator

The responsibilities of the `Location Administrator` system role are as follows:

- Creating location hierarchies
- Updating location hierarchies
- Moving location hierarchies
- Deleting location hierarchies
- Reading location-related audit data

The `Location Administrator` system role can be granted to persons or system identities.

This system role is granted with SOC. The SOC for this system role is defined relative to the location hierarchy.

For example, if John Doe is granted the `Location Administrator` system role with SOC over the United States location, then he can perform the following actions:

- Create locations within the United States and any of its child location nodes.
- Update the United States location node and any of its child location nodes.
- Move the child location nodes of the United States location node to any of its child location nodes.
- Delete the United States location and any of its child locations.
- Read location-related audit data of the United States location node and any of its child location nodes.

The following are the system privileges that are mapped to the `Location Administrator` system role:

- Audit all organization objects
- Manage all organization objects

### 3.1.9 User Administrator

The responsibilities of the `User Administrator` system role are as follows:

- Creating person records
- Updating person records
- Deleting person records
- Creating organization memberships
- Updating organization memberships
- Deleting organization memberships
- Reading person-related audit data

The `User Administrator` system role can be granted to persons or system identities.

This system role is granted with SOC. The SOC for this system role is defined relative to the reporting hierarchy.

For example, if John Doe is granted the `User Administrator` system role with SOC over the Consumer Marketing organization, then he can perform the following actions:

- Create person records within the Consumer Marketing organization and any of its child organizations.
- Update person records belonging to the Consumer Marketing organization and any of its child organizations.
- Delete person records belonging to the Consumer Marketing organization or any of its child organizations.
- Create, update, and delete location and cost center memberships of a person record belonging to the Consumer Marketing organization or any of its child organizations.
- Read person-related audit data of person records belonging to the Consumer Marketing organization and any of its child organizations.

The following are the system privileges that are mapped to the `User Administrator` system role:

- Audit Person objects
- Manage Person objects

### 3.1.10 Auditor

The responsibility of the `Auditor` system role is to evaluate the records in the Oracle Role Manager system for compliance or debugging purposes.

The `Auditor` system role is granted to persons.

A user who is granted this system role requires read-only access to all the records in the system. SOC is not applied to this system role.

The following are the system privileges that are mapped to the `Auditor` system role:

- Audit Approver Role objects
- Audit Business Role objects
- Audit IT Privilege objects
- Audit IT Role objects
- Audit Person objects
- Audit System Identity objects
- Audit System Role objects
- Audit all organization objects

### 3.1.11 Role Delegation Administrator

The responsibilities of the Role Delegation Administrator system role are as follows:

- Delegating roles

- Revoking delegated roles.

The `Role Delegation Administrator` system role can be granted to persons or system identities.

This system role is granted with SOC. The SOC for this system role is defined relative to the reporting organization hierarchy.

For example, if John Doe is granted the `Role Delegation Administrator` system role with SOC over Accounting organization, then:

- John can delegate roles that belong to the Accounting organization, its parent organization, or any of its child organizations.
- John can delegate roles *only* to people who belong to the Accounting organization or any of its child organizations.

Similarly, John Doe can revoke the delegated roles based on the criterion described in the preceding paragraph.

The following are the system privileges that are mapped to the `Role Delegation Administrator` system role:

- Delegate Business Role objects
- Delegate IT Role objects
- Delegate Person objects

## 3.2 Creating System Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for System Role objects and All for System Privilege objects
- Manage System Role objects and Manage System Privilege objects

For example, a user who is granted the `System Administrator` or `System Role Administrator` system role can perform the procedure described in this section.

---

---

### To create a system role:

1. On the first-level navigation bar, click **Administration**.
2. On the left pane, right-click the organization where you want to create the system role and then click **New System Role**.
3. In the **Display Name** field on the Attributes tab of the New System Role page, type the name of the system role being created.
4. If you want to enter a unique name for the system role, then enter it in the **Unique Name** field.
5. If you want to set SOC for the role, then:

---

---

**Note:** If you do not set SOC while creating the role, then you will not be able set SOC any time later. In addition, you cannot modify SOC after it is has been set.

---

---

- a. In the Sphere of Control field, click **Edit**.
  - b. On the page that is displayed, specify a search criterion for the hierarchy on which you want to set SOC.  
A list of hierarchies that meet the search criterion is displayed.
  - c. From this list, select the hierarchy on which you want to set SOC and then click **OK**.
6. If you want to enter a description for the system role, then enter it in the **Description** field.
  7. In the Status box, select the status of the system role.
  8. If you want to set an owner for the system role, then:
    - a. In the Owner field, click **Edit**.
    - b. On the page that is displayed, specify the search criterion for the person whom you want to set as the owner of the system role.  
A list of persons who meet the search criterion is displayed.
    - c. From this list, select the person whom you want to set as the owner and then click **OK**.
  9. To set the organization to which the system role must belong:

---

---

**Note:** By default, the system role that you create belongs to the organization that you select in Step 2. If you want to change the organization to which the role must belong, then perform the instructions in this step.

---

---

- a. In the Reporting Org field, click **Edit**.
- b. On the page that is displayed, specify the search criterion for the organization that you want to select.

---

---

**Note:** This is the organization within which the system role is listed after it is created.

---

---

A list of all organizations that meet the search criterion is displayed.

- c. From this list, select the organization and then click **OK**.
10. If you want to map system privileges to the system role:
    - a. Click the **Privileges** tab.
    - b. Click **Map Privilege**.
    - c. On the page that is displayed, specify the search criterion for the system privilege that you want to map. These are the system privileges that have already been created.  
A list of all system privileges that meet the search criterion is displayed.
    - d. From this list, select a system privilege and then click **OK**.  
A message indicating that the system privilege mapping to the system role was successful is displayed.

- e. Repeat Steps b through d for each system privilege that you want to map.
  11. If you want to grant a system role (while creating the system role) to an Oracle Role Manager user, then:
    - a. Click the **Members** tab.
    - b. Click **Grant System Role**.
    - c. On the page that is displayed, specify a search criterion for the person to whom you want to grant the system role.

A list of all persons who meet the search criterion is displayed.
    - d. From this list, select the person and then click **Next**.
    - e. If you want to set the scope of the grant to all nodes in the hierarchy that you chose in Step 5. c, then select **Set Sphere of Control to All Organizations in the Hierarchy** and click **Finish**. Alternatively, if you want to set the scope of the grant to a specific node within the hierarchy (that you chose in Step 5. c), then:
      - i. Select **Pick a Single Organization in the Hierarchy**.
      - ii. Click **Next**.
      - iii. Specify a search criterion for the node to which you want the grant to be limited. A list of all nodes that meet the search criterion is displayed.
      - iv. From this list, select the node and then click **Finish**. A message indicating that the role has been granted is displayed.
      - v. Repeat Steps b through e for each person to whom the role must be granted.
12. Click **Submit** to complete the procedure for creating the system role.

A message indicating that the role was created successfully is displayed.

### 3.3 Mapping and Unmapping System Privileges

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for System Role objects
- Manage System Role objects

For example, a user who is granted the `System Administrator` or `System Role Administrator` system role can perform the procedure described in this section.

---

---

**To map or unmap system privileges to or from system roles:**

1. On the first-level navigation bar, click **Administration**.
2. On the left pane, perform one of the following:
  - Right-click the **System Roles** node and then click **Search**.
  - Right-click the reporting organization within which you want to search the system role (whose system privileges must be mapped or unmapped), and then click **Search**.



3. On the System Roles page, specify the search criterion for the system role.  
A list of all system roles that meet the search criterion is displayed.
4. To display the details of the system role, click the View /Edit icon in the row for the system role.
5. Click the **Privileges** tab.
6. If you want to map system privileges, then:
  - a. Click **Map Privilege**.
  - b. On the page that is displayed, specify the search criterion for the system privilege that you want to map. These are the system privileges that have already been created.  
A list of all system privileges that meet the search criterion is displayed.
  - c. From this list, select a system privilege and then click **OK**.  
A message indicating that the system privilege mapping to the system role was successful is displayed.
  - d. Repeat Steps a through c for each system privilege that you want to map.
  - e. Proceed to Step 8
7. If you want to unmap system privileges, then:
  - a. Click the Delete icon in the row for the system privilege that you want to delete.  
A dialog box prompting you to confirm if you want to delete the system privilege is displayed.  

---

---

**Note:** Performing this step will only delete the mapping between the system privilege and the system role. It does not actually delete the system privilege.  

---

---
  - b. Click **OK**.  
A message indicating that the privilege mapping was successfully deleted is displayed.
  - c. Repeat Steps a and b for each system privilege that you want to unmap.
  - d. Proceed to Step 8
8. Click **Submit**.  
A message indicating that the system role was updated successfully is displayed.

## 3.4 Granting and Revoking System Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for System Role objects and All for Person objects
- Grant System Role objects and Grant Person objects

For example, a user who is granted the `System Administrator` or `System Role Grant Administrator` system role can perform the procedure described in this section.

---

---

### To grant or revoke a system role:

1. On the first-level navigation bar, click **Administration**.
2. On the left pane, perform one of the following:
  - Right-click the **System Roles** node and then click **Search**.
  - Right-click the reporting organization within which you want to search the system role and then click **Search**.
3. On the System Roles page, specify the search criterion for the system role that you want to grant or revoke.

A list of all system roles that meet the search criterion is displayed.
4. To display the details of the system role that you want to grant or revoke, click the View/Edit icon in the row for the system role.
5. Click the **Members** tab.
6. If you want to revoke the system role grant for a particular person, then:
  - a. Click the Delete icon in the row for that person.
  - b. On the page that is displayed, click **OK** to confirm that you want to revoke the system role grant.

A message indicating that the role grant was successfully deleted is displayed.
  - c. Proceed to Step 12.
7. If you want to grant the system role, then click **Grant System Role**.
8. On the page that is displayed, specify a search criterion for the person to whom the system role must be granted.

A list of all persons who meet the search criterion is displayed.
9. From this list, select the person and then click **Next**.
10. If the system role that you want to grant has a sphere of control set, then:

If you want to set the scope of the grant to all organizations in the hierarchy to which the system role belongs, then select **Set Sphere of Control to All Organizations in the Hierarchy** and click **Finish**. Alternatively, if you want to set the scope of the grant to a specific organization within the hierarchy to which the static business role belongs, then:

  - a. Select **Pick a Single Organization in the Hierarchy**.
  - b. Click **Next**.

- c. Specify a search criterion for the organization to which you want the grant to be limited.  
A list of all organizations that meet the search criterion is displayed.
  - d. From this list, select the organization to which you want the grant to be limited and then click **Next**.
  - e. Proceed to Step 12.
11. If the system role that you want to grant has no sphere of control, then click **Finish**.  
A message indicating that the system role has been granted is displayed.
  12. Click **Submit**.  
A message indicating that the system role was updated successfully is displayed.

## 3.5 Deleting System Roles

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for System Role objects
- Manage System Role objects

For example, a user who is granted the `System Administrator` or `System Role Administrator` system role can perform the procedure described in this section.

---

### To delete a system role:

1. On the first-level navigation bar, click **Administration**.
2. On the left pane, perform one of the following:
  - Right-click the **System Roles** node and then click **Search**.
  - Right-click the reporting organization within which you want to search the system role that you want to delete, and then click **Search**.
3. On the System Roles page, specify the search criterion for the system role that you want to delete.  
A list of all system roles that meet the search criterion is displayed.
4. Click the Delete icon in the row for the system role that you want to delete.  
A dialog box prompting you to confirm if you want to delete the system role is displayed.
5. Click **OK**.  
A message indicating that the system role was deleted successfully is displayed.



---

---

## Working with IT Privileges and IT Roles

This chapter discusses the procedure to create and manage IT privileges and IT roles. It contains the following sections:

- [Section 4.1, "IT Privileges"](#)
- [Section 4.2, "IT Roles"](#)

### 4.1 IT Privileges

As discussed in one of the earlier chapters, IT privileges associate themselves with IT resources.

This section discusses the following topics:

---

---

**Note:** Do not perform any of the procedures described in this section, if the Integration Library is installed. Creating, modifying, and deleting IT privileges must be performed in provisioning systems.

A provisioning system, such as Oracle Identity Manager, is the authoritative source for IT privilege data, and this data is imported into Oracle Role Manager by using the Integration Library.

---

---

---

---

**Note:** To perform the procedures described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Privilege objects
  - Manage IT Privilege objects
- 
- 
- [Creating IT Privileges](#)
  - [Modifying IT Privileges](#)
  - [Deleting IT Privileges](#)

#### 4.1.1 Creating IT Privileges

To create an IT privilege:

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Privileges**.

3. On the left pane, right-click the IT Privileges node and then click **New IT Privilege**.
4. In the **Display Name** field on the Attributes tab of the New IT Privilege page, type the name of the IT privilege being created.
5. If you want to enter a unique name for the IT privilege, then enter it in the **Unique Name** field.
6. If you want to enter privilege details for the IT privilege, then enter it in the **Privilege Details** field.
7. If you want to enter a description for the IT privilege, then enter it in the **Description** field.

For example, the description for the `Configure Default Router` IT privilege can be as follows:

Configure router to external networks.

8. Click **Submit**.

A message indicating that the IT privilege was created successfully is displayed.

## 4.1.2 Modifying IT Privileges

To modify an IT privilege:

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Privileges**.
3. On the left pane, right-click the IT Privileges node and then click **Search**.
4. On the right pane, specify the search criterion for the IT privilege that you want to modify.

A list of all IT privileges that meet the search criterion is displayed.

5. To display the details of the IT privilege that you want to modify, click the View/Edit icon in the row for the IT privilege.
6. Depending on the fields that you want to modify, perform one or all of Steps 4 through 7 of "[Creating IT Privileges](#)" on page 4-1.
7. Click **Submit**.

A message indicating that the IT privilege was updated successfully is displayed.

## 4.1.3 Deleting IT Privileges

To delete an IT privilege:

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Privileges**.
3. On the left pane, right-click the IT Privileges node and then click **Search**.
4. On the right pane, specify the search criterion for the IT privilege that you want to delete.

A list of all IT privileges that meet the search criterion is displayed.

5. Click the Delete icon in the row for the IT privilege that you want to delete.

A dialog box prompting you to confirm if you want to delete the IT privilege is displayed.

6. Click **OK**.

A message indicating that the IT privilege was deleted successfully is displayed.

## 4.2 IT Roles

This section discusses the following topics:

- [Creating IT Roles](#)
- [Mapping and Unmapping IT Privileges](#)
- [Granting and Revoking IT Roles](#)
- [Delegating IT Roles](#)
- [Deleting IT Roles](#)

### 4.2.1 Creating IT Roles

---



---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Role objects and All for IT Privilege objects
  - Manage IT Role objects and Manage IT Privilege objects
- 
- 

**To create an IT role:**

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Roles**.
3. On the left pane, right-click the organization where you want to create the IT role and then click **New IT Role**.
4. In the **Display Name** field on the Attributes tab of the New IT Role page, type the name of the IT role being created.
5. If you want to enter a unique name for the IT role, then enter it in the **Unique Name** field.
6. If you want to enter a description for the IT role, then enter it in the **Description** field.
7. If you want to delegate the IT role being created, then select **Can Be Delegated**.
8. If the IT role being created is related to finance, then select **Is Finance Related**.
9. If the IT role being created is a high-risk role, then select **Is High Risk**.
10. If the IT role being created is associated with non-public personal information, then select **Non-Public Personal Information Related**.
11. If the IT role being created is related to SOX, then select **Sarbanes-Oxley Related**.
12. In the Status box, select the status of the IT role.
13. If you want to set an owner for the IT role, then:

- a. In the Owner field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the person whom you want to set as the owner of the IT role.  
A list of persons who meet the search criterion is displayed.
  - c. From this list, select the person whom you want to set as the owner and then click **OK**.
14. To set the organization to which the IT role must belong:

---

---

**Note:** By default, the IT role that you create belongs to the organization that you select in Step 3. If you want to change the organization to which the role must belong, then perform the instructions in this step.

---

---

- a. In the Reporting Org field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the organization that you want to select.
- 
- 
- Note:** This is the organization that will be responsible for administering this IT role. In addition, this is also the organization within which the IT role is listed after it is created.
- 
- 
- A list of all organizations that meet the search criterion is displayed.
- c. From this list, select the organization and then click **OK**.
15. You cannot perform any action on the Members tab while creating an IT role. However, while you modify an IT role, the Members tab displays a list of people who have been granted this role. See "[Granting and Revoking IT Roles](#)" on page 4-6 for information about granting an IT role.
16. If you want to map IT privileges to the IT role, then:
- a. Click the **Privileges** tab.
  - b. Click **Map Privilege**.
  - c. On the page that is displayed, specify the search criterion for the IT privilege that you want to map. These are the IT privileges that have been created by performing the steps described in "[Creating IT Privileges](#)" on page 4-1.  
A list of all IT privileges that meet the search criterion is displayed.
  - d. From this list, select an IT privilege and then click **OK**.  
A message indicating that the IT privilege mapping to the IT role was created successfully is displayed.
  - e. Repeat Steps b through d for each IT privilege that you want to map.
17. You cannot perform any action on the Mappings tab while creating an IT role. However, while you modify an IT role, the Mappings tab displays a list of business roles to which the IT role is mapped. See "[Working with Business Roles](#)" on page 5-1 for information about mapping IT roles to business roles.



18. You cannot perform any action on the History tab while creating an IT role. However, while you modify an IT role the History tab displays a list of events for the IT role.

For example, if you update the Description field of the IT role, then this event is stored and displayed on the History tab.

19. Click **Submit** to complete the procedure for creating the IT role.

A message indicating that the IT role was successfully created is displayed.

## 4.2.2 Mapping and Unmapping IT Privileges

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Role objects
  - Manage IT Role objects
- 
- 

**To map or unmap an IT privilege to or from an IT role:**

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Roles**.
3. On the left pane, perform one of the following:
  - Right-click **IT Roles** and then click **Search**.
  - Right-click the reporting organization within which you want to search the IT role (whose IT privilege must be mapped or unmapped), and then click **Search**.
4. On the IT Roles page, specify the search criterion for the IT role.

A list of all IT roles that meet the search criterion is displayed.
5. To display the details of the IT role, click the View/Edit icon in the row for the IT role.
6. Click the **Privileges** tab.
7. If you want to map IT privileges, then:
  - a. Click **Map Privilege**.
  - b. On the page that is displayed, specify the search criterion for the IT privilege that you want to map. These are the IT privileges that have been created by performing the steps described in "[Creating IT Privileges](#)" on page 4-1.

A list of all IT privileges that meet the search criterion is displayed.
  - c. From this list, select an IT privilege and then click **OK**.

A message indicating that the IT privilege mapping to the IT role was created successfully is displayed.
  - d. Repeat Steps a through c for each IT privilege that you want to map.
8. If you want to unmap IT privileges, then:
  - a. Click the Delete icon in the row for the IT privilege that you want to delete.

A dialog box prompting you to confirm if you want to delete the IT privilege is displayed.

---

---

**Note:** Performing this step will only delete the mapping between the IT privilege and the IT role. It does not actually delete the IT privilege.

---

---

- b. Click **OK**.

A message indicating that the privilege mapping was successfully deleted is displayed.

- c. Repeat Steps a and b for each IT privilege that you want to unmap.

9. Click **Submit**.

A message indicating that the system role was updated successfully is displayed.

### 4.2.3 Granting and Revoking IT Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Role objects and All for Person objects
  - Grant IT Role objects and Grant Person objects
  - All for IT Role objects and Grant for Person objects
  - Grant for IT Role objects and All for Person objects
- 
- 

#### To grant or revoke an IT role:

1. On the first-level navigation bar, click **Organizations & People**.
2. On the second-level navigation bar, click **People**.
3. To search for the person to whom you want to grant an IT role, perform one of the following:
  - Right-click the **People** node and then click **Search**.
  - Right-click the reporting organization to which the person belongs, and then click **Search**.
4. On the People page, specify the search criterion for the person to whom you want to grant the IT role.

A list of all persons who meet the search criterion is displayed.
5. To display the details of the person, click the View/Edit icon in the row for the person.
6. Click the **IT Roles** tab.
7. If you want to grant the IT role, then:
  - a. If you want to check whether the IT role has already been granted to the person, then specify the search criterion for the IT role and click **Filter**. If the IT role is displayed, then it implies that this role has already been granted to the person. Therefore, you need not perform the remaining steps in this section.

- b. Click **Grant Role**.
- c. On the page that is displayed, specify a search criterion for the IT role that you want to grant.  
A list of all IT roles that meet the search criterion is displayed.
- d. From this list, select the IT role that you want to grant and then click **Finish**.
- e. Proceed to Step 9.
8. If you want to revoke the IT role grant for a particular person, then:
  - a. Click the Delete icon in the row for the IT role.
  - b. On the page that is displayed, click **OK** to confirm that you want to delete the IT role grant.  
A message indicating that the role grant was deleted successfully is displayed.
9. Click **Submit**.  
A message indicating that the person's information was updated successfully is displayed.

#### 4.2.4 Delegating IT Roles

You can delegate an IT role only if it was created with the Role Is Delegatable option selected. You select this option while performing Step 7 of the procedure described in "Creating IT Roles" on page 4-3.

Delegating roles enables you to distribute role administration across users in your enterprise. The status of the role (active or inactive) does not affect its ability to be delegated.

A person who has received a role through delegation can delegate the same role to another person.

##### To delegate an IT role:

---



---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Role objects and All for Person objects
  - Delegate IT Role objects and Delegate Person objects
- 
- 

1. On the first-level navigation bar, click **Organizations & People**.
2. On the left pane, perform one of the following:
  - Right-click the **People** node and then click **Search**.
  - Right-click the reporting organization within which the person to whom you want to delegate the IT roles exists, and then click **Search**.
3. On the People page, specify a search criterion for the person whose IT role must be delegated.  
A list of all users in the organization who satisfy the search criterion is displayed.
4. To display the details of the person, click the View/Edit icon in the row for the person.

5. Click the **IT Roles** tab.
6. Specify a search criterion for the role that you want to delegate.  
A list of all roles that meet the search criterion is displayed.
7. From this list, click the Delegate icon in the Actions column for the IT role that you want to delegate.
8. On the page that is displayed, specify a search criterion for the person to whom you want to delegate the IT role.  
A list of all persons who meet the search criterion is displayed.
9. From this list, select the person to whom you want to delegate the IT role and then click **OK**.  
A message indicating that the IT role was delegated is displayed.
10. Click **Submit**.  
A message indicating that the person information was updated successfully is displayed.

## 4.2.5 Deleting IT Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for IT Role objects
  - Manage IT Role objects
- 
- 

### To delete an IT role:

1. On the first-level navigation bar, click **Roles**.
2. On the second-level navigation bar, click **IT Roles**.
3. On the left pane, perform one of the following:
  - Right-click the **IT Roles** node and then click **Search**.
  - Right-click the reporting organization within which you want to search the IT role that you want to delete, and then click **Search**.
4. On the IT Roles page, specify the search criterion for the IT role that you want to delete.  
A list of all IT roles that meet the search criterion is displayed.
5. Click the Delete icon in the row for the IT role that you want to delete.  
A dialog box prompting you to confirm if you want to delete the IT role is displayed.
6. Click **OK**.  
A message indicating that the IT role was deleted successfully is displayed.

---

---

## Working with Business Roles

This chapter discusses the procedure to create and manage static and dynamic business roles. It contains the following sections:

- [Static Business Roles](#)
- [Dynamic Business Roles](#)

### 5.1 Static Business Roles

As discussed in the preceding chapter, a static business role must be granted manually. Static business roles do not depend on rules to determine who should be granted a particular role. However, these roles can have an eligibility rule, which enables you to refine role memberships.

This section discusses the following topics:

- [Creating Static Business Roles](#)
- [Granting and Revoking Static Business Roles](#)
- [Delegating Static Business Roles](#)

#### 5.1.1 Creating Static Business Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Business Role objects
  - Manage Business Role objects
- 
- 

**To create a static business role:**

1. On the first-level navigation bar, click **Roles**.
2. Click **Business Roles**.
3. On the left pane, right-click the organization where you want to create the static business role and then click **New Business Role**.

For example, if you want to create the `Comptroller` static business role, then you right-click the Accounting organization.

4. In the Business Role Type box, select **Static**, and then click **Submit**.

5. In the **Display Name** field on the Attributes tab of the New Business Role page, type the name of the static business role that you are creating.
6. If you want to enter a unique name for the static business role, then enter it in the **Unique Name** field.
7. If you want to set sphere of control (SOC) for the role, then:

---

---

**Note:** If you set SOC, then you cannot delegate static business roles.

If you do not set SOC while creating the role, then you will not be able to set SOC any time later. In addition, you cannot modify SOC once it has been set.

---

---

- a. In the Sphere of Control field, click **Edit**.
  - b. On the page that is displayed, specify a search criterion for the hierarchy on which you want to set the SOC.  
  
A list of hierarchies that meet the search criterion is displayed.
  - c. From this list, select the hierarchy on which you want to set SOC, and then click **OK**.
8. If you want to enter a description for the static business role, then enter it in the **Description** field.
  9. If you want to enter the responsibilities of the static business role, then enter it in the **Responsibilities** field.  
  
For example, the responsibilities of the Banking Clerk static business role are to assist banking clients with deposits, withdrawals, and opening new accounts.
  10. If you want to delegate the role, then select **Role Is Delegatable**.

---

---

**Note:** You cannot create the static business role if SOC is set and the Role Is Delegatable check box is selected.

---

---

The "[Delegating Static Business Roles](#)" on page 5-5 discusses the procedure to delegate static business roles.

11. In the Status box, select the status of the static business role.
12. If you want to set an owner for the static business role, then:
  - a. In the Owner field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the person whom you want to set as the owner of the static business role.  
  
A list of persons who meet the search criterion is displayed.
  - c. From this list, select the person whom you want to set as the owner and then click **OK**.
13. To set the organization to which the static business role must belong:

---



---

**Note:** By default, the static business role that you create belongs to the organization that you select in Step 3. If you want to change the organization to which the role must belong, then perform the instructions in this step.

---



---

- a. In the Reporting Org field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the organization that you want to select.  
A list of all organizations that meet the search criterion is displayed.
  - c. From this list, select the organization to which the static business role must belong, and then click **OK**.
14. If you want to set an eligibility rule, then:
- a. Click the **Grant Policy** tab.
  - b. In the text field, enter the eligibility rule in XML. See [Chapter 7, "Building Membership and Eligibility Rules"](#) for information about building rules using XML.
15. If you want to map IT roles to the static business role:
- a. Click the **Mappings** tab.
  - b. Click **Map IT Role**.
  - c. On the page that is displayed, specify the search criterion for the IT roles that you want to map. These are the IT roles that have already been created.  
A list of all IT roles that meet the search criterion is displayed.
  - d. From this list, select an IT role, and then click **OK**.  
A message indicating that the IT role has been mapped to the static business role is displayed.
  - e. Repeat Steps b through d for each IT role that you want to map.
16. Click **Submit**.  
A message indicating that the role has been created is displayed.

## 5.1.2 Granting and Revoking Static Business Roles

---



---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Business Role objects and All for Person objects
  - Grant Business Role objects and Grant Person objects
  - All for Business Role objects and Grant Person objects
  - Grant Business Role objects and All for Person objects
- 
- 

**To grant or revoke a static business role:**

1. On the first-level navigation bar, click **Organizations & People**.

2. Click **People**.
3. To search for the person to whom you want to grant a static business roles, perform one of the following:
  - Right-click **People** and then click **Search**.
  - Right-click the reporting organization to which the person belongs, and then click **Search**.
4. On the People page, specify the search criterion for the person to whom you want to grant a static business role.

A list of all persons who meet the search criterion is displayed.
5. To display the details of the person, click the View/Edit icon in the row for the person.
6. Click the **Business Roles** tab.
7. If you want to revoke the static business role grant for a particular person, then:
  - a. Click the Delete icon in the row for the static business role.
  - b. On the page that is displayed, click **OK** to confirm that you want to revoke the static business role grant.

A message indicating that the role grant was successfully deleted is displayed.
  - c. Proceed to Step 13.
8. If you want to check whether the static business role has already been granted to the person, then specify the search criterion for the static business role and click **Filter**. If the static business role is displayed, then it implies that this role has already been granted to the person. Therefore, you need not perform the remaining steps in this section.
9. Click **Grant Role**.
10. On the page that is displayed, specify a search criterion for the static business role that you want to grant.

A list of all static business roles that meet the search criterion is displayed.
11. From this list, select the static business role that you want to grant, and then click **Next**.
12. If you want to set SOC to all organizations in the hierarchy (selected in Step 7 of the "[Creating Static Business Roles](#)" on page 5-1 section), then select **Set Sphere of Control to All Organizations in the Hierarchy**, and click **Finish**. Alternatively, if you want to set the scope of the grant to a specific organization within the hierarchy to which the static business role belongs, then:
  - a. Select **Pick a Single Organization in the Hierarchy**.
  - b. Click **Next**.
  - c. Specify a search criterion for the organization to which you want the grant to be limited.

A list of all organizations that meet the search criterion is displayed.
  - d. From this list, select the organization and then click **Finish**.
13. Click **Submit**.

A message indicating that the person's information has been updated is displayed.



### 5.1.3 Delegating Static Business Roles

You can delegate a static business role only if it was created with the Role Is Delegatable option selected. You select this option while performing Step 10 of the procedure described in "[Creating Static Business Roles](#)" on page 5-1.

Delegating roles enables you to distribute role administration across users in your enterprise. The status of the role (active or inactive) does not affect its ability to be delegated.

A person who has received a role through delegation can delegate the same role to another person.

Suppose Angelyn, a Senior Manager of Corporate Security delegates the `Compliance Officer` static business role to Roger, a Manager in the audits department. Roger can delegate the `Compliance Officer` static business role to Sharon, an auditor in his team which enables her to monitor and ensure compliance with official regulations within Roger's team.

---



---

**Note:** You can delegate only static business roles. However, static business roles cannot be delegated if SOC is defined.

---



---

#### To delegate a static business role:

---



---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Business Role objects and All for Person objects
  - Delegate Business Role objects and Delegate Person objects
- 
- 

1. On the first-level navigation bar, click **Organizations & People**.
2. On the left pane, perform one of the following:
  - Right-click **People** and then click **Search**.
  - Right-click the reporting organization within which the person to whom you want to delegate the static business roles exists, and then click **Search**.
3. On the People page, specify a search criterion for the person whose static business role must be delegated.  
A list of all persons in the organization who satisfy the search criterion is displayed.
4. To display the details of the person, click the View/Edit icon in the row for the person.
5. Click the **Business Roles** tab.
6. Specify a search criterion for the role that you want to delegate.  
A list of all roles that meet the search criterion is displayed.
7. From this list, click the Delegate icon in the Actions column for the static business role that you want to delegate.
8. On the page that is displayed, specify a search criterion for the person to whom you want to delegate the static business role.

A list of all persons who meet the search criterion is displayed.

9. From this list, select the person to whom you want to delegate the static business role, and then click **OK**.

A message indicating that the static business role has been delegated is displayed.

10. Click **Submit**.

A message indicating that the person information has been updated is displayed.

## 5.2 Dynamic Business Roles

As discussed in the preceding chapter, a dynamic business role depends on a membership rule to determine role membership. This rule defines the conditions under which a user is automatically granted the dynamic business role.

The following section describes the procedure to create dynamic business roles in Oracle Role Manager.

### 5.2.1 Creating Dynamic Business Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Business Role objects
  - Manage Business Role objects
- 
- 

**To create a dynamic business role:**

1. On the first-level navigation bar, click **Roles**.
2. Click **Business Roles**.
3. On the left pane, right-click the organization where you want to create the dynamic business role, and then click **New Business Role**.
4. In the Business Role Type box, select **Dynamic**, and then click **Submit**.  
The New Business Role page is displayed in the right pane of the screen.
5. In the **Display Name** field on the Attributes tab of the New Business Role page, type the name of the dynamic business role being created.
6. If you want to enter a unique name for the dynamic business role, then enter it in the **Unique Name** field.
7. If you want to enter a description for the dynamic business role, then enter it in the **Description** field.
8. If you want to enter the responsibilities of the dynamic business role, then enter it in the **Responsibilities** field.  
For example, the responsibilities of the `Senior Accounting` dynamic business role are to define and enforce accounting policies.
9. In the Status box, select the status of the role being created.
10. If you want to set an owner for the dynamic business role, then:
  - a. In the Owner field, click **Edit**.

- b. On the page that is displayed, specify the search criterion for the person whom you want to set as the owner of the dynamic business role.  
A list of persons who meet the search criterion is displayed.
    - c. From this list, select the person whom you want to set as the owner, and then click **OK**.
11. To set the organization to which the dynamic business role must belong:
 

---



---

**Note:** By default, the dynamic business role that you create belongs to the organization that you select in Step 3. If you want to change the organization to which the role must belong, then perform the instructions in this step.

---



---

  - a. In the Reporting Org field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the organization that you want to select.

---



---

**Note:** This is the organization within which the dynamic business role is listed after it is created.

---



---

A list of all organizations that meet the search criterion is displayed.

  - c. From this list, select the organization and then click **OK**.
12. To set a membership rule, do the following:
  - a. Click the **Grant Policy** tab.
  - b. In the field, type the membership rule using XML. See [Chapter 7, "Building Membership and Eligibility Rules"](#) for information about building rules using XML.
13. If you want to check the list of members who will be automatically granted the role that is being created, then click the **Members** tab, specify the search criterion based on the membership rule created in the Grant Policy tab, and then click **Recalculate Membership**.
14. If you want To map IT roles to the dynamic business role:
  - a. Click the **Mappings** tab.
  - b. Click **Map IT Role**.
  - c. On the page that is displayed, specify the search criterion for the IT roles that you want to map. These are the IT roles that have already been created.  
A list of all IT roles that meet the search criterion is displayed.
  - d. From this list, select an IT role, and then click **OK**.  
A message indicating that the IT role has been mapped to the dynamic business role is displayed.
  - e. Repeat Steps b through d for each IT role that you want to map.
15. Click **Submit**.  
A message indicating that the role has been created is displayed.



---

---

## Working with Approver Roles

This chapter discusses the procedure to create and manage approver roles. It discusses the following topics:

- [Creating Approver Roles](#)
- [Assigning Approvers to Approver Roles](#)
- [Deleting Approver Roles](#)

### 6.1 Creating Approver Roles

As discussed in the preceding chapter, an approver role is a collection of approvers. Approver roles depend on membership rules to determine role memberships.

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Approver Role objects
  - Manage Approver Role objects
- 
- 

**To create an approver role:**

1. On the first-level navigation bar, click **Roles**.
2. Click **Approver Roles**.
3. On the left pane, right-click the organization where you want to create the approver role, and then click **New Approver Role**.
4. In the **Display Name** field on the Attributes tab of the New Approver Role page, type the name of the approver role that you are creating.
5. If you want to enter a unique name for the approver role, then enter it in the **Unique Name** field.
6. If you want to enter a description for the approver role, then enter it in the **Description** field.

For example, the Description field of the `Expense Reports Approver` approver role can be as follows:

The Expense Report Approver role is given to members of the accounting teams who approve expenses incurred by an employee for official purpose.

7. In the Status box, select the status of the approver role.

8. If you want to set an owner for the approver role, then:
  - a. In the Owner field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the person whom you want to set as the owner of the approver role.

A list of persons who meet the search criterion is displayed.
  - c. From this list, select the person whom you want to set as the owner, and then click **OK**.
9. To set the organization to which the approver role must belong:

---

---

**Note:** By default, the approver role that you create belongs to the organization that you select in Step 3. If you want to change the organization to which the role must belong, then perform the instructions in this step.

---

---

- a. In the Reporting Org field, click **Edit**.
  - b. On the page that is displayed, specify the search criterion for the organization that you want to select.

A list of all organizations that meet the search criterion is displayed.
  - c. From this list, select the organization and then click **OK**.
10. Click **Submit**.

A message indicating that the role has been created is displayed.

## 6.2 Assigning Approvers to Approver Roles

---

---

**Note:** The procedure described in this section must be performed only after the approver role to which the users must be assigned has been created. In addition, you must be a member of a system role containing one of the following system privileges, to perform the procedure described in this section:

- All for Approver Role objects
  - Manage Approver Role objects
- 
- 

### To assign approvers to an approver role:

1. On the first-level navigation bar, click **Roles**.
2. Click **Approver Roles**.
3. On the left pane, right-click **Approver Roles** and then click **Search** to search for the approver role to which you want to assign approvers. Alternatively, you can right-click the reporting organization within which you want to search the approver role and then click **Search**.
4. On the Approver Roles page, specify the search criterion for the approver role to which you want to add approvers.

A list of all approver roles that meet the search criterion is displayed.

5. To display the details of the approver role, click the View/Edit icon in the row for the approver role.
6. To define an approver rule, do the following:
  - a. Click the **Grant Policy** tab.
  - b. In the field, type the approver rule using XML. See [Chapter 7, "Building Membership and Eligibility Rules"](#) for information about building rules using XML.
7. If you want to check the list of members who will be automatically granted the role that is being created, click the **Members** tab, specify the search criterion based on the membership rule created in the Grant Policy tab, and then click **Recalculate Membership**.
8. Click **Submit**.

A message indicating that the Approver role was updated is displayed.

## 6.3 Deleting Approver Roles

---

---

**Note:** To perform the procedure described in this section, you must be a member of a system role containing one of the following system privileges:

- All for Approver Role objects
  - Manage Approver Role objects
- 
- 

### To delete an approver role:

1. On the first-level navigation bar, click **Roles**.
2. On the left pane, perform one of the following:
  - Right-click **Approver Roles** and then click **Search**.
  - Right-click the reporting organization within which you want to search the approver role that you want to delete, and then click **Search**.
3. On the Approver Roles page, specify the search criterion for the approver role that you want to delete.

A list of all approver roles that meet the search criterion is displayed.

4. Click the Delete icon in the row for the approver role that you want to delete.

A dialog box prompting you to confirm if you want to delete the approver role is displayed.

5. Click **OK**.

A message indicating that the approver role was deleted successfully is displayed.





---

## Building Membership and Eligibility Rules

You use XML to create membership rules and eligibility rules. Membership and eligibility rules are used while creating roles. This chapter describes the various elements used to build rules using XML.

The XML files located in the `ORM_HOME/samples/role_expressions` directory contain sample rules for your reference.

As mentioned earlier, the standard data model consists of objects, which are required for Oracle Role Manager to function as designed. Examples of objects available in the standard data model of Oracle Role Manager are `organization`, `role`, `abstractOrg`, `abstractIdentity`, and so on. See [Table A-1](#) for a complete list of objects available in the standard data model of Oracle Role Manager.

**See Also:** *Oracle Role Manager Developer's Guide* for detailed information about every object in the standard data model

The `predicate` element is the root element in XML used to define rules. The XML namespace is specified as an attribute of the `predicate` element as follows:

```
<predicate xmlns=http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0
input-type="person">
```

The `predicate` element can contain any one or a combination of the expressions discussed in this chapter.

This chapter includes the following sections:

- [Section 7.1, "Attribute Expressions"](#)
- [Section 7.2, "Hierarchy Expressions"](#)
- [Section 7.3, "Relative Object Expressions"](#)
- [Section 7.4, "Role Membership Expressions"](#)
- [Section 7.5, "Logical Expressions"](#)

### 7.1 Attribute Expressions

You can use the `attribute-expression` element whenever your rule requires some constraint on the `person` object in Oracle Role Manager.

[Example 7-1](#) shows XML for a sample rule that uses an attribute expression. This rule is as follows:

All individuals whose job title is Manager.

**Example 7–1 Sample XML That Uses the Attribute Expression**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <attribute-expression>
    <attribute attribute-id="jobTitle"/>
    <equals>
      <string-constant>Manager</string-constant>
    </equals>
  </attribute-expression>
</predicate>
```

The `attribute-expression` element must contain the following:

- [attribute Element](#)
- [Comparison Operator Element](#)
- [Constant Element](#)

**attribute Element**

The `attribute` element is an empty element. An **empty element** is an element that has no content and has only attributes. In other words, an empty element does not contain child elements.

The `attribute` element has the `attribute-id` attribute. The `attribute-id` attribute is a mandatory attribute, which can take values with respect to the person object.

For example, the `attribute-id` attribute can take values `givenName` (as shown in [Example 7–1](#)), `employeeNumber`, `departmentNumber`, `telephoneNumber` (as shown in [Example 7–2](#)), and so on.

See [Appendix A.1](#) for details about available values that the `attribute-id` attribute can take when the object is `person`.

**Comparison Operator Element**

All `attribute-expression` elements must contain one of the comparison operator elements described in [Table 7–1](#).

**Table 7–1 Comparison Operator Used in the attribute-expression Element**

Comparison Operator	Data Types with Which the Operator Can Be Used
<code>equals</code>	All data types
<code>not-equals</code>	All data types
<code>greater-than</code>	Integer, decimal, and datetime
<code>greater-than-equals</code>	Integer, decimal, and datetime
<code>less-than</code>	Integer, decimal, and datetime
<code>less-than-equals</code>	Integer, decimal, and datetime
<code>starts-with</code>	String
<code>ends-with</code>	String

[Example 7–1](#) and [Example 7–2](#) show attribute expressions containing the `equals` and `not-equals` comparison operator elements, respectively.

### Constant Element

You can select various constant elements depending on the attribute used. You must specify the corresponding value that the `attribute-id` attribute can take using one of the following elements:

- `integer-constant`
- `string-constant`
- `decimal-constant`
- `boolean-constant`
- `datetime-constant` (in the `YYYY-MM-DDThh:MM:ss.SSS` format, for example, `2008-06-20T15:20:00.000`)
- `null-constant`

[Example 7-1](#) and [Example 7-2](#) show attribute expressions containing the `string-constant` and `null-constant` elements, respectively.

#### **Example 7-2 Sample XML for Attribute Expression That Uses the null-constant Element**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <attribute-expression>
    <attribute attribute-id="telephoneNumber"/>
    <not-equals>
      <null-constant>null</null-constant>
    </not-equals>
  </attribute-expression>
</predicate>
```

## 7.2 Hierarchy Expressions

You can use the hierarchy expression when your rule contains an organizational hierarchy constraint. For example, you might want to create a dynamic business role that must be granted only to persons belonging to a specific organization. In this case, your rule requires a constraint on a specific organization. Therefore, you must use the hierarchy expression for creating the rule.

Begin a hierarchy expression with the `hierarchy-expression` element.

[Example 7-3](#) shows a sample XML for a rule that uses a hierarchy expression. This rule is as follows:

All individuals who are members of the Banking reporting organization and all its child organizations.

#### **Example 7-3 Sample XML That Uses the Hierarchy Expression**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <hierarchy-expression hierarchy-id="reportingHierarchy" cascade="true">
    <hierarchy-member>
      <aliased-reference
        object-type="organization"
        attribute-id="displayName"
        attribute-value="Banking"/>
    </hierarchy-member>
  </hierarchy-expression>
</predicate>
```

The `hierarchy-expression` element contains the following attributes:

- `hierarchy-id`

This is a mandatory attribute, which refers to the name of an existing hierarchy in Oracle Role Manager. It can take the values `reportingHierarchy`, `costCenterHierarchy`, and `locationHierarchy`.
- `cascade`

This is a mandatory attribute, and it can take a value of either `True` or `False`.

If the value of the `cascade` attribute is `True`, then the expression will include the specified hierarchy members and all its sub-hierarchy members.

If the value of the `cascade` attribute is `False`, then the expression will include only the specified hierarchy members.

[Example 7-3](#) shows a hierarchy expression containing the `cascade` attribute with the value `True`.

The `hierarchy-expression` element contains the `hierarchy-member` element, which in turn contains the `aliased-reference` element.

The `aliased-reference` element must contain the following attributes:

- `object-type`

This is a mandatory attribute, and it can take `abstractOrg` and all objects (such as `organization`, `ou`, `country`, and `floor`) that have been inherited from the `abstractOrg` object as its value.

See [Table A-1](#) for a complete list of objects that have been inherited from the `abstractOrg` object type.
- `attribute-id`

This is a mandatory attribute, and it can take values based on the object specified.

For example, if the value of the `object-type` attribute is `organization`, then the `attribute-id` attribute can take values such as `displayName` (as shown in [Example 7-3](#)) and `orgHead_id`.

See [Appendix A.1](#) for details about available values for the `attribute-id` attribute.
- `attribute-value`

This is also a mandatory attribute, and it can take values based on the `attribute-id` attribute specified.

For example, if the `attribute-id` is `displayName`, then `attribute-value` can take values such as `Banking`, `Marketing`, and `Financial Services`.

---



---

**Note:** The following are some points to note when using hierarchy expressions:

- Changes to the organizational hierarchies such as change of display name have no impact on the XML rule created.
  - Change in rules in response to changes in organizational hierarchy details are not dynamic.
  - Oracle Role Manager administrators who create rules must be aware of the changes that affect these rules to avoid invalidating the rule unintentionally.
- 
- 

## 7.3 Relative Object Expressions

You can use the relative object expression if you have to define a rule in terms of relationships. In other words, it is used to define relative roles. All relative object expressions contain a subject, an object, and a relationship between the two.

[Example 7-4](#) shows a sample XML for a rule that uses a relative object expression. This rule is as follows:

All people who have a manager relationship to at least one other person.

### **Example 7-4 Sample XML That Uses the Relative Object Expression**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <relative-object-expression
    subject-type="person"
    relationship-path-id="managedPeople"
    relative-object-type="person"/>
</predicate>
```

Relative object expressions begin with the `relative-object-expression` element. This element contains the following attributes:

- `subject-type`  
This is a mandatory attribute. It can take object values `organization`, `person`, and `role`.
- `relative-object-type`  
This is a mandatory attribute. It can take object values `organization`, `person`, and `role`.
- `relationship-path-id`  
This is also a mandatory attribute. It takes a value that can determine the relationship between the subject and the object. That is, it determines the relationship between the entities mentioned in the `subject-type` and the `relative-object-type` attributes.

For example, you can use the `relationship-path-id` attribute that takes the `manager` value to determine the relationship between two `person` objects.

Another example is to use the `relationship-path-id` attribute that takes the `managedPeople` value (as shown in [Example 7-4](#)) to determine people who are managers to at least one other person.

You can have relationships between a person and another person, person and roles, and organization and organization.

See [Appendix A.3](#) for details about the available relationships for various objects.

The `relative-object-expression` element can contain an `attribute-expression` element as its child element. The behavior of an `attribute-expression` element in the `role-member-expression` element and the `attribute-expression` element (described in "[Attribute Expressions](#)" on page 7-1) is similar. However, the `attribute-expression` element when used independently, considers only `person` as the object type. The `attribute-expression` element when used with the `role-membership-expression` element considers the value that is specified in the `relative-object-type` attribute as the object type.

For example, you might want to create a role that must be granted to persons who have a manager named John. Therefore, there is a relationship that exists between John and the persons to whom you want to grant the role.

[Example 7-5](#) shows a sample XML for a rule that uses a relative object expression with the attribute expression as the child element. This rule is as follows:

All people who have a manager by the name Jane Doe.

**Example 7-5 Sample XML That Uses the Relative Object Expression and the Attribute Expression Element**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <relative-object-expression
    subject-type="person"
    relationship-path-id="manager"
    relative-object-type="person">
    <attribute-expression>
      <attribute attribute-id="displayName"/>
      <equals>
        <string-constant>Jane Doe</string-constant>
      </equals>
    </attribute-expression>
  </relative-object-expression>
</predicate>
```

For example, you might want to create a rule that will grant a person membership to a dynamic business role, based on the person's location.

[Example 7-5](#) shows a sample XML for a rule that uses a relative object expression. In addition, this rule depicts a relationship between a person and a location. This rule is as follows:

All people who reside in the Americas location.

**Example 7-6 Sample XML That Uses the Relative Object Expression to Depict the Person-Organization Combination**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <relative-object-expression
    subject-type="person"
    relationship-path-id="parent_location_organization"
    relative-object-type="abstractOrg">
    <attribute-expression>
      <attribute attribute-id="displayName"/>
    </attribute-expression>
  </relative-object-expression>
</predicate>
```

```

    <equals>
      <string-constant>Americas</string-constant>
    </equals>
  </attribute-expression>
</relative-object-expression>
</predicate>

```

## 7.4 Role Membership Expressions

Role membership expressions are used when you have to define a rule that considers members of another role, which is a static business role.

---



---

**Note:** Role membership expressions must be used for static role references only.

---



---

Role membership expressions are also used when you are referencing a role attribute and verifying whether a person is a member of the resulting set of roles. This is illustrated by the following example:

Suppose you are creating an XML rule for a dynamic business role. This XML rule grants the dynamic business role to all individuals whose job title is Manager and have membership to the Risk Manager static business role.

A sample XML for the example in the preceding section is shown in [Example 7-7](#). This rule uses the `role-member-expression` element.

### **Example 7-7** Sample XML That Uses the Role Membership Expression

```

<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <and-expression>
    <expressions>
      <attribute-expression>
        <attribute attribute-id="jobTitle"/>
        <equals>
          <string-constant>Manager</string-constant>
        </equals>
      </attribute-expression>
      <role-member-expression>
        <aliased-reference
          object-type="abstractRole"
          attribute-id="displayName"
          attribute-value="Risk Manager"/>
      </role-member-expression>
    </expressions>
  </and-expression>
</predicate>

```

Role membership expressions begin with the `role-member-expression` element. This element contains the `aliased-reference` element. The behavior of the `aliased-reference` element in the `role-member-expression` element and the `hierarchy-expression` element is the same. See [Section 7.2, "Hierarchy Expressions"](#) for information about `aliased-reference` element.

## 7.5 Logical Expressions

Logical expressions can be formed by using the logical operators `and`, `or`, and `not`. Logical expressions enclose all the primary expressions such as attribute expressions, hierarchy expressions, role membership expressions, and relative object expressions.

You can use a logical expression when you have to use a combination of two or more primary expressions.

The logical expression elements that are available are as follows:

- `and-expression`
- `or-expression`
- `not-expression`

Each of these logical expression elements, except for the `not-expression` element, must contain the `expressions` element because the `and`, and `or` logical operators require two operands.

[Example 7-8](#) is a sample XML for a rule that automatically grants a dynamic business role to all individuals in the Accounting subtree of the reporting organization and who are managed by a person named John:

### **Example 7-8 Sample XML That Uses the Logical Expression**

```
<predicate xmlns="http://xmlns.oracle.com/iam/rm/rule/predicate/config/1_0"
input-type="person">
  <and-expression>
    <expressions>
      <hierarchy-expression hierarchy-id="reportingHierarchy" cascade="true">
        <hierarchy-member>
          <aliased-reference
            object-type="organization"
            attribute-id="displayName"
            attribute-value="Accounting" />
        </hierarchy-member>
      </hierarchy-expression>
      <relative-object-expression
        subject-type="person"
        relationship-path-id="manager"
        relative-object-type="person">
        <attribute-expression>
          <attribute attribute-id="givenName" />
          <starts-with>
            <string-constant>John</string-constant>
          </starts-with>
        </attribute-expression>
      </relative-object-expression>
    </expressions>
  </and-expression>
</predicate>
```



---

---

## About the XML Schema Definition

This appendix lists all the elements that are valid according to the schema definition and the various attributes that are valid for each element. It also lists the set of values that each of these attributes can take.

The elements along with their attributes and attribute values are explained here for easy reference. For complete XML schema information, refer to:

- `oracle.iam.rm.rule.predicate.config_1_0.xsd`

**To access the XML schema:**

1. Navigate to the `ORM_HOME\lib` directory.
2. Extract the contents of the `server.jar` file into a temporary location using any unzip utility or the jar command-line tool, which is part of the Sun Java Development Kit.
3. From the temporary location, navigate to `META-INF\schemas`.

This directory contains the `oracle.iam.rm.rule.predicate.config_1_0.xsd` file.

- `standard.xml`

The `standard.xml` file contains the standard data model that supports the Oracle Role Manager user interface.

**To access the standard.xml file:**

1. Navigate to the `ORM_Home\config` directory.
2. Extract the contents of the `standard.car` file into a temporary location using any unzip utility or the jar command-line tool, which is part of the Sun Java Development Kit.
3. From the temporary location, navigate to the `config\oracle.iam.rm.temporal` directory.

This directory contains the `standard.xml` file.

---

---

**Note:** If there are customizations to the Oracle Role Manager sample data model, then all the attributes in this appendix can take user-defined values as per the customizations made in the XSD.

---

---

Topics in this appendix include:

- [Section A.1, "Attribute Expressions"](#)

- [Section A.2, "Hierarchy Expressions"](#)
- [Section A.3, "Relative Object Expressions"](#)
- [Section A.4, "Role Membership Expressions"](#)

## A.1 Attribute Expressions

The `attribute-expression` element has the attributes `object-type` and `attribute-id`.

The `attribute-id` attribute takes values based on the value of the `object-type` attribute specified in the `attribute-expression` element.

[Table A-1](#) lists the `object-type` attributes and its corresponding `attribute-id` values. The `Inherits From` column in [Table A-1](#) gives the name of the supertype from which the `object-type` attribute mentioned in `object-type` column is inherited.

**See Also:** *Oracle Role Manager Developer's Guide* for detailed information about every object

**Table A-1** *Attribute Values for object-type and attribute-id*

<b>object-type</b>	<b>Inherits From</b>	<b>Values for attribute-id</b>
<code>abstractIdentity</code>	NA	<code>displayName</code> <code>locale</code> <code>status</code> <code>uniqueName</code> <code>userID</code> <code>userPassword</code>

**Table A-1 (Cont.) Attribute Values for object-type and attribute-id**

object-type	Inherits From	Values for attribute-id
person	abstractIdentity	<p>All values for the attribute-id attribute of the abstractIdentity object-type (listed earlier in this table).</p> <p>In addition, it can take the following values:</p> <p>audio  businessCategory  carLicense  costCenterOrg_id  departmentNumber  description  destinationIndicator  employeeNumber  employeeType  fax  givenName  homePhone  homePostalAddress  initials  internationalISDNNumber  jobTitle  jpegPhoto  l (<b>Note:</b> This attribute-id attribute refers to theLDAP attribute for the locality of the person)  locationOrg_id  mail  manager_id  mobile  pager  photo  physicalDeliveryOfficeName  postalAddress  postalCode  postOfficeBox  preferredDeliveryMethod  preferredLanguage  registeredAddress  reportingOrg_id  roomNumber  seeAlso  sn (<b>Note:</b> This refers to the surname of the person)  st  street  telephoneNumber  telexNumber  userCertificate  userSMIMECertificate  x121Address</p>
abstractOrg	NA	<p>costCenterHierarchyRoot_id  costCenterOrg_id  description  displayName  locationHierarchyRoot_id  locationOrg_id  orgHead_id  reportingHierarchyRoot_id  reportingOrg_id  uniqueName</p>

**Table A-1 (Cont.) Attribute Values for object-type and attribute-id**

<b>object-type</b>	<b>Inherits From</b>	<b>Values for attribute-id</b>
building	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  buildingName postalAddress telephoneNumber
country	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  c ( <b>Note:</b> This attribute-id attribute refers to the two-letter country code to which the organization belongs.)
division	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).
dcObject	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).
floor	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  floorIdentifier
locality	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  l ( <b>Note:</b> This attribute-id attribute refers to the LDAP attribute.) seeAlso st street
organization	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  businessCategory destinationIndicator fax internationalISDNNumber l ( <b>Note:</b> This attribute-id attribute refers to the LDAP attribute for the locality of the organization) physicalDeliveryOfficeName postalAddress postalCode postOfficeBox preferredDeliveryMethod registeredAddress seeAlso st street telephoneNumber telexNumber x121Address

**Table A-1 (Cont.) Attribute Values for object-type and attribute-id**

<b>object-type</b>	<b>Inherits From</b>	<b>Values for attribute-id</b>
ou (Note: This object-type attribute refers to an organizational unit)	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  businessCategory destinationIndicator fax internationalISDNNumber l physicalDeliveryOfficeName postalAddress postalCode postOfficeBox preferredDeliveryMethod registeredAddress seeAlso st street telephoneNumber telexNumber x121Address
room	abstractOrg	All values for the attribute-id attribute of the abstractOrg object-type (listed earlier in this table).  roomNumber seeAlso telephoneNumber
abstractRole	NA	costCenterOrg_id description displayName eligibilityRule isDelegatable locationOrg_id membershipRule reportingOrg_id roleType simpleDynamic socHierarchy_id status uniqueName
approverRole	abstractRole	All values for the attribute-id attribute of the abstractRole object-type (listed earlier in this table).  roleOwner_id
businessRole	abstractRole	All values for the attribute-id attribute of the abstractRole object-type (listed earlier in this table).  responsibility roleOwner_id
itRole	abstractRole	All values for the attribute-id attribute of the abstractRole object-type (listed earlier in this table).  roleOwner_id

**Table A-1 (Cont.) Attribute Values for object-type and attribute-id**

object-type	Inherits From	Values for attribute-id
systemRole	abstractRole	All values for the attribute-id attribute of the abstractRole object-type (listed earlier in this table).  roleOwner_id

## A.2 Hierarchy Expressions

As discussed in the preceding chapter, the `hierarchy-expression` element contains the `hierarchy-member` element. This element in turn contains the `aliased-reference` element.

The `aliased-reference` element uses the attributes `object-type` and `attribute-id`. The `object-type` attribute can take the values `abstractOrg` and its inherited object types. For a corresponding list of values that these `object-type` attributes can take, see [Table A-1](#).

## A.3 Relative Object Expressions

You can use the `relative-object-expression` element to determine approver roles. It contains the attributes `subject-type`, `relationship-path-id`, and `relative-object-type`. The `subject-type` and `relative-object-type` attributes take the values `organization`, `person`, and `role`. However, the `relationship-path-id` attribute takes a value depending on the `subject-type` and `relative-object-type` attributes. You can have various `subject-type` and `relative-object-type` combinations such as `person-person`.

[Table A-2](#) lists the values that the `relationship-path-id` attribute takes when a `person-person` combination is used.

**Table A-2 Attribute Values for relationship-path-id**

Combination	relationship-path-id Attributes
person-person	managedPeople manager secretarialClients secretary
person-organization	orgHead headedOrgs
person-itRole	roleOwner ownedITRoles
person-systemRole	roleOwner ownedSystemRoles
person-businessRole	roleOwner ownedBusinessRoles
person-approverRole	roleOwner ownedApproverRoles

**Table A-2 (Cont.) Attribute Values for relationship-path-id**

Combination	relationship-path-id Attributes
abstractOrg-abstractOrg	parent_reporting_organization child_reporting_organization parent_location_organization child_location_organization parent_cost_center_organization child_cost_center_organization

## A.4 Role Membership Expressions

As discussed in the preceding chapter, the `role-member-expression` element contains the `aliased-reference` element.

The `aliased-reference` element uses the attributes `object-type` and `attribute-id`. The `object-type` attribute can take the values `abstractRole` and its inherited object types. For a corresponding list of values that these `object-type` attributes can take, see [Table A-1](#).





---

---

# Index

## A

---

approver roles, 1-12  
    creating, 6-1  
    deleting, 6-3  
approvers, 1-12  
attribute expressions, 7-1, A-2  
attributes  
    attribute-id, 7-2, 7-4  
    attribute-value, 7-4  
    cascade, 7-4  
    hierarchy-id, 7-4  
    object-type, 7-4  
    relationship-path-id, 7-5  
    relative-object-type, 7-5  
    subject-type, 7-5  
audit information, 1-2, 1-3

## C

---

compliance reporting, 1-2, 1-5  
cost center hierarchies, 1-3  
cost centers  
    creating, 2-6  
    deleting, 2-16  
    modifying, 2-15  
creating  
    approver roles, 6-1  
    dynamic business roles, 5-6  
    IT privileges, 4-1  
    IT roles, 4-3  
    static business roles, 5-1  
    system roles, 3-8

## D

---

delegating  
    IT roles, 4-7  
    static business roles, 5-5  
deleting  
    approver roles, 6-3  
    IT privileges, 4-2  
    IT roles, 4-8  
    system roles, 3-13

## E

---

eligibility rules, 1-7, 5-3  
    *See also* rules

## G

---

grantee, 1-8  
granting  
    IT roles, 4-6  
    static business roles, 5-3, 5-4  
    system roles, 3-12

## H

---

Health Insurance Probability and Accountability  
    Act, 1-3  
hierarchies  
    *See* organizational hierarchies  
hierarchy expressions, 7-3, A-6  
HIPAA, 1-3

## I

---

identity management systems  
    provisioning systems, 1-1, 1-2, 1-3, 1-5  
    role management systems, 1-1, 1-2  
integration with provisioning systems, 1-5  
IT privileges, 1-8  
    creating, 4-1  
    modifying, 4-2  
IT roles, 1-8, 4-3  
    delegating, 4-7  
    granting, 4-6

## L

---

layout of pages in UI, 2-2  
location hierarchies, 1-3  
locations  
    creating, 2-6  
    deleting, 2-16  
    modifying, 2-15  
log in to Oracle Role Manager, 2-1  
logical expressions  
    and, 7-8  
    not, 7-8

or, 7-8

## M

---

### mapping

- IT privileges, 4-5
  - system privileges, 3-10, 3-11
- membership lists, 1-6
- membership rules, 1-6, 1-7, 5-7
- See also* rules
- modifying IT privileges, 4-2

## N

---

### navigation options

- Administration, 2-20
- Home, 2-3
- Organizations & People, 2-5
- Roles, 2-18

## O

---

objects, 1-13

Oracle Identity Manager, 1-5

### organizational hierarchies

- cost centers, 1-3
- locations, 1-3
- reporting, 1-3

## P

---

page layout, UI, 2-2

### persons

- creating, 2-9
- deleting, 2-18
- modifying, 2-15

polyarchy, 1-3

*See also* organizational hierarchies

### predefined system roles, 3-1

- auditor, 3-7
- cost center administrators, 3-5
- location administrators, 3-6
- reporting organization administrators, 3-4
- role administrators, 3-2, 3-3
- role delegation administrators, 3-7
- role grant administrators, 3-4
- system administrator, 3-2
- system role administrators, 3-2
- system role grant administrators, 3-2
- user administrators, 3-6

### privileges, 1-1

- IT privileges, 1-8
- system privileges, 1-13

### procedures

- assigning approver roles, 6-2
- creating
  - IT privileges, 4-1
  - IT roles, 4-4
- creating approver roles, 6-1
- creating dynamic business roles, 5-6
  - mapping IT roles, 5-7

- setting an owner, 5-6
  - setting membership rules, 5-7
  - setting the organization, 5-7
- creating IT roles, 4-3
- creating static business roles, 5-1, 6-1
- mapping IT roles, 5-3
  - setting an owner, 4-3, 5-2, 6-2
  - setting eligibility rules, 5-3
  - setting the organization, 4-4, 5-2, 6-2
  - setting the sphere of control, 5-2
- creating system roles
- granting system roles, 3-10
  - mapping system privileges, 3-9
  - setting an owner, 3-9
  - setting the organization, 3-9
  - setting the sphere of control, 3-8
  - setting the status, 3-9
- delegating
- IT roles, 4-7
  - static business roles, 5-5
- deleting
- approver roles, 6-3
  - IT privileges, 4-2
  - IT roles, 4-8
- granting
- IT roles, 4-6
  - static business roles, 5-3, 5-4
  - system roles, 3-10, 3-12
- mapping
- IT privileges, 4-5
  - system privileges, 3-11
- modifying IT privileges, 4-2
- revoking
- IT roles, 4-6
  - system roles, 3-12
- unmapping
- IT privileges, 4-5
  - system privileges, 3-11
- provisioning systems, 1-1, 1-2, 1-3, 1-5

## R

---

### RBAC

*See* role-based access control

relative object expressions, 7-5, A-6

reporting hierarchies, 1-3

### reporting organizations

- creating, 2-6
- deleting, 2-16
- modifying, 2-15

### revoking

- IT roles, 4-6
- static business roles, 5-3
- system roles, 3-12

role delegation, 1-4, 4-7, 5-5

role lifecycle management, 1-2

role management systems, 1-1, 1-2

role membership expressions, 7-7, A-7

### role status

- active, 1-5

- inactive, 1-5
- role-based access control, 1-3
- roles
  - approver roles, 1-12
  - business roles, 1-6
    - dynamic, 1-6
    - static, 1-7
  - IT roles, 1-8
  - system roles, 1-13
- rules
  - eligibility, 1-7
  - membership, 1-6, 1-7, 1-12

- not-expression, 7-8
- or-expression, 7-8
- predicate, 7-1
- relative-object-expression, 7-5
- role-membership-expression, 7-7

XML expressions

- attribute expressions, 7-1, A-2
- hierarchy expressions, 7-3, A-6
- relative object expressions, 7-5, A-6
- role membership expressions, 7-7, A-7

## S

---

- sample data, 1-4, 1-15, 3-1
- Sarbanes-Oxley Act, 1-3
- SOX, 1-3
- sphere of control, 1-8, 1-14
- standard model, 1-4
- standard roles
  - See* roles
- static business roles
  - creating, 5-1
  - delegating, 5-5
  - granting, 5-3
- system identities, 1-13
- system permissions, 1-13
- system privileges
  - mapping, 3-10
  - unmapping, 3-10
- system roles, 1-13
  - creating, 3-8
  - deleting, 3-13
  - granting, 3-12
  - revoking, 3-12

## T

---

- transaction, 2-4
- transaction status
  - canceled, 2-4
  - finalized, 2-4
  - pending, 2-4

## U

---

- unassigned nodes, 2-16, 2-19
- unmapping
  - IT privileges, 4-5
  - system privileges, 3-10

## X

---

- XML elements
  - and-expression, 7-8
  - attribute-expression
    - attribute, 7-2
    - comparison operators, 7-2
    - constant elements, 7-3
  - hierarchy-expression, 7-4

