Oracle® Fusion Middleware

Oracle Authorization Policy Manager Administrator’s Guide
(Oracle Fusion Applications Edition)

11*g* Release 1 (11.1.1.5.0)

E20839-01

August 2011

Oracle Fusion Middleware Oracle Authorization Policy Manager Administrator's Guide (Oracle Fusion Applications Edition), 11*g* Release 1 (11.1.1.5.0)

E20839-01

Primary Author: Carlos Subi

Contributing Author:

Contributor: Akila Natarajan, Sanatan Sahgal, Sanjeev Topiwala, Sivakumar Venugopal, and Roger Wigenstam.

Contents

4 Querying Security Artifacts

5 Managing Security Artifacts

6 Delegated Administration

7 Upgrading Oracle Fusion Applications Policies

8 Customizing the User Interface

9 Internationalization

10 Oracle Fusion Applications Data Role Templates

11 Managing Oracle Fusion Applications Data Security Policies

A Using an OpenLDAP Identity Store

B Troubleshooting Oracle Authorization Policy Manager

Index

List of Examples

List of Figures

List of Tables

Preface

This guide explains the features, configuration, and use of Oracle Authorization Policy Manager, a tool to manage global and application security artifacts.

This preface addresses the following topics:

- Audience
- Documentation Accessibility
- Related Documentation
- Conventions

Audience

The intended audience of this guide are security administrators.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documentation

Information about security administration is also found in the following documents:

- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Security and Administrator's Guide for Web Services*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*

For a comprehensive list of Oracle documentation or to search for a particular topic within Oracle documentation libraries, see `http://www.oracle.com/technology/documentation/index.html`.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action.
italic	Italic type indicates book titles, emphasis, terms defined in text, or placeholder variables for which you supply particular values.
`monospace`	Monospace type within a paragraph indicates commands, URLs, Java class names and method names, file and directory names, text that appears on the screen, or text that you enter.

1 Introduction to Oracle Authorization Policy Manager

Oracle Authorization Policy Manager is graphical interface tool to manage application authorization policies. This chapter describes the basic functionality of this tool in the following sections:

- Audience and Prerequisites
- What Is Oracle Authorization Policy Manager?
- The Big Picture

1.1 Audience and Prerequisites

The intended users of Oracle Authorization Policy Manager are security administrators.

Oracle Authorization Policy Manager requires that:

- The domain policy store be LDAP- or DB-based; the only supported LDAP policy store type is Oracle Internet Directory; the only supported DB policy store type is Oracle RDBMS. *Before* using Oracle Authorization Policy Manager, make sure that the policy store has been reassociated to any of the supported repositories. For details on reassociating the domain policy store, see *Oracle Fusion Middleware Application Security Guide*.
- The domain identity store be LDAP-based; supported identity store types are:
  - Oracle Internet Directory
  - Oracle Virtual Directory
  - WebLogic EmbeddedLDAP
  - Sun Java System Directory Service version 6.3
  - Active Directory 2003, 2008
  - Novell eDirectory 8.8
  - OpenLDAP 2.2. For the special configuration required for this type, see Appendix A, "Using an OpenLDAP Identity Store."
  - Tivoli Directory Server

  For information about Oracle Fusion Middleware Certification and Supported Configurations, visit `http://www.oracle.com/technology/software/products/ias/files/fusion_certification.html`.

- Two particular data sources be set: mds-ApplicationMDSDB and APMDBDS. The first data source can be configured with the WebLogic Console by navigating to **JDBC > Data Sources**. Table 1–1 describes the characteristics of these data sources.

Table 1–1 Required Data Sources

Data Source Name	JNDI Name	Description
mds-ApplicationMDSDB	jdbc/mds/mds-ApplicationMDSDBDS	Stores MDS-related documents used by the application.
APMDBDS	jdbc/APMDBDS	Required to use the 3-way-diff patch method.

Applications whose policies are managed with Oracle Authorization Policy Manager are assumed to use Oracle Platform Security Services for authorization. For details about integrating an application with these services, see *Oracle Fusion Middleware Application Security Guide*.

For additional data source requirements when using Data Role Templates, see Chapter 10.1, "Prerequisites for Using Templates."

1.2 What Is Oracle Authorization Policy Manager?

A security administrator can use WLST commands or Fusion Middleware Control to manage application policies. On the one hand, using WLST command requires manually running commands; on the other hand, even though Fusion Middleware Control offers a graphical user interface, it is a rather complex tool that requires that the administrator work with low-level security artifacts and know names and concepts familiar to, typically, only developers (such as permission class names or task-flow names, for example).

Oracle Authorization Policy Manager greatly simplifies the creation, configuration, and administration of application policies over those two other tools by offering:

- User-friendly names and descriptions of security artifacts; for details, see Chapter 2, "The OPSS Authorization Model."
- A way to organize application roles by business, product, or any other parameter specific to an application; for details, see Section 2.3.5, "Role Categories."
- A uniform graphic interface to search, create, browse, and edit security artifacts; for details, see Chapter 4, "Querying Security Artifacts," and Chapter 5, "Managing Security Artifacts."
- A way to specify a subset of applications that a role can manage; for details, see Chapter 6, "Delegated Administration."
- The ability to generate external roles and data security grants automatically from a template; for details, see Chapter 10, "Oracle Fusion Applications Data Role Templates."

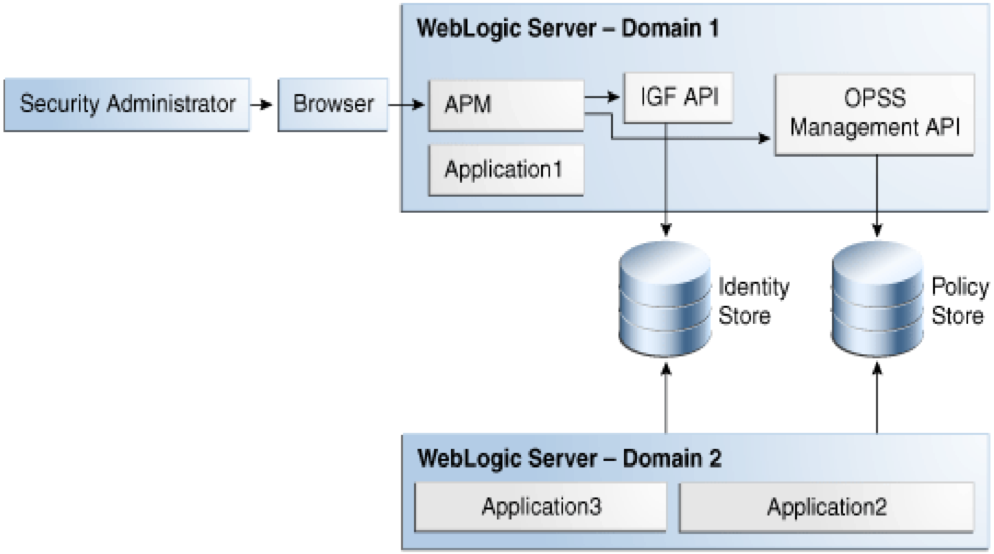
1.3 The Big Picture

Figure 1–1 illustrates how a security administrator accesses Oracle Authorization Policy Manager, and how the tool communicates with the domain policy and identity stores within the context of Oracle WebLogic server.

That figure also illustrates the fact that Oracle Authorization Policy Manager can access policies (and identities) shared by different domains. Oracle Authorization

Policy Manager uses OPSS management APIs to access the policy store and IGF APIs to access the identity store.

Figure 1–1 APM Deployed in a WebLogic Domain



Oracle Authorization Policy Manager does not support the management of users and external roles; these artifacts can only be viewed with the tool. Their provision and management is typically accomplished using Oracle Identity Manager. Changes to the identity store are immediately visible in Oracle Authorization Policy Manager.

1.3.1 Installing and Configuring Oracle Authorization Policy Manager

This section provides links to other documentation that describe the following topics:

- Installation
- High Availability
- SSL
- Loggers

1.3.1.1 Installation

For details about installing Oracle Authorization Policy Manager, see *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

1.3.1.2 High Availability

For details about high availability for Oracle Authorization Policy Manager, see *Oracle Fusion Middleware High Availability Guide*.

1.3.1.3 SSL

The connections that Oracle Authorization Policy Manager establishes with the policy store, the identity store, and the database can be secured through one-way SSL. The access to Oracle Authorization Policy Manager via a browser can also be secured through one-way SSL. These settings are similar to those of any other application running in the Oracle WebLogic server.

For details about configuring SSL in Oracle Fusion Middleware applications when OHS is not being used, see chapter 12 in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

For details about configuring SSL in Oracle Fusion Middleware applications when OHS is being used, see chapter 6 in *Oracle Fusion Middleware Administrator's Guide*.

1.3.1.4 Loggers

Setting the loggers and a log level for Oracle Authorization Policy Manager is similar to setting them for any other application running in the Oracle WebLogic server. For details, see *Oracle Fusion Middleware Application Security Guide*.

2 The OPSS Authorization Model

This chapter describes the OPSS authorization model and the security objects used in the model. These objects, which a security administrator can manage with Oracle Authorization Policy Manager, are explained in the following sections:

- The Basic Security Artifacts
- External Roles
- The Policy Model

The terms defined in this chapter are used in the Oracle Authorization Policy Manager user-interface and throughout this guide.

2.1 The Basic Security Artifacts

An *application stripe* is a logical subset of the domain policy store where the application policies are kept. Unless specified otherwise, the application stripe name is derived from the application display name: an application with display name `appName(version)` has application stripe name `appName#vers`. An application stripe can be shared by several applications.

The first distinction among security artifacts accessible with Oracle Authorization Policy Manager is between *global* and *application-specific* artifacts.

Global artifacts include users, external roles, and system policies and they apply to all application stripes. Even though system policies are stored in the domain policy store, in this release, Oracle Authorization Policy Manager does not support viewing or managing system policies. System policies are instead managed with Fusion Middleware Control, as explained in *Oracle Fusion Middleware Application Security Guide*.

Application-specific artifacts include the resource catalog, application policies, application roles, and role categories, and they apply to just an application stripe.

2.2 External Roles

An *external role* is a collection of users and other groups. The term external role is often synonymous with the terms *enterprise role* or *enterprise group*, and it is typically implemented as LDAP groups in the identity store. Similar to other kind of roles, external roles can be structured hierarchically.

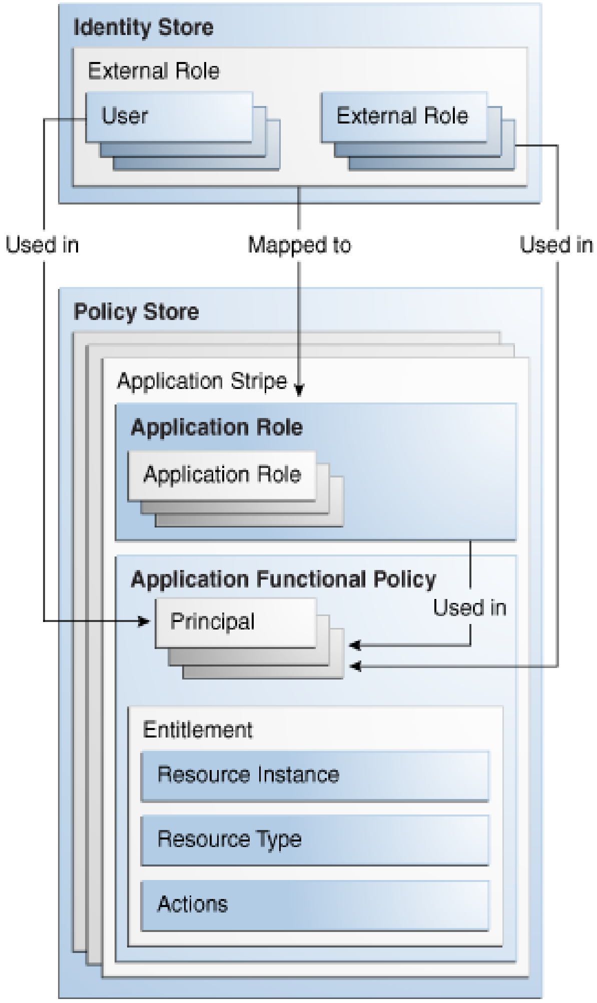
For details about the role hierarchy and permission inheritance, see *Oracle Fusion Middleware Application Security Guide*.

Note: Within Oracle Authorization Policy Manager, external roles (and users) are viewable only; they are typically managed with a different tool, such as Oracle Identity Manager. For details, see *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

2.3 The Policy Model

An application policy can be based on an entitlement (combination of resources and actions across multiple resource types) or on a set of selected resources and actions. Figure 2–1 illustrates the logical model of an entitlement-based application policy (The figure does not illustrate that external roles can be hierarchical).

Figure 2–1 Entitlement-Based Application Policy Logical Model



The components and details of an application stripe are explained in the following sections:

- Application Role
- Principal
- The Resource Catalog

2.3.1 Application Role

An *application role* is a collection of users, groups, and other application roles; it can be hierarchical. Application roles are defined by application policies and not necessarily known to a JavaEE container. Application roles can be many-to-many mapped to external roles. For example, the external group `employee` (stored in the identity store) can be mapped to the application role `helpdesk service request` (in one stripe) and to the application role `self service HR` (in another stripe).

2.3.2 Principal

A *principal* is the identity to which the authorization in the policy is granted. A principal can be a user, an external role, or an application role. Most frequently, it is an application role.

2.3.3 The Resource Catalog

The resource catalog comprises resource types, resources, actions, and entitlements.

2.3.3.1 Resource Type

A *resource type* represents the type of a secured artifact. UI artifacts, such as ADF Taskflows, pages, buttons, fields, web services, reports, URLs, and scheduled jobs, are examples of resource types. Essentially, a resource type is a template for creating resources.

A resource type is associated with one Java class (the matcher class) that describes the actions that can be invoked on instances of the resource type. For example, for the resource type ADF Taskflow, the permission class allows Viewing or Customizing task-flows.

The following points apply to the specification of a resource type:

- The name is required and case insensitive.
- The matcher class name is required and case insensitive. Typically, the matcher class is the provided OPSS class `ResoucePermission`, although it can be a custom class. If two or more resource types are to share a matcher class, then that class must be either the class `ResourcePermission`, or a class extending the abstract class `AbstractTypedPermission`, or a class implementing the class `TypePermission` and extending the class `java.security.Permission`. For further details about the matcher class, see *Oracle Fusion Middleware Application Security Guide*.
- The description string is optional and case insensitive.
- The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in Oracle Authorization Policy Manager, and it provides extra information that helps security administrators identify artifacts.

- The list of actions is optional, case sensitive, and can be empty. An empty action list indicates that the actions on instances of the resource type are determined externally and are opaque to Oracle Authorization Policy Manager, that is, that they are not relevant for resources of this type (in which case the resource is treated as a named resource).

For details about creating a resource type, see Section 5.1.2, "Managing Application Resource Types."

An *action* is tied to a resource type and defines an operation allowed on a resource. The matcher class associated with a resource type typically describes the list of actions for the resource type. The following are some examples of actions on resources:

- Get or post, on a URL.
- Read, write, copy, edit, or delete, on a file.
- Deposit, withdraw, view balance, view history, transfer to savings, or transfer from savings, on a checking bank account.

2.3.3.2 Resource

A *resource* or *resource instance* is an instance of a resource type that represents a concrete resource; it defines an application resource that can be secured by a policy, such as URLs, EJBs, JSPs. At runtime, the application passes the resource name to have permissions checked to determine whether a principal is authorized.

A resource requires an associated resource type, and it can exist independent of entitlements. Note the following points about the case sensitivity of the various strings in a resource specification:

- The name is required and case sensitive. At runtime, this is the name that the application passes to the have permissions checked to determine whether a user is authorized.
- The description is optional and case insensitive.
- The display name is required and case insensitive. Specifying a meaningful display name is recommended since it is displayed in Oracle Authorization Policy Manager, and it provides extra information that helps security administrators identify artifacts.

For details about creating a resource, see Section 5.1.3, "Managing Application Resources."

2.3.3.3 Permission and Entitlement

A *permission* aggregates a class, resources, and, for each resource, a subset of the actions allowed by the type of the resource.

An *entitlement or permission set* represents a small set of resources and privileges needed to perform a task, that is, it groups related resources, possibly of different types, needed to perform a business function. Entitlements are reusable collections of permissions that can be granted to multiple principals.

For example, the entitlement Maintain Purchase Orders groups the following resources:

```
Resource Type: ADF Taskflow
Resource: PO Summary
Action: view

Resource Type: ADF Taskflow
```

```
Resource: PO Details
Action: view

Resource Type: ADF Taskflow
Resource: Supplier Details
Action: view

Resource Type: Web Service
Resource: SpendingLimitCheckWS
Action: invoke

Resource Type: Workflow
Resource: POApproval
Action: submit
```

Note the following points about the case sensitivity of the various strings in an entitlement specification:

- The name is required and case insensitive.
- The description is optional and case insensitive.
- The display name is required and case insensitive. Specifying a meaningful display name is recommended since it is displayed in Oracle Authorization Policy Manager, and it provides extra information that helps security administrators identify artifacts.

For details about creating an entitlement, see Section 5.1.4, "Managing Application Entitlements."

2.3.4 Application Policy

An *application policy* is a functional policy that specifies a set of permissions that an entity (the grantee, a principal or code source) is allowed within an application, such as viewing web pages or modifying reports. That is, it specifies who can do what in an application.

An application policy uses:

- Principals as grantees, and must have at least one principal (Note that, in this release of Oracle Authorization Policy Manager, code sources are *not* allowed as grantees).
- Either one or more permissions, or an entitlement, but not both. Policies that use an entitlement are called *entitlement-based policies*; policies that use one or more permissions are called *resource-based policies*.

The application policy model is illustrated in Figure 2–1.

Oracle Authorization Policy Manager provides a rich user interface that allows security administrators to query, provision, and manage application policies. For details, see Chapter 4, "Querying Security Artifacts," and Chapter 5, "Managing Security Artifacts."

> **Note:** Entitlement-based policies correspond closely with business functions. They are recommended in cases in which a business function considers securing a collection of resources; an entitlement can be used in one or more grants.

2.3.5 Role Categories

A role category is a collection of application roles. Role categories allow administrators organizing application roles in arbitrary flat collections. Role categories are not used in policy evaluations at runtime.

Role categories are *independent* of (and should not be confused with) the role hierarchy, which applies to both application and external roles. For details about the role hierarchy and permission inheritance, see *Oracle Fusion Middleware Application Security Guide*.

Role category names are case insensitive. For details about creating a role category, see Section 5.1.6, "Managing Application Role Categories."

3

Getting Started with Oracle Authorization Policy Manager

Oracle Authorization Policy Manager user interface uses the following general operational principle: first the administrator identifies a security object (by browsing or searching), and then, once the object has been selected, he chooses one of the operations available on it.

This chapter describes the major tabs, the navigation panel, how to use the navigation panel to carry out simple queries on various artifacts, the online help system, and some frequent uses of Oracle Authorization Policy Manager.

This information is presented in the following sections:

- The Three Major Tabs
- The Welcome Page
- The Navigation Panel
- Finding Artifacts with a Simple Search
- Online Help
- Some Frequently Used Operations

3.1 The Three Major Tabs

Oracle Authorization Policy Manager contains the following four major tabs:

- The Authorization Management Tab
- The System Configuration Tab
- The Policy Upgrade Management Tab

3.1.1 The Authorization Management Tab

The Authorization Management tab is used to search and maintain security artifacts. For details, see Chapter 4, "Querying Security Artifacts," and Chapter 5, "Managing Security Artifacts."

3.1.2 The System Configuration Tab

The System Configuration tab is used to specify delegated administrators, that is, to define the external roles that can manage a prescribed set of applications. For details, see Chapter 6, "Delegated Administration."

3.1.3 The Policy Upgrade Management Tab

This tab is available for Oracle Fusion Applications only.

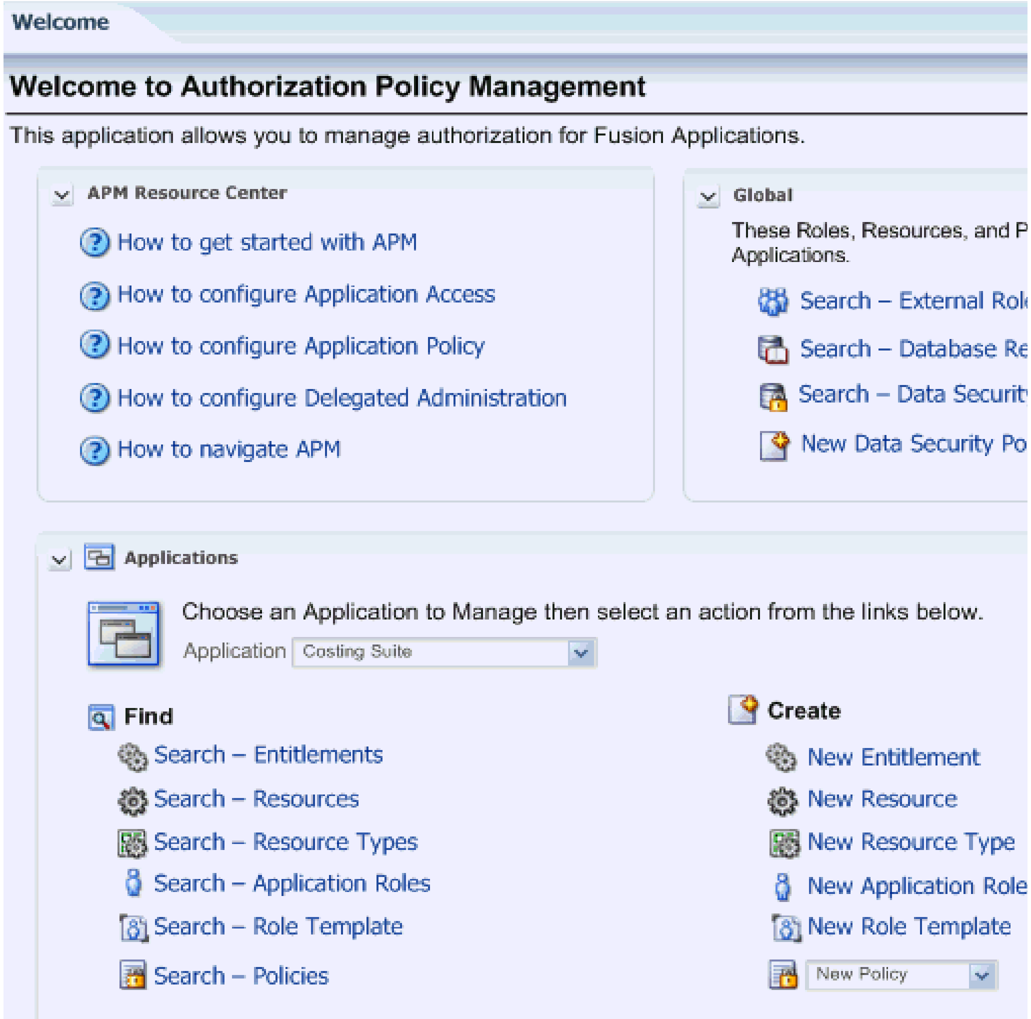
The Policy Upgrade Management tab is used to upgrade application policies in the LDAP-based domain policy store with the changes introduced by a new release of the application while preserving customizations introduced in the application stripe. For details, see Chapter 7, "Upgrading Oracle Fusion Applications Policies."

3.2 The Welcome Page

Upon a successful log in, Oracle Authorization Policy Manager displays the **Welcome** page, partially illustrated in Figure 3–1. This page contains is divided into the following areas:

- The **APM Resource Center** area contains links to some of the most commonly used procedures, including how to get started; configuring application access (or how to define the map between application roles and external roles), an application policy, delegated administration; and how to navigate through the tool UI.
- The **Global** area contains links to procedures that pertain artifacts shared across all applications, including searching external roles.
- The **Applications** area contains, at the top, a pull-down listing the application stripes in the policy store used to select the stripe to manage. This area also contains links to procedures, including searching and creating entitlements, resources, resource types, application roles, and application policies.

Figure 3–1 The Welcome Page



This application allows you to manage authorization for Fusion Applications.

APM Resource Center
How to get started with APM
How to configure Application Access
How to configure Application Policy
How to configure Delegated Administration
How to navigate APM
Global

These Roles, Resources, and P
Applications.

Choose an Application to Manage then select an action from the links below.

Application: Costing Suite

3.3 The Navigation Panel

The navigation panel helps users finding security artifacts by browsing or searching. For details about using the navigation panel to search, see Finding Artifacts with a Simple Search.

The navigation panel, partially illustrated in Figure 3–2, is a collapsible and expandable panel that contains, from top to bottom, the following UI functions:

- A pull-down list to select the scope of a simple search. The scope can be global or specific to a selected application stripe.
- A pull-down list to select the artifact to query with a simple search. When the search scope is global, the list shows global artifacts; when specific to an application stripe, it shows application policy artifacts.
- A text box to enter a string that the simple search should match. The string you enter is compared against the name *and* display name of security artifacts, and those that match are displayed in the Search Results tab.
- The **Browse** tab, which displays the following expandable and collapsible hierarchy of nodes:

  - The **Global** node, from where to access global artifacts such as external roles, policies, role templates, and database resources. These last two artifacts are available for Oracle Fusion Applications only.
  - One node per application stripe and to which the logged in user has access. Note that the list of applications shown *depends* on the logged in user. For details, see Chapter 6, "Delegated Administration."

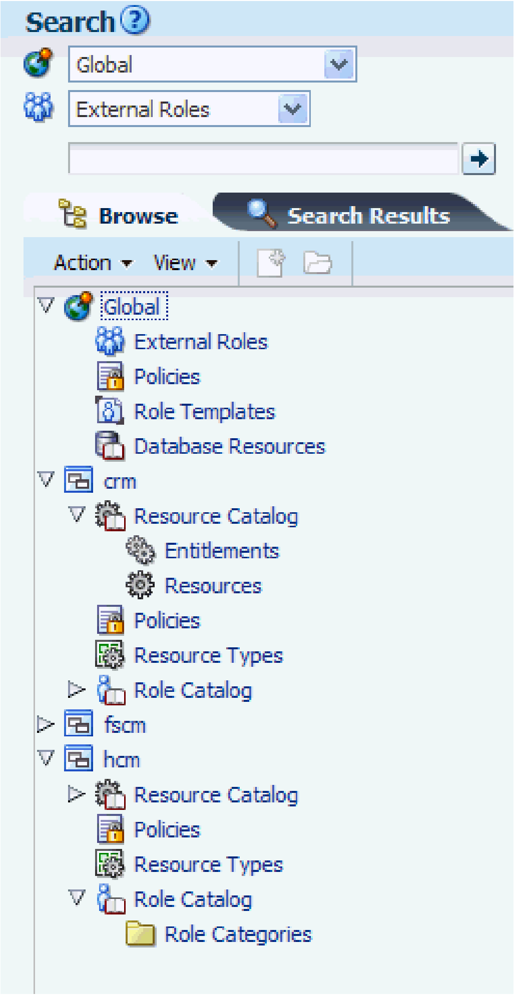
    From any of these nodes, one can access application-specific artifacts such as resource types, entitlements, resources, policies, and the role category.

    Note: As mentioned above, each node in the hierarchy identifies a application stripe in the domain policy store. Several applications *can* share a logical stripe.

    Typically, each J2EE/ADF or J2SE application has its own application stripe which is not shared with any other applications; but when several applications make up a larger logical application, then an application stripe can be shared by those applications members of the larger one.

- The **Search Results** tab, which displays the results of the last simple search.

Figure 3–2 The Navigation Panel



3.4 Finding Artifacts with a Simple Search

The top of the navigation panel, shown in Figure 3–2, is used to specify simple queries. Advanced queries are also available; for details see Chapter 4, "Querying Security Artifacts."

To specify a simple search, proceed as follows:

1. Select the search scope from the pull-down list at the top of the navigation panel.
2. Select the object type to search from the pull-down list second from the top. The list of available object types varies according to the search scope selected.

   If you select Resource Instance (on an application), you must also select the Resource Type from the pull-down list next to the object type box.
3. Enter a string to match in the text box, possibly using the wildcard characters % or * (the wild character matches any character in the pattern).

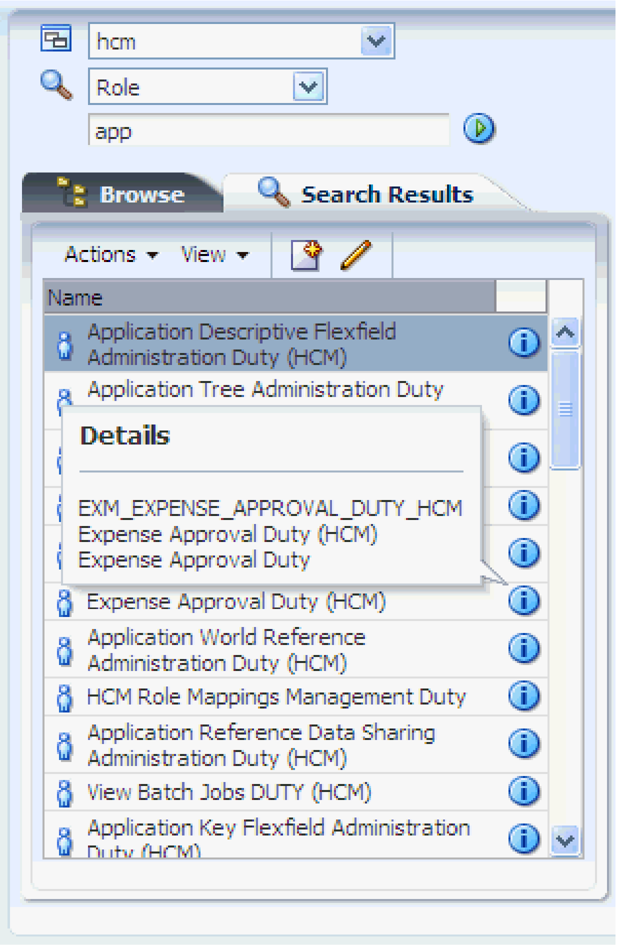
   The search returns all names and display names of the object type selected that match the specified string; leave this box empty to obtain the list of all objects of the specified type.

4. Click the Go button to trigger the search and to display the results in the tab **Search Results**, which is automatically brought to the foreground when the search is completed. Positioning the cursor on the blue information button next to an item displays the item details. The Search Results tab shows at most the first 200 matches found by the search.

5. Once an item is selected in the Search Results, it can be opened or edited by clicking **Open** or **Edit** at the top of the table.

Figure 3–3 illustrates the results of a simple search on roles for an application and the details of an application role returned by the simple search.

Figure 3–3 The Search Results Tab



hcm

Role

app

Application Descriptive Flexfield Administration Duty (HCM)

Application Tree Administration Duty

EXM_EXPENSE_APPROVAL_DUTY_HCM
Expense Approval Duty (HCM)
Expense Approval Duty

Expense Approval Duty (HCM)

Application World Reference Administration Duty (HCM)

HCM Role Mappings Management Duty

Application Reference Data Sharing Administration Duty (HCM)

View Batch Jobs DUTY (HCM)

Application Key Flexfield Administration Duty (HCM)

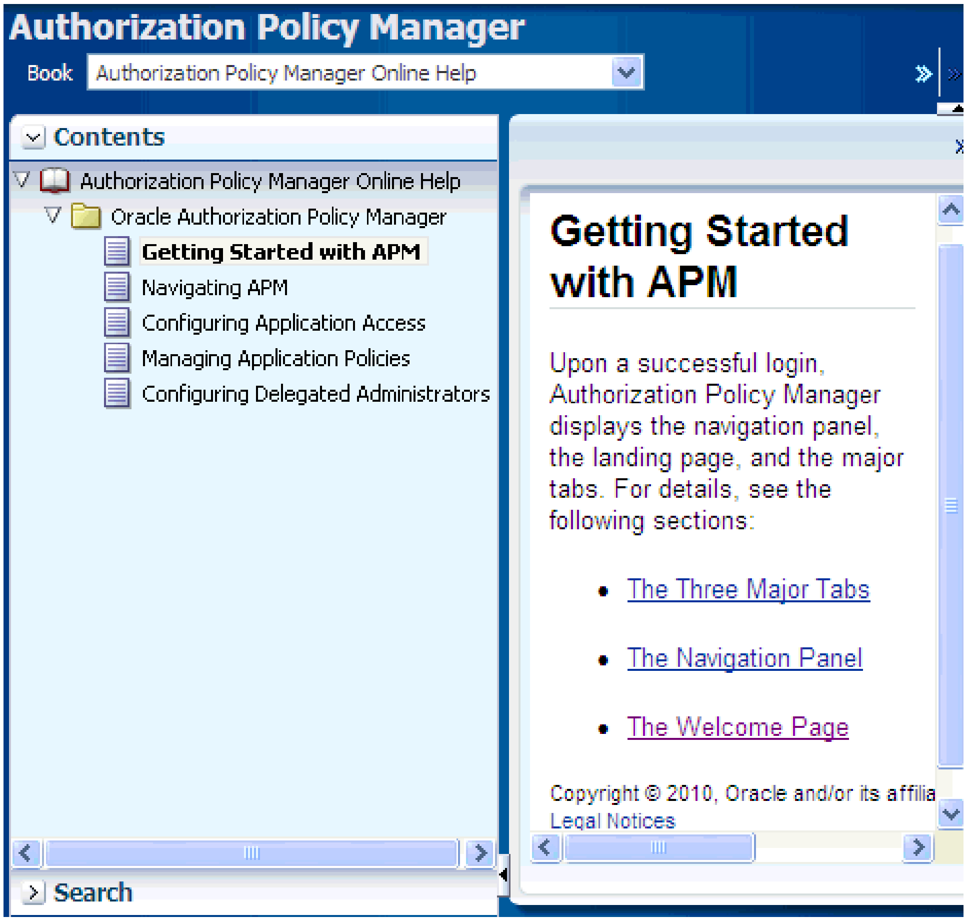
3.5 Online Help

To access online help documentation, on the upper right corner of any window, click Help to bring up the help window, partially illustrated in Figure 3–4.

In this window, you can select the documentation to view by choosing an item from the pull-down **Book** box.

Also you can search for a string in a displayed page (**Find in Page**) or within either of the two books available (select book and use **Search**).

Figure 3–4 Online Help Window


Authorization Policy Manager
Book
Authorization Policy Manager Online Help
Contents
Authorization Policy Manager Online Help
Oracle Authorization Policy Manager
Getting Started with APM
Navigating APM
Configuring Application Access
Managing Application Policies
Configuring Delegated Administrators
Search

Getting Started with APM

Upon a successful login, Authorization Policy Manager displays the navigation panel, the landing page, and the major tabs. For details, see the following sections:

- The Three Major Tabs
- The Navigation Panel
- The Welcome Page

Copyright © 2010, Oracle and/or its affilia
Legal Notices

3.6 Some Frequently Used Operations

The following scenarios describe frequent uses of Oracle Authorization Policy Manager:

- Find artifacts whose names or display names match a pattern. For details, see Finding Artifacts with a Simple Search.
- Given an external role, view all the application roles mapped to the external role. For details, see Section 5.4, "Mapping Application Roles to an External Role."
- Given an application role, view all the external roles mapped to the application role. For details, see Section 5.5, "Mapping External Roles to an Application Role."
- Given an application role, view the application hierarchy at the role. For details, see Section 5.3, "Managing the Application Role Hierarchy."
- Given an entitlement, view all application policies that use the entitlement. For details, see Section 4.6.1, "Finding Application Policies that Match Entitlements or Resources."
- Given a principal (that is, a user, an external role, or an application role), view all the application policies that use the principal. For details, see Section 4.6.2, "Finding Application Policies that Match Principals."

4 Querying Security Artifacts

Oracle Authorization Policy Manager allows two kinds of queries over OPSS security objects: simple and advanced. Simple queries are conducted in the navigation panel of the Authorization Management tab, and they involve matching names and display names only, as explained in Section 3.4, "Finding Artifacts with a Simple Search." Advanced queries are conducted in different pages of the Authorization Management tab, and they use the operators start with, ends with, contains, and equal to, which allow specifying more sophisticated matchings.

This chapter explains how to specify advanced queries, in the following sections:

There is no support for wildcard characters in advanced queries. In particular, the characters * or % are treated as plain characters in the specification of any advanced search parameter.

4.1 Searching External Roles

To search external roles, proceed as follows:

1. Expand **Global** in the navigation panel to expose the **External Roles** under it.
2. Either double-click External Roles or select it and click **Open** to display the **Search - External Roles** tab in the Authorization Management tab.
3. In the Search area of that tab, enter the query parameters as follows:
   - Select an operator for the Name from the first pull-down list and enter a string to match.
   - Select an operator for the Display Name from the second pull-down list and enter a string to match.

- Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.

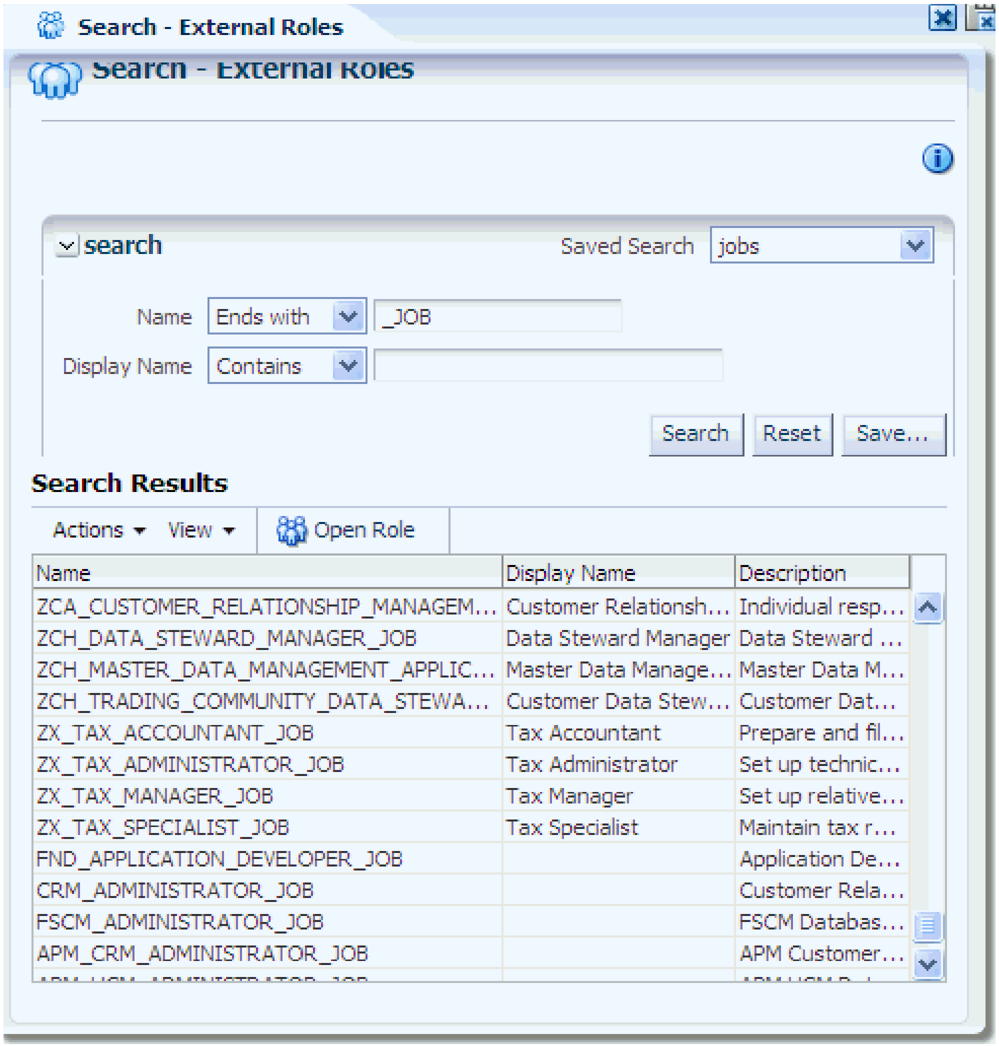
4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a saved search from this pull-down list fills in the query parameters automatically with the saved values.

5. Click **Search** to trigger the search. All external roles matching the query parameters are displayed in the **Search Results** area.

   The action at the top of this table allows viewing the details of a role (**Open Role**).

Figure 4–1 illustrates the results of an advanced search on external roles with previously saved query parameters (under jobs).

Figure 4–1 External Roles - Advanced Search



Saved Search: jobs

Name: Ends with _JOB

Display Name: Contains

Search Results

Name	Display Name	Description
ZCA_CUSTOMER_RELATIONSHIP_MANAGEM...	Customer Relationsh...	Individual resp...
ZCH_DATA_STEWARD_MANAGER_JOB	Data Steward Manager	Data Steward ...
ZCH_MASTER_DATA_MANAGEMENT_APPLIC...	Master Data Manage...	Master Data M...
ZCH_TRADING_COMMUNITY_DATA_STEWA...	Customer Data Stew...	Customer Dat...
ZX_TAX_ACCOUNTANT_JOB	Tax Accountant	Prepare and fil...
ZX_TAX_ADMINISTRATOR_JOB	Tax Administrator	Set up technic...
ZX_TAX_MANAGER_JOB	Tax Manager	Set up relative...
ZX_TAX_SPECIALIST_JOB	Tax Specialist	Maintain tax r...
FND_APPLICATION_DEVELOPER_JOB		Application De...
CRM_ADMINISTRATOR_JOB		Customer Rela...
FSCM_ADMINISTRATOR_JOB		FSCM Databas...
APM_CRM_ADMINISTRATOR_JOB		APM Customer...

4.2 Searching Application Roles

To query application roles, proceed as follows:

1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.

2. Either double-click **Role Catalog** or select it and click **Open** to display the **Search - Role Catalog** tab in the Authorization Management tab.

3. In the Search area of that tab, enter the query parameters as follows:

   - Select an operator for the Role Name from the first pull-down list and enter a string to match.
   - Select an operator for the Display Name from the second pull-down list and enter a string to match.
   - Select an operator for the Category and enter a string to match.
   - Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.

4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a saved search from this pull-down list fills in the query parameters automatically with the saved values.

5. Click **Search** to trigger the search. All role categories matching the entered specifications are displayed in the table **Search Results**. Figure 4–2 illustrates this page.

   The actions at the top of this table allow:

   - Creating a new application policy (**New Policy**) based on an application role selected from the table. For details, see Section 5.1.5.1, "Creating a Policy."
   - Creating a new application role (**New**). For details, see Section 5.1.1.1, "Creating a Role."
   - Modifying or deleting a role selected from the table (**Open**, **Delete**). For details, Section 5.1.1.2, "Modifying a Role."

     Deleting a role deletes the role and all roles nested in it; Oracle Authorization Policy Manager prompts for a confirmation before executing this cascading deletion. All references to a removed role are removed from application policies in the application stripe.
   - Finding the policies matching a role selected from the table (**Find Policies**). To search policies that match entitlements or resources, see Finding Application Policies that Match Entitlements or Resources.

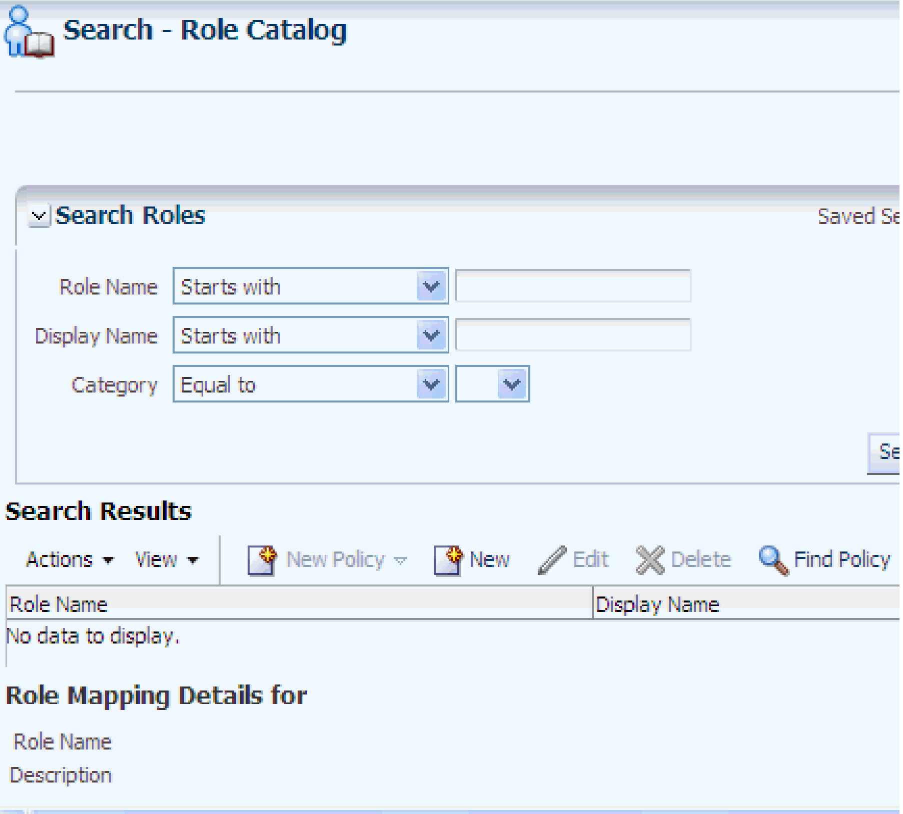
6. In addition, to modify the external roles assigned (mapped) to an application role in the Search Results table, select a role to display the area **Role Mapping Details** for the selected role.

   In that area, the table External Role Assignments lists the external roles mapped to the application role. The actions at the top of this table allow:

   - Adding an external role (**Add External Role**).
   - Removing an external role (**Remove External Role**).
   - Viewing an external role selected from the table (**Open External Role**).

   For details about the external roles, see sections Section 5.2, "Viewing the External Role Hierarchy," and Section 5.5, "Mapping External Roles to an Application Role."

Figure 4–2 Application Roles - Advanced Search



Role Name Starts with

Display Name Starts with

Category Equal to

No data to display.

4.3 Searching Application Resource Types

To search application resource types, proceed as follows:

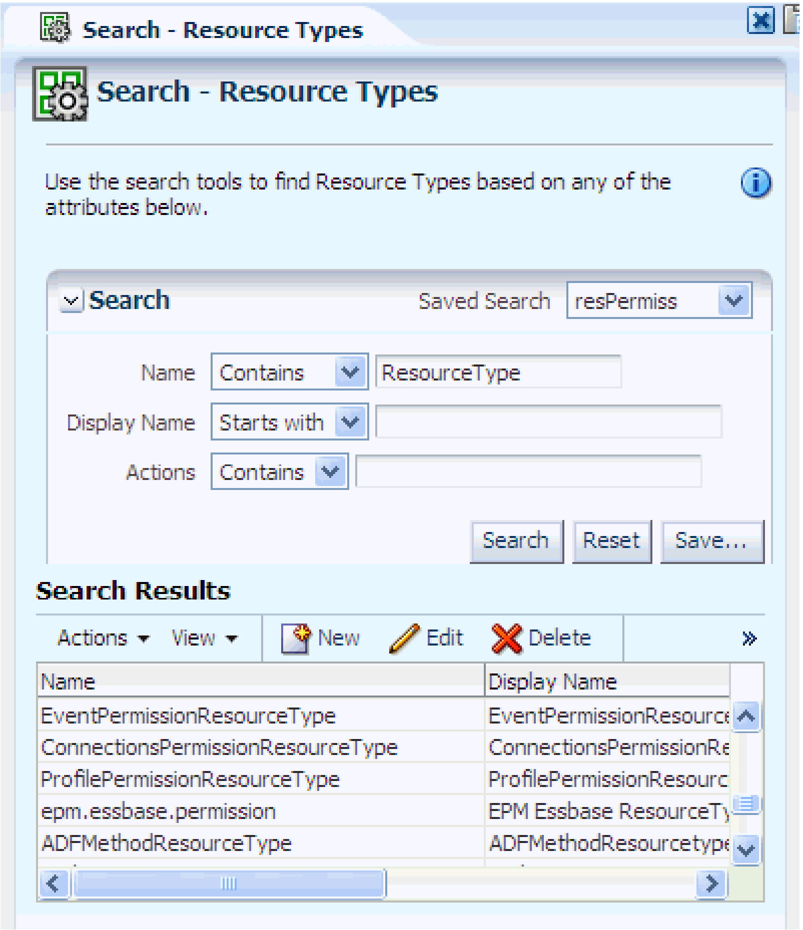
1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.
2. Either double-click **Resource Types** or select it and click **Open** to display the **Search - Resource Types** tab in the Authorization Management tab.
3. In the Search area of that tab, enter the query parameters as follows:
   - Select an operator for the Name from the first pull-down list and enter a string to match.
   - Select an operator for the Display Name from the second pull-down list and enter a string to match.
   - Select an operator for Actions and enter a string to match.
   - Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.
4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a saved search from this pull-down list fills in the query parameters automatically with the saved values.
5. Click **Search** to trigger the search. All resource types matching the entered specifications are displayed in the table **Search Results**.

The actions at the top of this table allow:

- Creating a resource type (**New**)
- Editing a resource type (**Open**)
- Deleting a resource type (**Delete**)

Figure 4–3 illustrates the results of an advanced search on resource types with previously saved query parameters (under resPermiss).

Figure 4–3 Resource Types - Advanced Search



Search - Resource Types

Use the search tools to find Resource Types based on any of the attributes below.

Saved Search: resPermiss

Name: Contains ResourceType

Display Name: Starts with

Actions: Contains

Search Results

Name	Display Name
EventPermissionResourceType	EventPermissionResource
ConnectionsPermissionResourceType	ConnectionsPermissionRe
ProfilePermissionResourceType	ProfilePermissionResourc
epm.essbase.permission	EPM Essbase ResourceTy
ADFMethodResourceType	ADFMethodResourcetype

4.4 Searching Application Resources

To search application resources, proceed as follows:

1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.
2. Either double-click **Resources** or select it and click **Open** to display the **Search - Resources** tab in the Authorization Management tab.
3. In the Search area of that tab, enter the query parameters as follows:
   - Select an operator for the Name from the first pull-down list and enter a string to match.

- Select an operator for the Display Name from the second pull-down list and enter a string to match.
- Select an operator for the Resource Type and then select a resource type from the pull-down list to the right. This selection is required.
- Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.

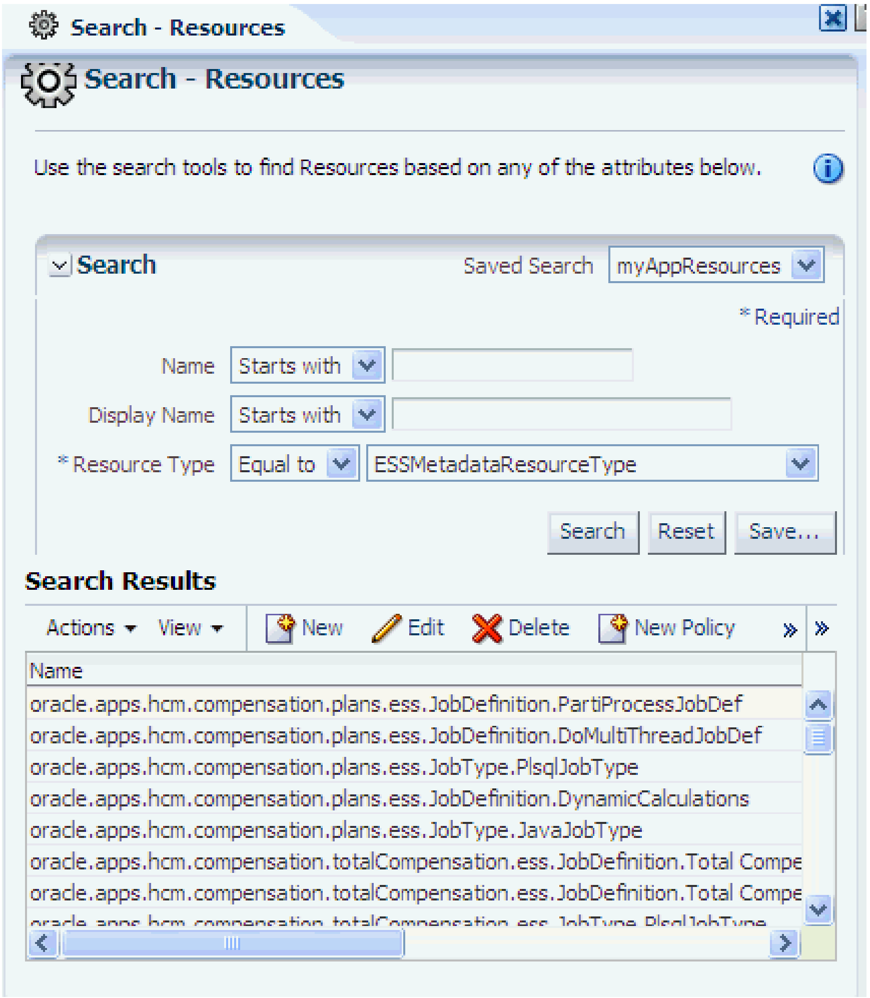
4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a saved search from this pull-down list fills in the query parameters automatically with the saved values.
5. Click **Search** to trigger the search. All resources matching the entered specifications are displayed in the table **Search Results**.

   The actions at the top of this table allow:

   - Creating a resource (**New**)
   - Editing a resource (**Open**)
   - Deleting a resource (**Delete**)
   - Creating a new policy based on a resource (**New Policy**)
   - Finding policies that contain a resource (**Find Policy**)
   - Detaching the Search Results table (**Detach**)

Figure 4–4 illustrates the results of an advanced search on resources with previously saved query parameters (under myAppResources).

Figure 4–4 Resources - Advanced Search



Use the search tools to find Resources based on any of the attributes below.

Saved Search: myAppResources

* Required

Name	Starts with	
Display Name	Starts with	
* Resource Type	Equal to	ESSMetadataResourceType

Name
oracle.apps.hcm.compensation.plans.ess.JobDefinition.PartiProcessJobDef
oracle.apps.hcm.compensation.plans.ess.JobDefinition.DoMultiThreadJobDef
oracle.apps.hcm.compensation.plans.ess.JobType.PlsqlJobType
oracle.apps.hcm.compensation.plans.ess.JobDefinition.DynamicCalculations
oracle.apps.hcm.compensation.plans.ess.JobType.JavaJobType
oracle.apps.hcm.compensation.totalCompensation.ess.JobDefinition.Total Compe
oracle.apps.hcm.compensation.totalCompensation.ess.JobDefinition.Total Compe
oracle.apps.hcm.compensation.totalCompensation.ess.JobType.PlsqlJobType

4.5 Searching Application Entitlements

To search application entitlements, proceed as follows:

1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.
2. Either double-click **Entitlements** or select it and click **Open** to display the **Search - Entitlements** tab in the Authorization Management tab.
3. In the Search area of that tab, enter the query parameters as follows:
   - Select an operator for the Name from the first pull-down list and enter a string to match.
   - Select an operator for the Display Name from the second pull-down list and enter a string to match.
   - Select an operator for the Resource and enter a string to match.
   - Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.
4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a

saved search from this pull-down list fills in the query parameters automatically with the saved values.

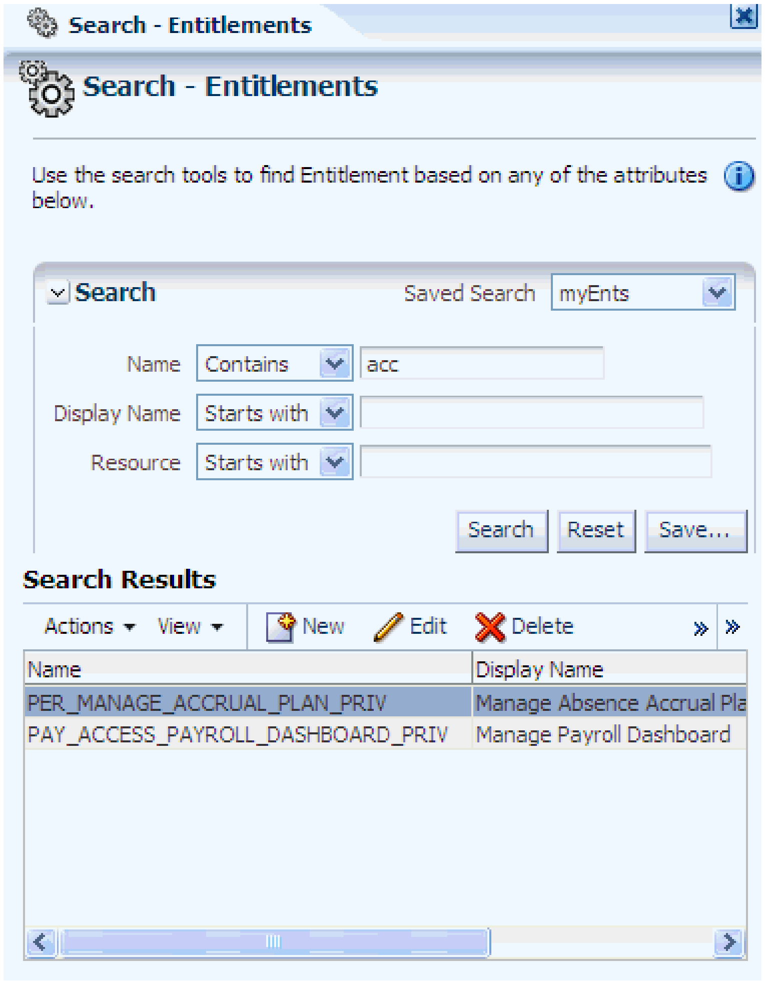
5. Click **Search** to trigger the search. All entitlements matching the entered specifications are displayed in the table **Search Results**.

   The actions at the top of this table allow:

   - Creating an entitlement (**New**)
   - Editing an entitlement (**Open**)
   - Delete an entitlement (**Delete**)
   - Creating a new policy based on an entitlement (**New Policy**)
   - Finding policies that contain an entitlement (**Find Policy**)
   - Detaching the Search Results table (**Detach**)

Figure 4–5 illustrates the results of an advanced search on entitlements with previously saved query parameters (under myEnts).

Figure 4–5 Entitlements - Advanced Search



Search - Entitlements

Search - Entitlements

Use the search tools to find Entitlement based on any of the attributes below.

Search

Saved Search: myEnts

Name: Contains: acc

Display Name: Starts with:

Resource: Starts with:

Search Results

Name	Display Name
PER_MANAGE_ACCRUAL_PLAN_PRIV	Manage Absence Accrual Pla
PAY_ACCESS_PAYROLL_DASHBOARD_PRIV	Manage Payroll Dashboard

4.6 Searching Application Policies

Application policies can be searched by specifying entitlements, resources, or principals to match, as explained in the following sections:

- Finding Application Policies that Match Entitlements or Resources
- Finding Application Policies that Match Principals

Alternative ways of finding application policies that contain an entitlement or a resource is available using the action menu **Find Policy** as explained in sections Searching Application Entitlements and Searching Application Resources.

4.6.1 Finding Application Policies that Match Entitlements or Resources

To query application policies that match entitlements or resources, proceed as follows:

1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.
2. Either double-click **Policies** or select it and click **Open** to display the **Search - Policies** tab in the Authorization Management tab.
3. In this tab, click **Function Resource** to display the page where you specify parameters for entitlement and/or resource names.
4. Select an operator for the Entitlement Name from the first pull-down list and enter a string to match, and/or select an operator for the Resource Name from the second pull-down list and enter a string to match.

   At least one of Entitlement Name or Resource Name must be specified.
5. Click **Search** to trigger the search.
6. To view all entitlement-based policies matching the specification, click **Entitlement Policies**. The actions **New Policy** and **Delete** at the top of table in this area allows creating an entitlement-based policy and deleting a policy.
7. To view all resource-based policies matching the specification, click **Resource Based Policies**. The actions **New Policy**, **Open**, and **Delete** at the top of table in this area allows creating, editing, and deleting a resource-based policy.
8. To view the details of a item, linger the cursor over the information blue button.

4.6.2 Finding Application Policies that Match Principals

To query application policies that match principals, proceed as follows:

1. Select an application in the navigation panel and expand it to expose all nodes in the hierarchy.
2. Either double-click **Policies** or select it and click **Open** to display the **Search - Policies** tab in the Authorization Management tab.
3. In this tab, click **Principal** to display the page where you specify parameters for the principal to match.
4. Select the type of principal from the first pull-down, an operator from the second pull-down list, and enter a string to match.
5. Click **Search** to trigger the search.
6. To view all entitlement-based policies matching a principal, select a principal from the **Found Principals** table, and click **Entitlement Policies**. The **New Policy** menu at the top of table allows creating an entitlement-based policy.

7. To view all resource-based policies matching a principal, select a principal from the **Found Principals** table, and click **Resource Based Policies**. The **New Policy** and **Open** menus at the top of table in this area allows creating and editing a resource-based policy.
8. To view the details of a item, linger the cursor over the information blue button.

4.7 Searching Data Role Templates

Data Role Templates can be searched by specifying a template name, display name, and group id, as explained in the following procedure.

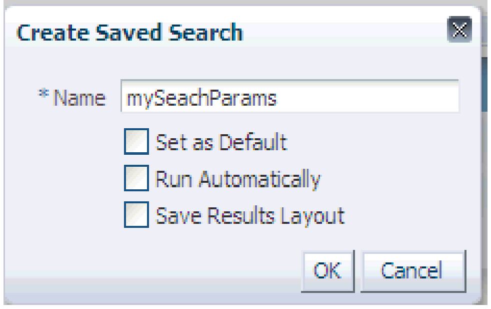
1. Select **Global > Role Templates** in the navigation panel and then click Open (the folder icon on top of the panel) to display the **Search - Role Templates** page.
2. In that page enter the following query data:
   - An operator and a string to match for the template name.
   - An operator and a string to match for the template display name.
   - An operator and a string to match for the template group id.
3. Click **Search** to trigger the search and to display the templates that match the entered specification in the **Search Results** table.
4. To view an item from that table, either double-click the item or select it and click **Open**.
5. To create a new data role template, click **New**.

4.8 Reusing Search Parameter Values

Advanced search allows saving the set of parameters used in the search. This option facilitates reproducing the results of a previous search quickly without the need to enter the same set of values multiple times.

A set of parameters is given a name and saved using the button **Save...**, and it is reused using the pull-down list **Saved Search**. Selecting a set of parameters from that list, automatically fills in the search parameters with the saved values. Figure 4–6 illustrates the Create Saved Search dialog.

Figure 4–6 Saving the Parameters of a Search



Create Saved Search

* Name mySeachParams

□ Set as Default

□ Run Automatically

□ Save Results Layout

5 Managing Security Artifacts

This chapter describes the procedures an administrator follows to manage application-specific security artifacts, view the external role hierarchy, manage the application role hierarchy, and manage the many-to-many mapping of application roles to external roles from both the application and the external role point of view.

This chapter is divided into the following sections:

- Managing Application Security Artifacts
- Viewing the External Role Hierarchy
- Managing the Application Role Hierarchy
- Mapping Application Roles to an External Role
- Mapping External Roles to an Application Role

5.1 Managing Application Security Artifacts

Oracle Authorization Policy Manager allows performing CRUD (create, read, update, delete) operations on several application security artifacts.

The menu **New**, to create an artifact, is available in the Browser and Search Results tabs of the navigation panel, and advanced search results tables.

The menu **Open**, to view and modify an artifact, is available in the Search Results tab of the navigation panel and advanced search results tables.

The menu **Delete**, to remove an artifact, is available in advanced search results tables.

The following sections describe how to manage specific security artifacts:

- Managing Application Roles
- Managing Application Resource Types
- Managing Application Resources
- Managing Application Entitlements
- Managing Application Policies
- Managing Application Role Categories

> **Note:** In regards to enterprise users and external roles, Oracle Authorization Policy Manager provides viewing and searching functionality only. To manage users and external roles, use Oracle Identity Manager or some other identity management tool.

5.1.1 Managing Application Roles

The following sections describe how to manage application roles:

- Creating a Role
- Modifying a Role

5.1.1.1 Creating a Role

To create an application role, proceed as follows:

1. In the navigation panel, right-click the application **Role Catalog** icon and select **New**, to open an Untitled page on the right panel.
2. In the **General** tab of the page, enter the following data for the role being created:
   - A role name (required)
   - A display name (required)
   - A description (optional). Although optional, it is recommended because it can provide useful information about the role.
   - A role category, to which the role being created belongs (optional)
3. Click **Save**. Note the following changes in the page: (a) the title Untitled changes to the string entered for display name; (b) two other tabs, **Application Role Hierarchy** and **External Role Mapping**, become available.
4. To position the role being created in the application role hierarchy:
   1. Bring the **Application Role Hierarchy** tab to the foreground.
   2. To view or specify the application roles this role inherits, select **Inherits** and click **Add** to display the **Add a Role** dialog.

      In the **Add a Role** dialog, query application roles with a given display name (empty string fetches all roles), select one or more roles from the results (Ctrl-click allows selecting one role at the time), and then click **Add**, to display the selected roles in the Inherits table.

      To delete a role from the Inherits table, select the role and click **Remove**; only roles directly under the top can be removed. To view a role, select the role and click **Open**; to find the policies that use a role, select the role and click **Find Policies**. To create a policy based on the application role, click **Create Policy** at the top of the page.

      To specify application roles for a role in the Inherits table, select the role, and click **Add** to display the **Add a Role** dialog. In that dialog, click the radio button for the selected role, and proceed to search and select roles to add. Then click Add, to display the added roles under the selected role.
   3. To view the application roles that this role is inherited by, select **Is Inherited By**.

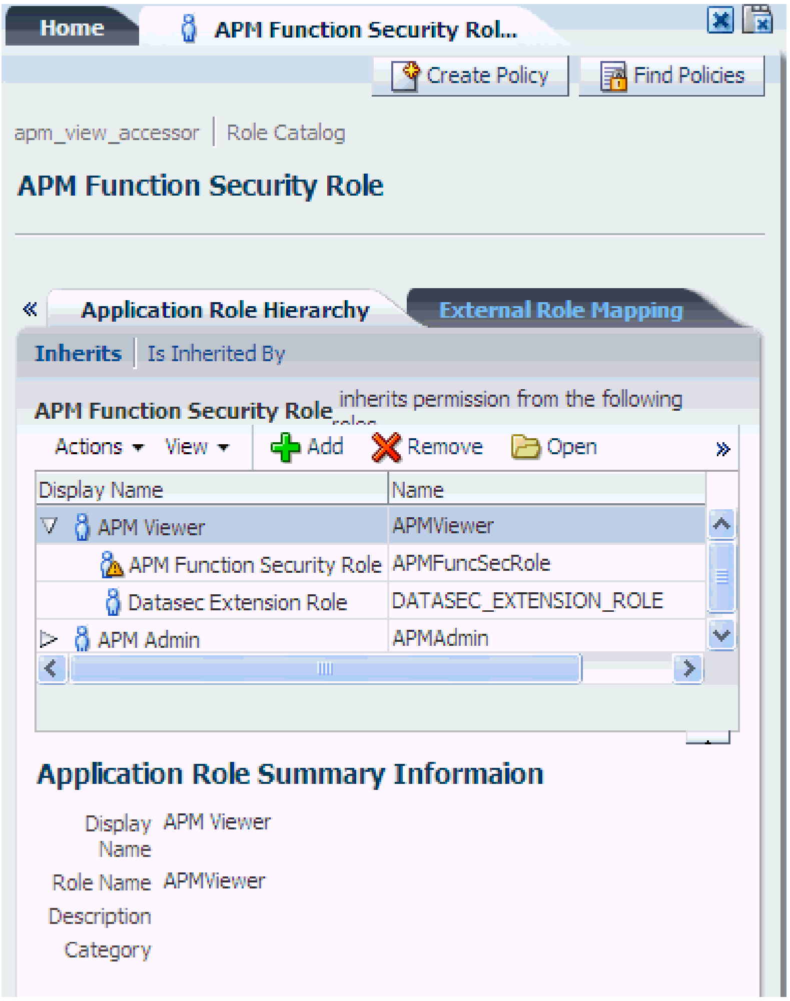
      To view a role in the Is Inherited table, select the role and click **Open**; to view the policies that use a role, select the role and click **View Policies**.

   In both pages, Inherits and Is Inherited By, the bottom area displays the summary information of a role selected from the table.
5. To map external roles to the application role being created:
   1. Bring the **External Role Mapping** tab to the foreground.

2. Click **Add** to display the **Add a Role** dialog, or select an item an click **Remove** to delete it.
3. In the **Add a Role** dialog, query external roles with a given display name (empty string fetches all roles), select one or more roles from the results (Ctrl-click allows selecting one role at the time), and then click **Add**, to display the selected roles in the External Roles tab.

Figure 5–1 illustrates part of the ApplicationRole Hierarchy tab.

Figure 5–1 Roles that an Application Role Inherits



APM Function Security Role

APM Function Security Role inherits permission from the following roles

Display Name	Name
APM Viewer	APMViewer
APM Function Security Role	APMFuncSecRole
Datasec Extension Role	DATASEC_EXTENSION_ROLE
APM Admin	APMAdmin

Application Role Summary Informaion

Display Name APM Viewer

Role Name APMViewer

Description

Category

5.1.1.2 Modifying a Role

Deleting a role deletes the role and all roles nested in it; Oracle Authorization Policy Manager prompts a confirmation before executing this cascading deletion. Moreover, all references to a removed role are removed from application policies in the application stripe.

To delete an application role, use the procedure in Section 4.2, "Searching Application Roles" to identify the role in the Search Results table of an advanced search, select the role, and then click **Delete**.

To modify or view an application role, proceed as follows:

1. Select the application role in the Search Results of the navigation panel, and double-click it or click **Open** to display the page for the application role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. Modify, as appropriate, the current specifications in the General, Application Role Hierarchy, and External Role Mapping tabs. If any data in the General tab is changed, click **Apply**.

5.1.2 Managing Application Resource Types

The following sections describe how to manage application resource types:

- Creating a Resource Type
- Modifying a Resource Type

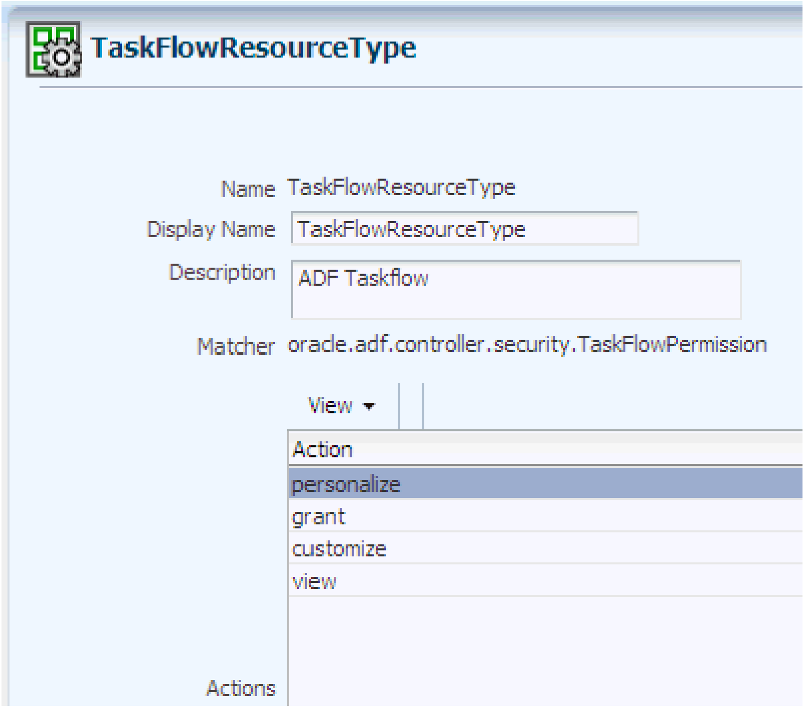
5.1.2.1 Creating a Resource Type

To create an application resource type, proceed as follows:

1. In the navigation panel, right-click the application **Resource Types** icon and select **New**, to open an Untitled page on the right panel.
2. In that page, enter the following data for the resource type being created:
   - A name (required).
   - A display name (required).
   - A description (optional). Although optional, it is recommended because it can provide useful information about the resource type.
   - A fully qualified name of the permission class for the resource type, in the box labeled **Matcher** (required). For details about the matcher class of a resource type, see Section 2.3.3.1, "Resource Type."
   - The actions allowed by the type - to insert an action in the current list, click **New** to display the **New Action** dialog; enter the name of the action and then click **Save**; the Action list is then updated with the new action.
3. Click **Save**. The tab changes its title to the name of the resource type just created.

Figure 5–2 illustrates part of the page for the resource type *TaskFlowResourceType*.

Figure 5–2 Creating a Resource Type



TaskFlowResourceType

Name TaskFlowResourceType

Display Name TaskFlowResourceType

Description ADF Taskflow

Matcher oracle.adf.controller.security.TaskFlowPermission

Action
personalize
grant
customize
view

5.1.2.2 Modifying a Resource Type

To modify an application resource instance type, proceed as follows:

1. Identify the application resource type to modify or view. For details, see Section 4.3, "Searching Application Resource Types."
2. Select the resource, and click **Open** to open the page for the resource. (The Delete and New menus, also available, allows deleting a selected resource or creating a new one).
3. In that page, modify the resource type as appropriate.
4. Click **Apply** to save changes.

5.1.3 Managing Application Resources

The following sections describe how to manage application resources:

- Creating a Resource
- Modifying a Resource

5.1.3.1 Creating a Resource

To create an application resource instance, proceed as follows:

1. In the navigation panel, right-click the application **Resources** icon and select **New**, to open an Untitled page on the right panel.
2. In that page, enter the following data for the resource instance being created:
   - A name (required)
   - A display name (required)

  - A description (optional). Although optional, it is recommended because it can provide useful information about the resource instance.
  - A resource type - Select a resource type for the instance from the pull-down **Resource Types** (required)

3. Click **Save**. The tab changes its title to the name of the resource instance just created.

5.1.3.2 Modifying a Resource

To modify an application resource instance, proceed as follows:

1. Identify the application resource to modify or view. For details, see Section 4.4, "Searching Application Resources."
2. Select the resource, and click **Open** to open the page for the resource. (The Delete menu, also available, allows deleting a selected resource).
3. In that page, modify the resource as appropriate.
4. Click **Apply** to save changes.

Alternatively, use a simple search to identify the resource, select it, and then click **Open** to edit its attributes.

5.1.4 Managing Application Entitlements

The following sections describe how to manage application entitlements:

- Creating an Entitlement
- Modifying an Entitlement

5.1.4.1 Creating an Entitlement

To create an application entitlement, proceed as follows:

1. In the navigation panel, right-click the application **Entitlements** icon and select **New**, to open an Untitled page on the right panel.
2. In that page, enter the following data for the entitlement being created:
   - A name (required)
   - A display name (required)
   - A description (optional). Although optional, it is recommended because it can provide useful information about the entitlement.
3. Add resources to the entitlement being created. There are two ways of accomplishing this task; the first way is as follows:
   1. List the resources available to the application by performing a regular search on resource instances.
   2. Drag an drop resource instances from the **Search Results** tab (on the navigation panel) into the area labeled **Resources**.

   The second, alternative way is as follows:

   1. Click **Add** at the top of the area **Resources**, to display the **Add Resource** dialog.

2. In that dialog, search for the available resources whose names or display names match a string, and a selected Resource Type. The resources matching the query are displayed in the table at the bottom of the dialog.

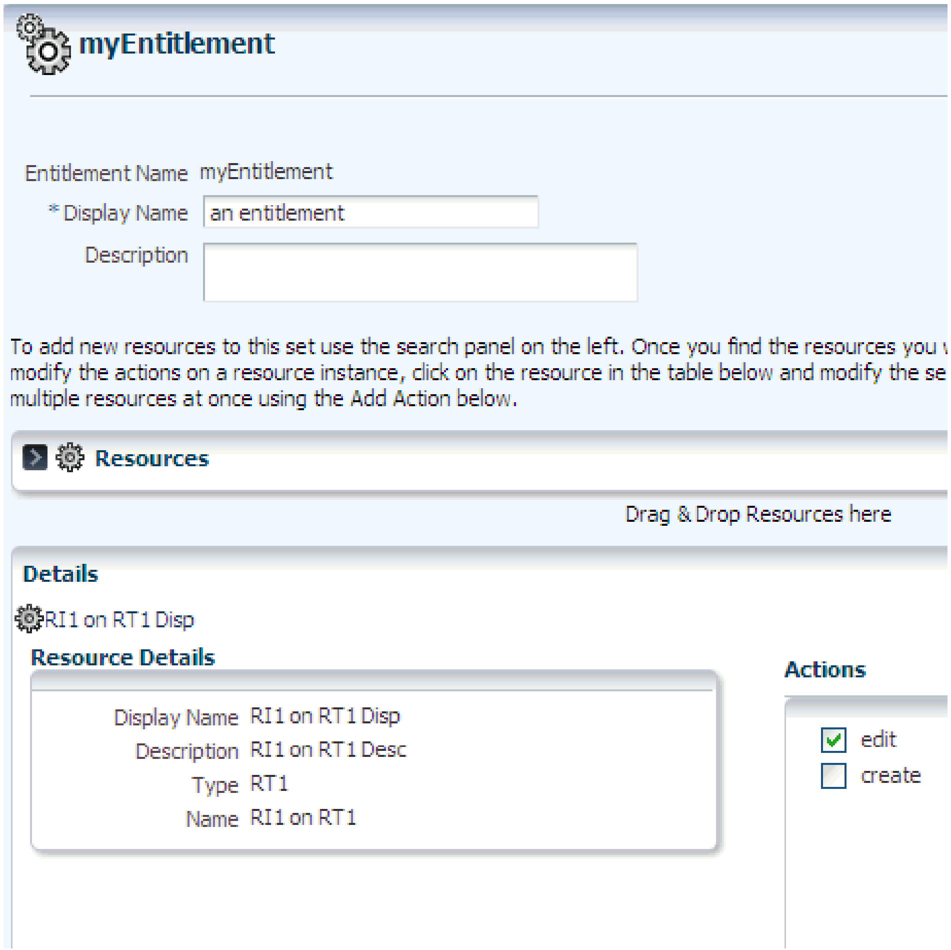
3. From the results, select the resources to add (the combination ctrl-left click allows you to select multiple items from the list), and then click **Add**. Only resources not already in the Resources list are allowed to be added.

4. Select actions for resources - First select a resource that you have added (from the Resources list) to display the resource details in the **Resource Details** area at the bottom of the page. Then check the desired actions for that resource in the area **Actions**. Only the actions allowed for the type of the selected resource are available in this area. Repeat this step for each of the resources you have added to the entitlement being created.

5. Click **Save**. The page changes its title to the name of the entitlement just created.

Figure 5–3 illustrates part of the page after the entitlement *myEntitlement* has been created and in which the area Resources has been collapsed.

Figure 5–3 Creating an Entitlement



myEntitlement

Entitlement Name myEntitlement

* Display Name an entitlement

Description

To add new resources to this set use the search panel on the left. Once you find the resources you v
modify the actions on a resource instance, click on the resource in the table below and modify the se
multiple resources at once using the Add Action below.

Resources

Drag & Drop Resources here

Details

RI1 on RT1 Disp

Resource Details

Display Name RI1 on RT1 Disp
Description RI1 on RT1 Desc
Type RT1
Name RI1 on RT1

Actions

☑ edit
□ create

5.1.4.2 Modifying an Entitlement

To modify or view an entitlement, proceed as follows:

1. Select the entitlement in the Search Results of the navigation panel, and double-click it or click **Open** to display the page for the entitlement. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. Modify, as appropriate, the current specifications in the page.
3. Click **Apply** to save changes.

5.1.5 Managing Application Policies

The following sections describe how to manage application functional policies:

- Creating a Policy
- Modifying a Policy

5.1.5.1 Creating a Policy

The following procedure describes a way to create an application policy based in an application role; alternative ways to create policies based on a principal, an entitlement, or a resource by using the **New Policy** menu are described in Section 4.6.1, "Finding Application Policies that Match Entitlements or Resources," and Section 4.6.2, "Finding Application Policies that Match Principals."

To create an application policy based on a specific application role, proceed as follows:

1. Select **Policies** under the application for which you want to create the policy, and double-click it or click **Open** to display the **Search - Policies** page.
2. In that page, bring the tab **Principal** to the foreground and specify parameters for a **Search**, to locate and select the principals (application role, external role, or user) on which to base the policy being created.
3. In the tab **Function Security**, at the bottom area of the page, select either **Entitlement Policies** or **Resource Based Policies** (according to the kind of policy to create), and then click New Policy to display an **Untitled** policy page.

   If creating an entitlement-based policy, then in the Untitled page:

   1. Add principals to the policy - Either use the button **Add** at the top of the **Principal** table, or, alternatively, perform a simple search on application roles, external roles, or users, and drag-and-drop items from the search results into the Principal table. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
   2. Add an entitlement to the policy - Either use the button **Add** at the top of the **Entitlement** table, or, alternatively, perform a simple search on the application entitlements, and drag-and-drop an entitlement from the search results into the Entitlement table.
   3. Click **Save**.

   If creating a resource-based policy, then in the Untitled page:

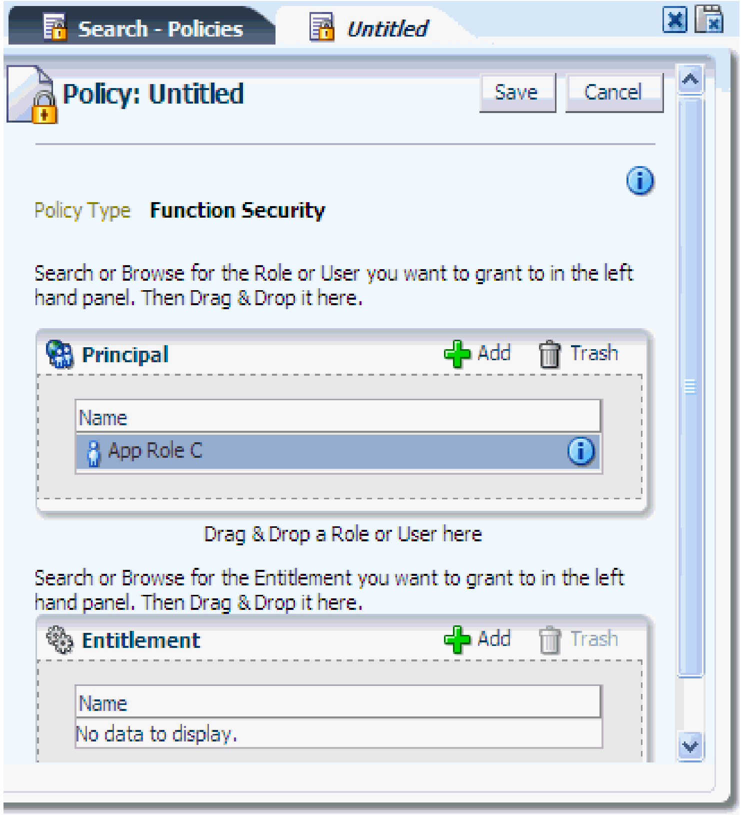
   1. Add principals to the policy - Either use the button **Add** at the top of the **Principal** table, or, alternatively, perform a simple search on application roles, external roles, or users, and drag-and-drop items from the search results into the Principal table. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
   2. Add resource instances to the policy - Either use the button **Add** in the **Resources** table, or, alternatively, perform a simple search on the application

resource instances, and drag-and-drop a resource instances from the search results into the Resources table.

3. For each of the resource instance added, select a resource instance and specify the actions allowed by checking the appropriate boxes in the **Actions** area at the bottom of the page.
4. Click **Save**.

Figure 5–4 illustrates part of the page after creating a policy based on an entitlement.

Figure 5–4 Creating an Entitlement-Based Policy



Policy Type Function Security

Search or Browse for the Role or User you want to grant to in the left hand panel. Then Drag & Drop it here.

Name
App Role C

Search or Browse for the Entitlement you want to grant to in the left hand panel. Then Drag & Drop it here.

Name
No data to display.

5.1.5.2 Modifying a Policy

Entitlement-based policies cannot be modified.

To modify or view a resource-based policy, proceed as follows:

1. Identify the resource-based application policy to modify or view in either of the following ways:
   - By matching an application role in the policy. For details, see step 7 in procedure in Section 4.6.2, "Finding Application Policies that Match Principals."
   - By matching a resource name in the policy. For details, see step 7 in procedure in Section 4.6.1, "Finding Application Policies that Match Entitlements or Resources."
2. Select the policy, and click **Open** to open the page for the policy.
3. In that page, modify the policy attributes as appropriate.

4. Click **Apply** to save changes.

5.1.6 Managing Application Role Categories

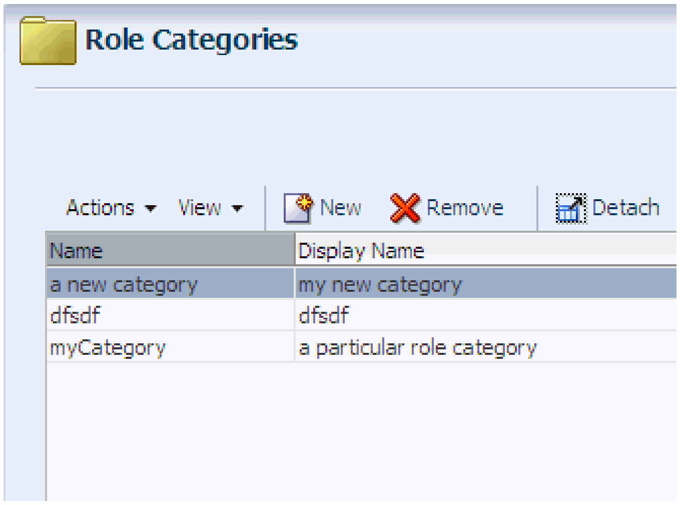
Oracle Authorization Policy Manager does not support modifying role categories, but only creating and deleting them.

To create an application role category, proceed as follows:

1. In the navigation panel, right-click the application **Roles Categories** icon and select **New**, to open an Untitled page on the right panel.
2. In that page, click New to display the **New Category** dialog.
3. In that dialog, enter the following data for the category being created:
   - A name (required)
   - A display name (required)
   - A description (optional). Although optional, it is recommended because it can provide useful information about the category.
4. Click **Create**: the new category is displayed in the list under the Role Categories page.

Figure 5–5 partially illustrates the Role Categories page after a category has been created.

Figure 5–5 Creating an Application Role Category



Name	Display Name
a new category	my new category
dfsdf	dfsdf
myCategory	a particular role category

5.2 Viewing the External Role Hierarchy

To view the external role hierarchy under a given external role, proceed as follows:

1. Select an external role in the Search Results of the navigation panel, and double-click it or select it and click the View icon to display the page for the external role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. In that page, select the **External Role Hierarchy** tab.

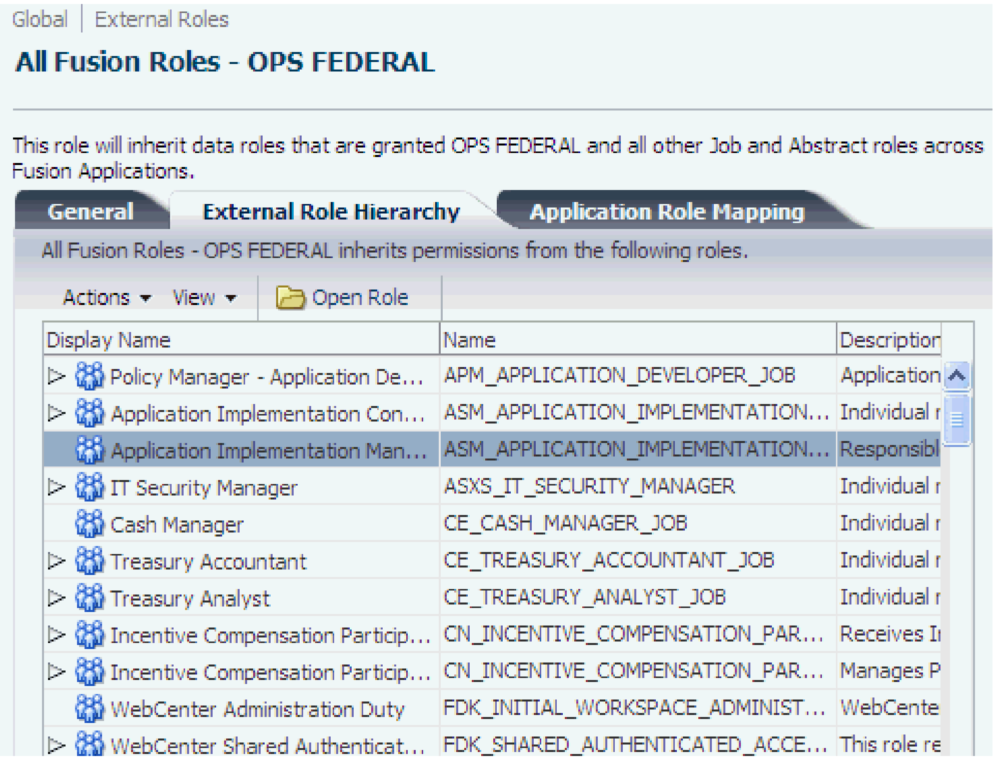
3. The table in that tab displays all the external roles from which the selected role inherits permissions. Any external role in the table admits being expanded to further show the deeper levels of the hierarchy.

   In addition, the actions at the top of the table allow:

   - Opening a selected external role for view (**Open Role**)

Figure 5–6 partially illustrates the External Role Hierarchy tab for the external role OPS FEDERAL.

Figure 5–6 External Role Hierarchy



Global | External Roles

All Fusion Roles - OPS FEDERAL

This role will inherit data roles that are granted OPS FEDERAL and all other Job and Abstract roles across Fusion Applications.

All Fusion Roles - OPS FEDERAL inherits permissions from the following roles.

Display Name	Name	Description
▷ Policy Manager - Application De...	APM_APPLICATION_DEVELOPER_JOB	Application
▷ Application Implementation Con...	ASM_APPLICATION_IMPLEMENTATION...	Individual r
Application Implementation Man...	ASM_APPLICATION_IMPLEMENTATION...	Responsibl
▷ IT Security Manager	ASXS_IT_SECURITY_MANAGER	Individual r
Cash Manager	CE_CASH_MANAGER_JOB	Individual r
▷ Treasury Accountant	CE_TREASURY_ACCOUNTANT_JOB	Individual r
▷ Treasury Analyst	CE_TREASURY_ANALYST_JOB	Individual r
▷ Incentive Compensation Particip...	CN_INCENTIVE_COMPENSATION_PAR...	Receives I
▷ Incentive Compensation Particip...	CN_INCENTIVE_COMPENSATION_PAR...	Manages P
WebCenter Administration Duty	FDK_INITIAL_WORKSPACE_ADMINIST...	WebCente
▷ WebCenter Shared Authenticat...	FDK_SHARED_AUTHENTICATED_ACCE...	This role re

5.3 Managing the Application Role Hierarchy

This section explains how to view and modify an application role hierarchy, specifically, the hierarchy of application roles below and above a given application role.

- Roles that an Application Role Inherits
- Roles that Inherit an Application Role

5.3.1 Roles that an Application Role Inherits

To view or modify the application role hierarchy below a given application role, proceed as follows:

1. Select an application role in the Search Results of the navigation panel, and double-click it or click Open to display the page for the application role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."

2. Bring the tab **Application Role Hierarchy** to the foreground and select **Inherits**.
3. The table in that region displays the application roles under the role.

   The actions at the top of this table allow:

   - Adding application roles (**Add**)
   - Removing a selected role (**Remove**)
   - Opening for viewing a selected role (**Open**)
   - Viewing the policies that contain a selected role (**View Policies**)

5.3.2 Roles that Inherit an Application Role

To view or modify the application role hierarchy above a given application role, proceed as follows:

1. Select an application role in the Search Results of the navigation panel, and double-click it or click Open to display the page for the application role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. Bring the tab **Application Role Hierarchy** to the foreground and select **Is Inherited By**.
3. The table in that region displays the application roles under the role.

   The actions at the top of this table allow:

   - Adding application roles (**Add**)
   - Removing a selected role (**Remove**)
   - Opening for viewing a selected role (**Open**)
   - Viewing the policies that contain a selected role (**View Policies**)

5.4 Mapping Application Roles to an External Role

To map application roles to an external role, proceed as follows:

1. Select the external role in the Search Results of the navigation panel, and double-click it or click Open to display the page for the external role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. In that page, select the **Role Mapping** tab.
3. In that tab, in the table in the area **External Role Hierarchy**, select **Map Roles** to display the Map Application Roles to External Roles dialog.
4. Use that dialog to search and select the application roles you want to map into the external role, and then click **Map Roles**. The current list of application roles mapped to the external role is shown in the table in the area **Application Role Hierarchy for:**.

   In addition, the actions at the top of the table allow:

   - Removing roles from the map (**Remove Roles**)
   - Opening a selected external role for view (**Open Role**)
   - Finding policies that contain a selected role (**Find Policies**)

5.5 Mapping External Roles to an Application Role

To map external roles to an application role, proceed as follows:

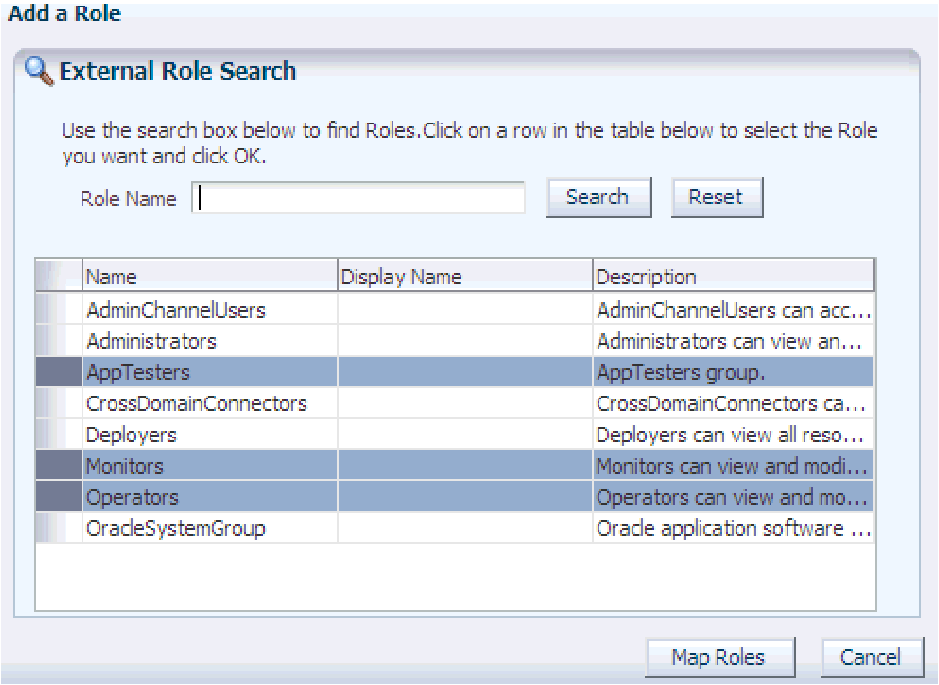
1. Select an application role in the Search Results of the navigation panel, and double-click it or click Open to display the page for the application role. For details, see Section 3.4, "Finding Artifacts with a Simple Search."
2. Bring the tab **External Role Mapping** tab to the foreground.
3. In that tab, click **Add** to display the **Add a Role** dialog. Use this dialog to search and select the set of external roles to be mapped to the application role; then click **Map Roles**.

   The table showing the external roles mapped to the application role is then updated to include the selected roles. In addition to adding external roles, the actions at the top of this table allow:

   - Removing a selected role (**Remove**)
   - Opening for viewing a selected role (**Open**)

Figure 5–7 illustrates the Add a Role dialog with results of an External Role Search and three external roles selected.

Figure 5–7 Selecting the External Roles to Map to an Application Role

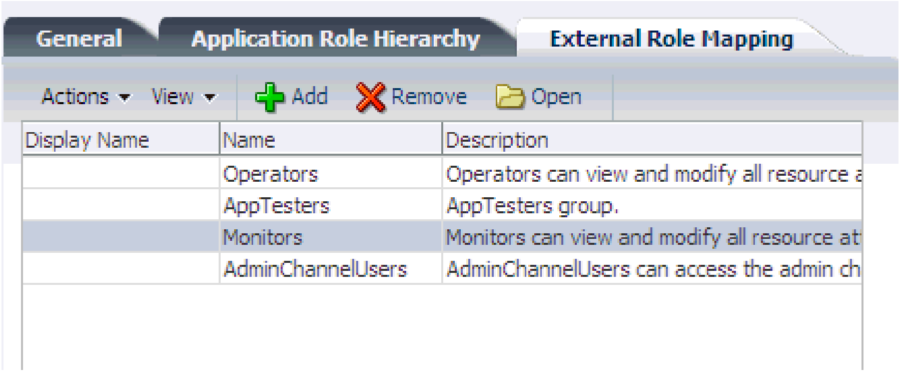


Use the search box below to find Roles.Click on a row in the table below to select the Role you want and click OK.

Name	Display Name	Description
AdminChannelUsers		AdminChannelUsers can acc...
Administrators		Administrators can view an...
AppTesters		AppTesters group.
CrossDomainConnectors		CrossDomainConnectors ca...
Deployers		Deployers can view all reso...
Monitors		Monitors can view and modi...
Operators		Operators can view and mo...
OracleSystemGroup		Oracle application software ...

Figure 5–8 illustrates the External Role Mapping tab displaying the external roles mapped to an application role.

Figure 5–8 Displaying the External Roles Mapped to an Application Role



Display Name	Name	Description
	Operators	Operators can view and modify all resource a
	AppTesters	AppTesters group.
	Monitors	Monitors can view and modify all resource at
	AdminChannelUsers	AdminChannelUsers can access the admin ch

An alternative way to add external roles to an application role (with the action menu **Add External Role)** is explained in Section 4.2, "Searching Application Roles."

6 Delegated Administration

This chapter describes a special role with permissions to manage a specified set of applications, so that only that role can view, access, and have administrator privileges to artifacts in the set of applications.

This chapter is divided into the following sections:

- Delegated Administrators
- Managing Delegated Administrators

6.1 Delegated Administrators

A delegated administrator is a role that can administer a given set of applications. A delegated administrator (and only a delegated administrator) can view or modify policies for that set of applications. Oracle Authorization Policy Manager allows you to specify delegated administrator roles, to determine which applications it can manage, and to map external roles to it. All these functions are available in the System Configuration tab.

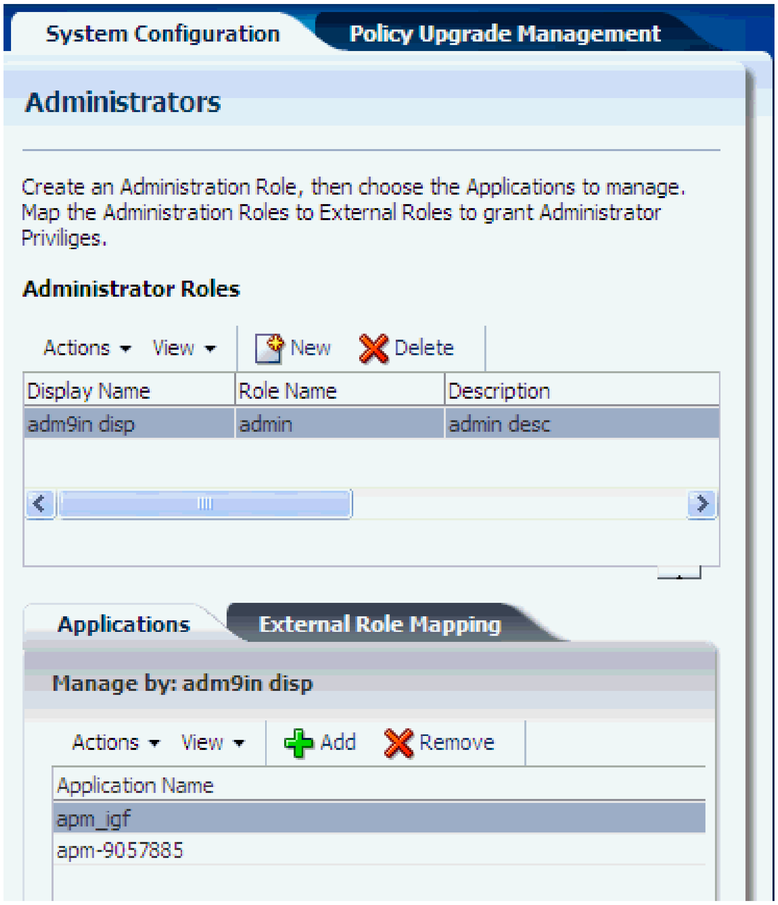
The Browser tab in the Navigation Panel displays only the set of application stripes that the logged in user is authorized to administer. All stripes that a delegated administrator *cannot* administer are also hidden in other pages, such as the page that displays how an external role maps to application roles in multiple stripes.

6.2 Managing Delegated Administrators

The System Configuration tab, partially illustrated in Figure 6–1, displays the current list of delegated administrator roles, the application stripes managed by a delegated administrator (in the Applications tab), and the external roles mapped into it (in the External Role Mapping tab). This page also allows creating a delegated administrator and modifying an existing one, as explained in the following sections:

- Managing Delegated Administrators
- Managing the Applications Assigned to a Delegated Administrator
- Managing the External Roles Mapped to a Delegated Administrator

Figure 6–1 The System Configuration Tab



Create an Administration Role, then choose the Applications to manage. Map the Administration Roles to External Roles to grant Administrator Priviliges.

Administrator Roles

Display Name	Role Name	Description
adm9in disp	admin	admin desc

Manage by: adm9in disp

Application Name
apm_igf
apm-9057885

6.2.1 Managing Delegated Administrators

To add a delegated administrator, proceed as follows:

1. Click the **System Configuration** tab.
2. In the **Administrator Roles** area, click **New** to display the **New Administrator Role** dialog.
3. In that dialog, enter a name, a display name, and (optionally) a description for the role being created, and then click **Save.** The table in the Administrator Roles area is updated to include the new role.

To remove a delegated administrator, proceed as follows:

1. Click the **System Configuration** tab.
2. In the **Administrator Roles** area, select an administrator from the list and click **Delete**.

6.2.2 Managing the Applications Assigned to a Delegated Administrator

To add an application to the set of applications managed by a delegated administrator, proceed as follows:

1. Click the **System Configuration** tab.

2. Select a delegated administrator role from the table in the **Administrator Roles** area.
3. Click the **Applications** tab, to display the current list of applications managed by the selected role.
4. Click **Add** to display the **Add Application** dialog showing the list of applications.
5. In that dialog, select the application(s) to include, and click **Add**. The list of applications in the Applications table is updated with the items you have selected.

To remove an application from the set of applications managed by a delegated administrator, proceed as follows:

1. Click the **System Configuration** tab.
2. Select a delegated administrator role from the table in the **Administrator Roles** area.
3. Click the **Applications** tab, to display the current list of applications managed by the selected role.
4. Select an application from the table, and click **Remove**.

6.2.3 Managing the External Roles Mapped to a Delegated Administrator

To map external roles to a delegated role, proceed as follows:

1. Click the **System Configuration** tab.
2. Select a delegated administrator role from the table in the **Administrator Roles** area.
3. Click the **External Role Mapping** tab, to display the current list of external roles mapped by the selected role.
4. Click **Add** to display the **Add a Role** dialog.
5. In that dialog, search and select the external roles to add to the map, and click **Map Roles**. The list of roles in the External Role Mapping table is updated with the items you have selected.

To remove an external role from the list of external roles mapped to a delegated role, proceed as follows:

1. Click the **System Configuration** tab.
2. Select a delegated administrator role from the table in the **Administrator Roles** area.
3. Click the **External Role Mapping** tab, to display the current list of external roles mapped by the selected role.
4. Select a role from the table, and click **Remove**.

7 Upgrading Oracle Fusion Applications Policies

The information in this chapter is specific to Oracle Fusion Applications only.

This chapter describes how to use Oracle Authorization Policy Manager to upgrade application policies in an LDAP-based domain policy store with the changes introduced by a new release of the application.

Details are explained in the following sections:

7.1 Overview

First we introduce some terms used throughout this chapter, and then an overview of the process of upgrading the policy store.

7.1.1 Terminology

The following terms refer to the three policy stores involved in an application policy upgrading. They are also used in the Oracle Authorization Policy Manager user-interface.

Baseline - The original policy store, represented by the XML file `jazn-data.xml` and available with the application out-of-the-box. Presumably, this policy store was migrated to the domain policy store when the application was first deployed.

Production - The domain policy store, where the current state of application policies reside. This store is assumed LDAP-based. Presumably, policies in the application stripe in this store has undergone modifications since the application was first deployed.

Patch - The policy store of the new version of the application, represented by the XML file `jazn-data.xml` and available with the new application out-of-the-box.

7.1.2 Upgrading Process Overview

Application policy upgrading allows security administrators to solve the following problem, with which they are faced every time a new version of an application is released.

Out-of-the-box, an application typically includes the file `jazn-data.xml` (baseline policy store) that describes the application policies for that particular version of the application. Typically, at application deployment the baseline policy store is migrated to the domain policy store (production policy store) for the first time.

Thereafter, application policies in the production store may undergo modifications to accommodate evolving requirements; these changes include adding, deleting, or modifying any application-specific security artifact such as roles, grants, resource types, resources, and entitlements.

When a new version of the application is available and before that new version is deployed, a security administrator needs to:

- Identify the customizations that have been introduced since the migration of the old application version, that is, the delta between the baseline and the production stores.
- Identify the differences between the customized application policies and the policies in the new application version, that is, the delta between the production and patch stores.
- Decide, for each difference, which artifact to use.

Oracle Authorization Policy Manager facilitates the resolution of each of the above tasks by providing a security administrator with a user interface that allows him to:

- Analyze a new patch, that is, generate all differences.
- Inspect and decide, for each difference reported by the analysis, which specification to use.
- Apply the patch.

> **Important:** Before patching application policies, make sure that you backup the policy store as explained in Prerequisites to Patching Policies.

7.2 Prerequisites to Patching Policies

The analysis must be performed first. The resolution of changes and conflicts is performed next. These tasks do not have any particular requirements and can be accomplished at different times during one Oracle Authorization Policy Manager session or even across different sessions.

Before applying a patch, however, proceed as follows:

1. Take off line any WebLogic domain that uses the policy store where the application policies to be patched reside.
2. Backup the policy store by using either of the following tools:
    1. Oracle Internet Directory `ldifwrite` to obtain an LDIF file for the policy store. For an example of use of this command, see *Oracle Fusion Middleware Application Security Guide*.

2. Oracle Platform Security Services `migrateSecurityStore` to export the policy store into a replica of it. For details about this command, see *Oracle Fusion Middleware Application Security Guide*.

Now you can apply the patch.

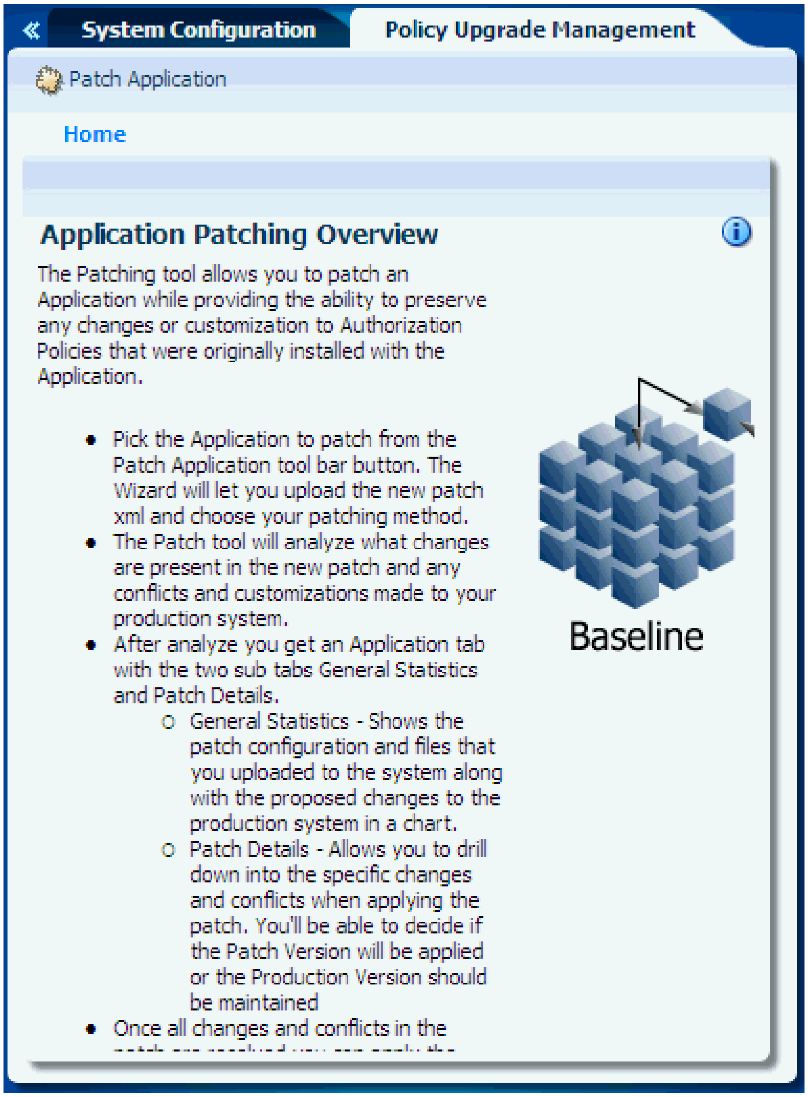
If for any reason the policy store needs to be restored, proceed as follows:

1. If you have saved the policy store in an LDIF file, use `bulkload` to restore it. For details about this command, see *Oracle Fusion Middleware Application Security Guide*.
2. If you have exported the policy store, use Oracle Platform Security Services `migrateSecurityStore` to restore it. For details about this command, see *Oracle Fusion Middleware Application Security Guide*.

7.3 The Policy Upgrade Management Tab

The **Policy Upgrade Management** tab, partially illustrated in Figure 7–1, contains the tab **Home**, where the upgrading process begins and which succinctly describes the steps you follow to upgrade application policies. The first step is to select the application whose policies to upgrade.

Figure 7–1 The Policy Upgrade Management Tab



Application Patching Overview

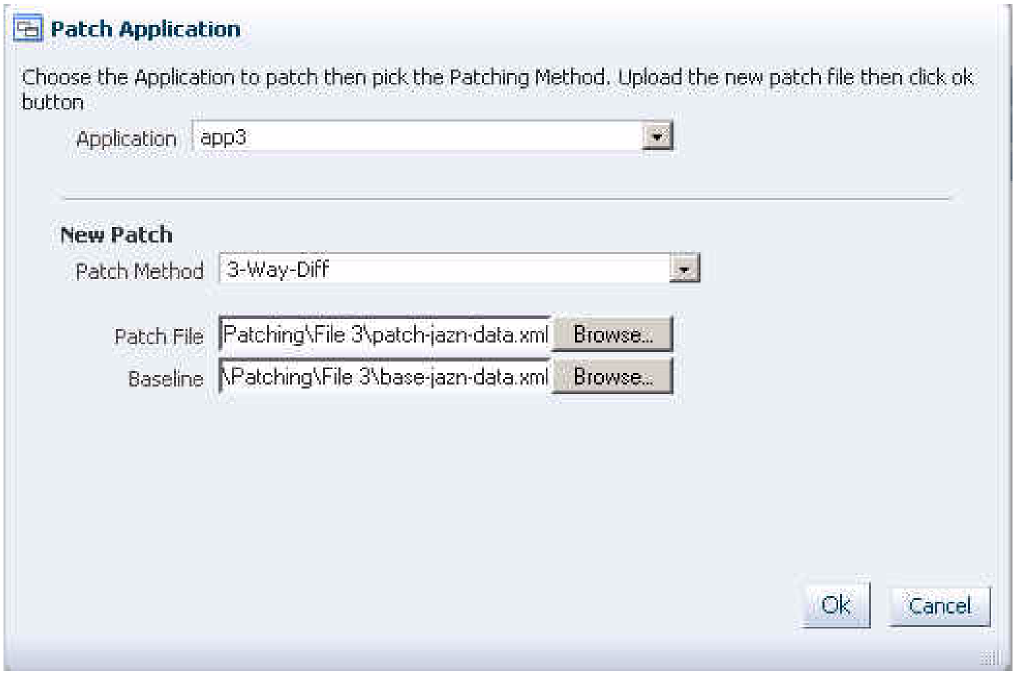
The Patching tool allows you to patch an Application while providing the ability to preserve any changes or customization to Authorization Policies that were originally installed with the Application.

- Pick the Application to patch from the Patch Application tool bar button. The Wizard will let you upload the new patch xml and choose your patching method.
- The Patch tool will analyze what changes are present in the new patch and any conflicts and customizations made to your production system.
- After analyze you get an Application tab with the two sub tabs General Statistics and Patch Details.
    - General Statistics - Shows the patch configuration and files that you uploaded to the system along with the proposed changes to the production system in a chart.
    - Patch Details - Allows you to drill down into the specific changes and conflicts when applying the patch. You'll be able to decide if the Patch Version will be applied or the Production Version should be maintained
- Once all changes and conflicts in the patch are resolved you can apply the

To select application policies to patch, proceed as follows:

1. In the Home tab of the Policy Upgrade Management page, click the button **Patch Application** at the top left corner of the page to bring up the **Patch Application** dialog illustrated in Figure 7–2.

Figure 7–2 Patch Application Dialog



Patch Application

Choose the Application to patch then pick the Patching Method. Upload the new patch file then click ok button

Application: app3

New Patch

Patch Method: 3-Way-Diff

Patch File: Patching\File 3\patch-jazn-data.xml

Baseline: \Patching\File 3\base-jazn-data.xml

2. In this dialog, select the application to patch from the pull-down **Application** list. Since this list shows the applications currently deployed in the domain, to allow selecting it, the application must be deployed.

   Once you selected the application, the dialog takes a different form according to whether or not the application selected has a patching in progress:

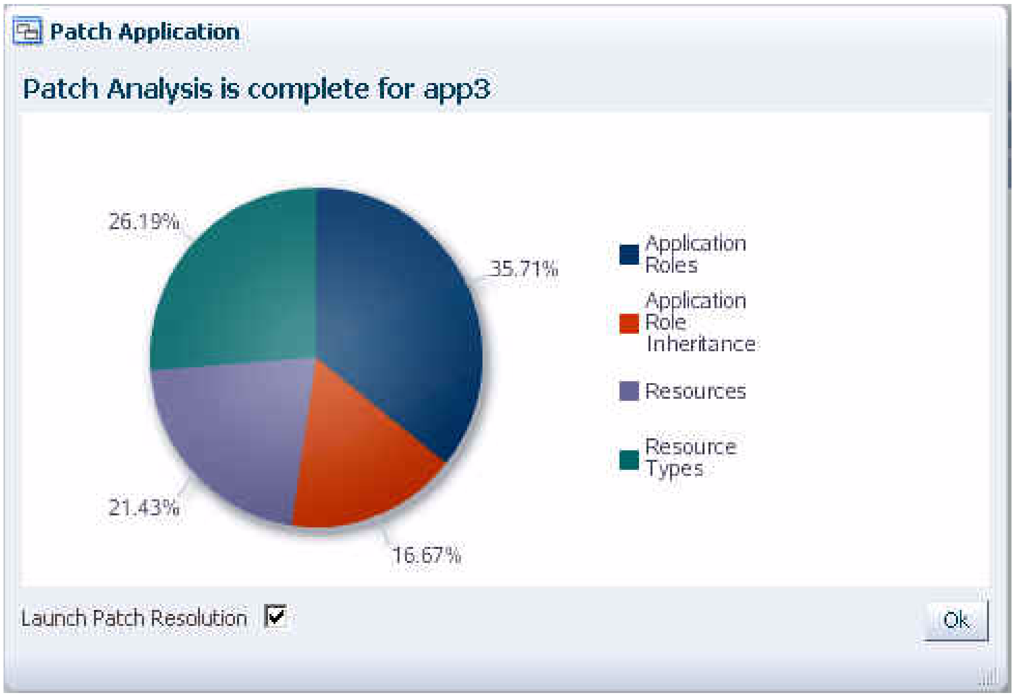
   - If the application has a patching in progress, then you can continue with it or abort it.
   - Otherwise, if the application does not have a patching in progress, then you can initiate a new patching process by selecting the **Baseline** file, the **Patch file,** and then click **OK**. The only **Patch Method** available in this release is a 3-way DIFF, which considers differences between the baseline, the production, and the patch stores.

   The **Baseline** specifies the location of the baseline policy store.

   The **Patch file** specifies the location of the patch policy store.

3. From here on, it is assumed that you have started a new patching process. Oracle Authorization Policy Manager displays an indicator showing the progress of the analysis phase in the Patch Application dialog. Once this phase is completed, the Patch Application dialog displays the statistics of the analysis as illustrated in Figure 7–3.

Figure 7–3 Statistics of a Patch Analysis



Patch Application

Patch Analysis is complete for app3

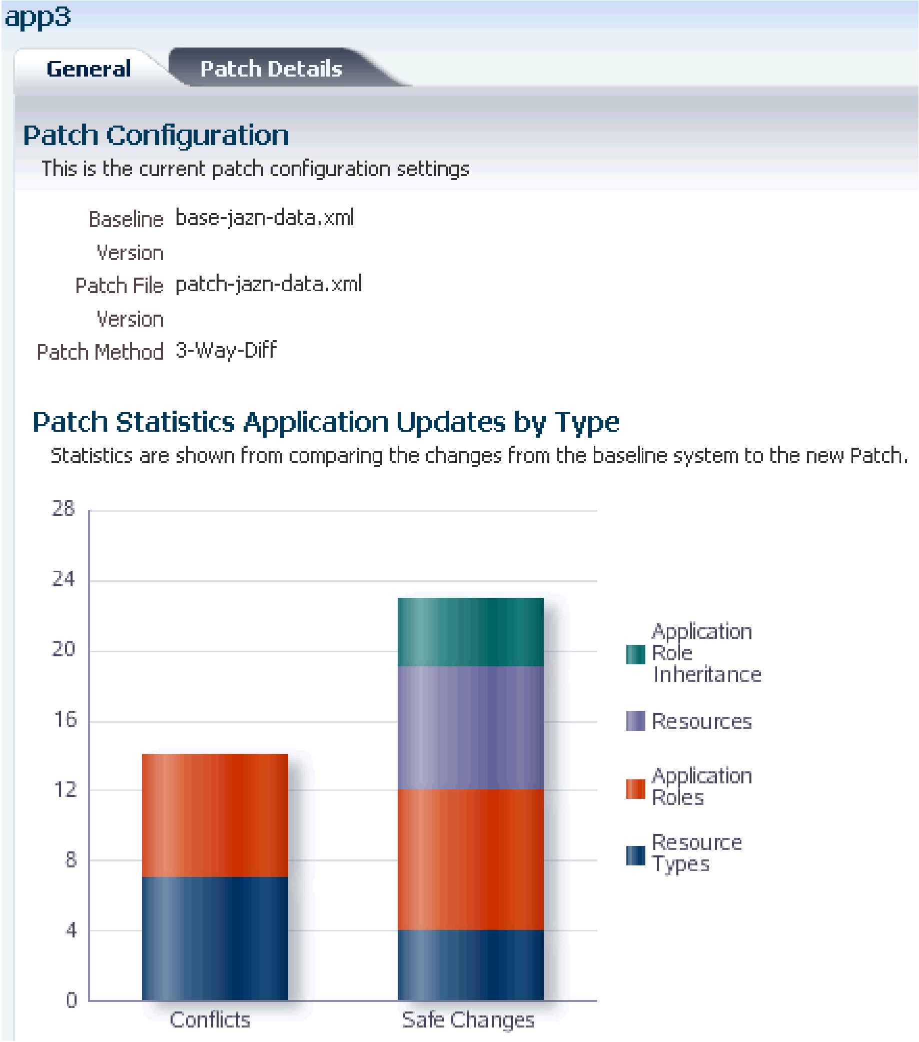
Launch Patch Resolution ☑

4. To launch the patch resolution phase, check the box **Launch Patch Resolution** (checked by default), and then click **OK**.

   Oracle Authorization Policy Manager then creates a new tab (named after the application display name) that contains the details of the results, that is, the conflicts and differences encountered, in two sub-tabs:

   - **General** - This tab displays the files you have specified at the start of the patching and a chart showing the number changes and conflicts found, per artifacts, between the baseline and the patch stores. For details about these terms, see Changes and Conflicts. Figure 7–4 illustrates the General tab.

Figure 7–4 The General Tab



app3

General | Patch Details

Patch Configuration

This is the current patch configuration settings

Baseline Version: base-jazn-data.xml

Patch File Version: patch-jazn-data.xml

Patch Method: 3-Way-Diff

Patch Statistics Application Updates by Type

Statistics are shown from comparing the changes from the baseline system to the new Patch.

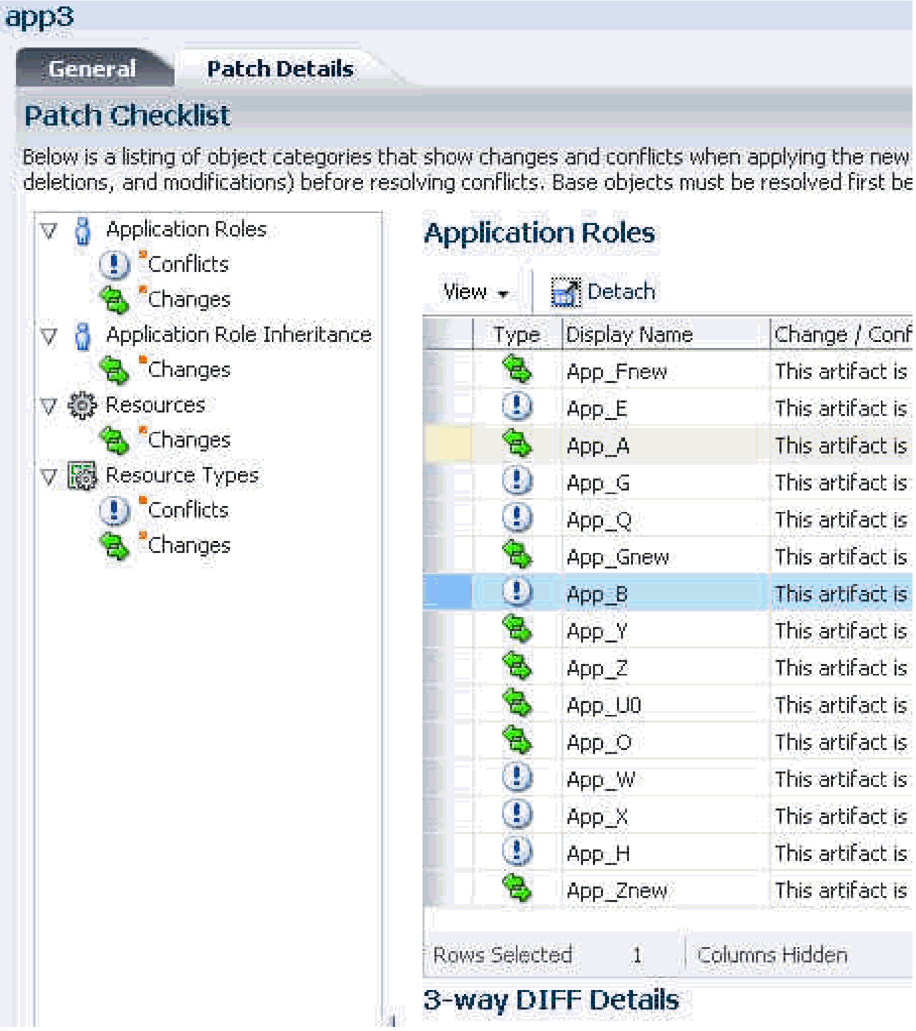
To terminate the current patching process and to delete the analysis data gathered thus far, click the button **Discard**; once the patch is discarded, the tab for the application is deleted from the Patching tab.

- **Patch Details** - This tab displays the proposed changes and conflicts encountered per security artifact. The details of this tab are explained in the next section.

7.4 Analyzing Patch Differences

The **Patch Details** tab, illustrated partially in Figure 7–5, contains two major areas: the left area displays a hierarchical overview of changes and conflicts per artifact that resulted from the comparisons; the right area displays the details of changes and conflicts for an artifact selected from the left area.

Figure 7–5 The Patch Details Tab



Below is a listing of object categories that show changes and conflicts when applying the new deletions, and modifications) before resolving conflicts. Base objects must be resolved first be

Application Roles

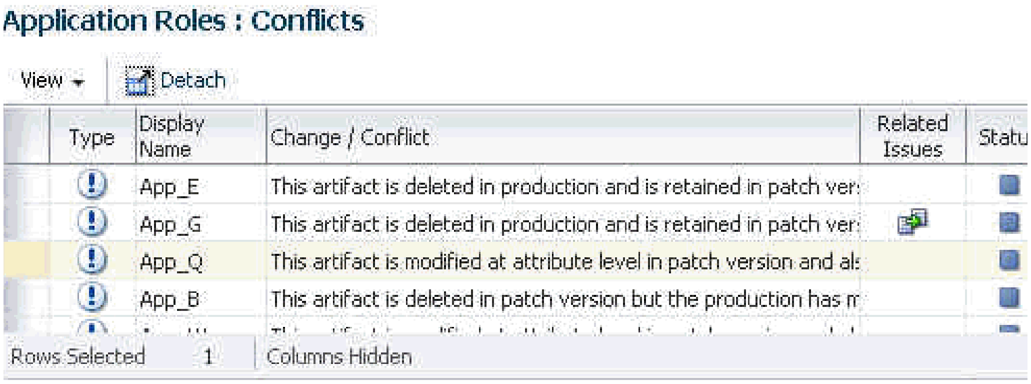
Type	Display Name	Change / Conf
⇄	App_Fnew	This artifact is
!	App_E	This artifact is
⇄	App_A	This artifact is
!	App_G	This artifact is
!	App_Q	This artifact is
⇄	App_Gnew	This artifact is
!	App_B	This artifact is
⇄	App_Y	This artifact is
⇄	App_Z	This artifact is
⇄	App_U0	This artifact is
⇄	App_O	This artifact is
!	App_W	This artifact is
!	App_X	This artifact is
!	App_H	This artifact is
⇄	App_Znew	This artifact is

To view the specifics of an object's differences, click **Changes** or **Conflicts** under the object; the differences are then displayed in the right area of the tab. Each row in the table identifying a difference has a type that indicates whether the difference is a change (double arrow icon) or a conflict (exclamation mark icon). For details about these terms, see Changes and Conflicts.

To view a change or conflict for an artifact, select the corresponding icon (Changes or Conflicts) under the artifact. All changes or conflicts are then displayed in a table at the top of the page.

Figure 7–6 partially illustrates the page showing role conflicts.

Figure 7–6 Viewing Artifact Conflicts



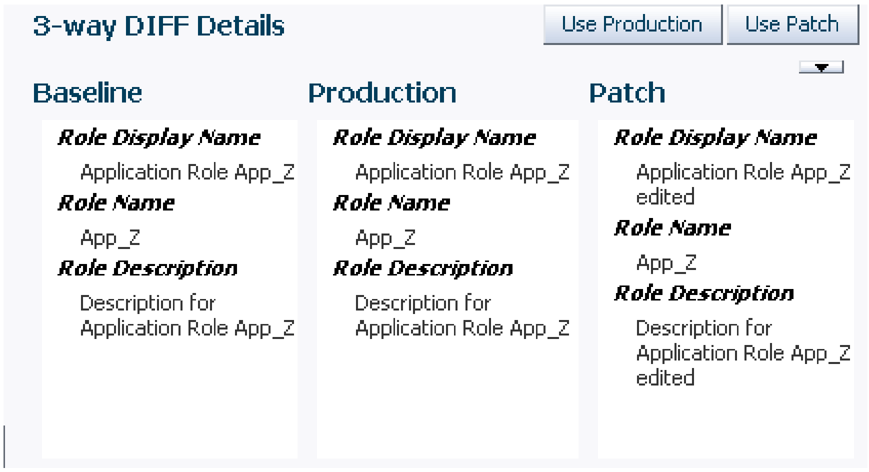
Application Roles : Conflicts

Type	Display Name	Change / Conflict	Related Issues	Statu
!	App_E	This artifact is deleted in production and is retained in patch ver:		■
!	App_G	This artifact is deleted in production and is retained in patch ver:	⧉	■
!	App_Q	This artifact is modified at attribute level in patch version and al:		■
!	App_B	This artifact is deleted in patch version but the production has m		■

Rows Selected 1 Columns Hidden

To view conflict details for a specific item in the table, select the item to display the different specifications found in the 3-Way DIFF Details area. Figure 7–7 illustrates the differences for a role.

Figure 7–7 Displaying Difference Details



3-way DIFF Details

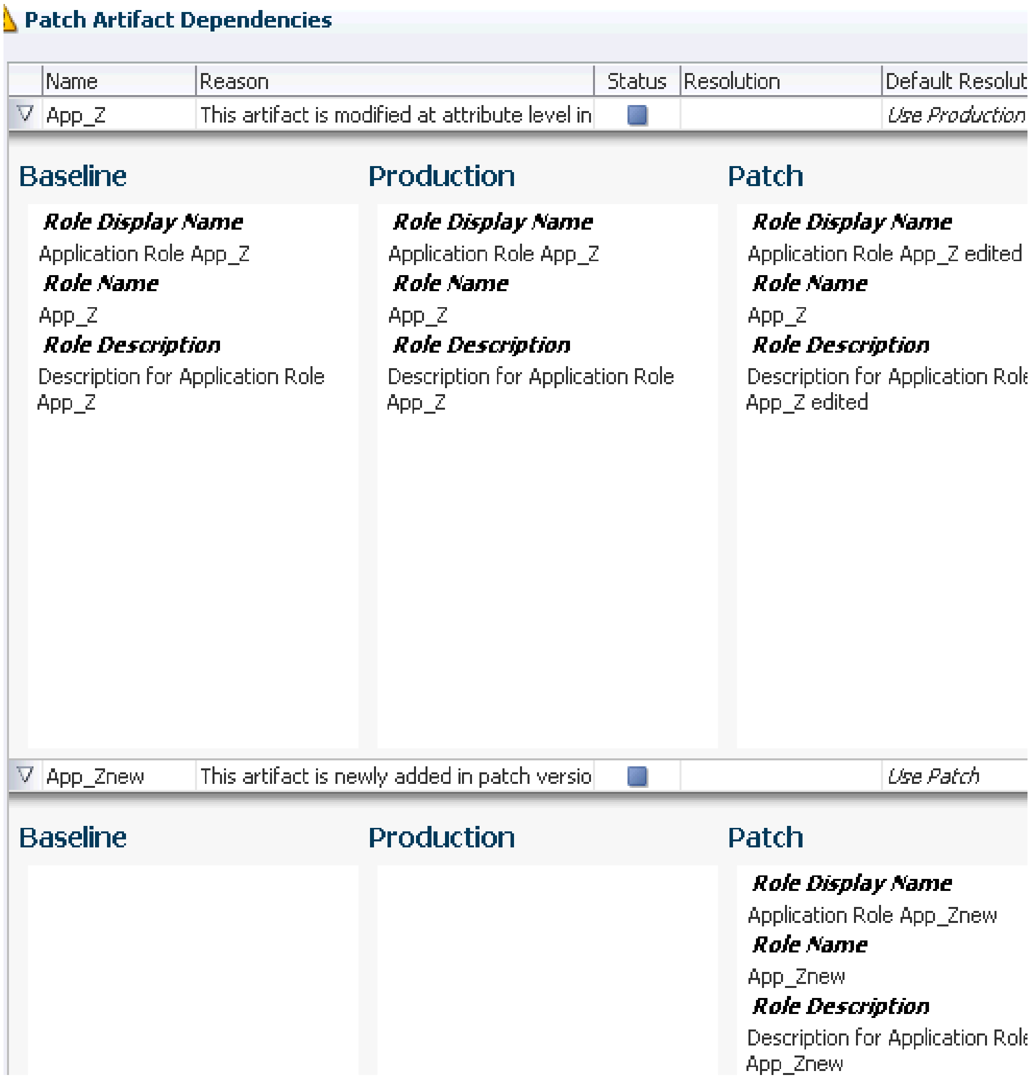
Baseline	Production	Patch
Role Display Name	***Role Display Name***	***Role Display Name***
Application Role App_Z	Application Role App_Z	Application Role App_Z edited
Role Name	***Role Name***	***Role Name***
App_Z	App_Z	App_Z
Role Description	***Role Description***	***Role Description***
Description for Application Role App_Z	Description for Application Role App_Z	Description for Application Role App_Z edited

The **Status** column shows whether a change or a conflict has been resolved (green check icon) or not (gray square icon).

The **Related Issues** column shows whether a change or conflict has implied dependencies; to view them, click the icon in this column to display the **Patch Artifact Dependencies** dialog, which displays, among other information, the reasons why other artifacts would be affected when resolving a difference for an artifact.

Figure 7–8 partially illustrates the dependencies implied by differences in a pair of roles. Specifically, it illustrates a baseline role App_Z that is not modified in the production store but modified in the patch store as follows: (a) the display name and the role description are changed; and (b) the new role App_Znew is a child of the role App_Z.

Figure 7–8 Viewing Dependencies Implied by a Conflict or Change



Patch Artifact Dependencies

	Name	Reason	Status	Resolution	Default Resolut
▽	App_Z	This artifact is modified at attribute level in	■		*Use Production*

Baseline

Role Display Name
Application Role App_Z
Role Name
App_Z
Role Description
Description for Application Role App_Z

Production

Role Display Name
Application Role App_Z
Role Name
App_Z
Role Description
Description for Application Role App_Z

Patch

Role Display Name
Application Role App_Z edited
Role Name
App_Z
Role Description
Description for Application Rol
App_Z edited

	Name	Reason	Status	Resolution	Default Resolut
▽	App_Znew	This artifact is newly added in patch versio	■		*Use Patch*

Baseline

Production

Patch

Role Display Name
Application Role App_Znew
Role Name
App_Znew
Role Description
Description for Application Rol
App_Znew

7.5 Resolving Patch Differences

A patch difference identifies a disparity between the specifications of a security artifact in the some of the policy stores involved in the analysis. Oracle Authorization Policy Manager lists patch differences as changes or conflicts. These terms and how to resolve them are explained in the following sections:

- Changes and Conflicts
- Resolving Changes and Conflicts

7.5.1 Changes and Conflicts

To better explain the terminology used, assume that Abase, Aprod, and Apatch denote the states of an artifact in the baseline, production, and patch stores, respectively.

A patch difference is called a *change* when Abase and Apatch are equal, and Aprod is different to Apatch.

A patch difference is called a *conflict* when Abase and Apatch are different, and Aprod is different from Apatch.

7.5.2 Resolving Changes and Conflicts

Resolving an artifact change or conflict means choosing which specification to use: the one in the production store or the one in the patch store.

Even though there is a default resolution for each artifact change or conflict, it is recommended that all changes and conflicts be resolved manually before you proceed forward to applying the patch.

To resolve a change or conflict for an artifact, proceed as follows:

1. Select the artifact in the **Conflicts** table, to display the specifications for the artifact found in each of the three stores at the bottom of the page.
2. Inspect specification differences and decide which one to use; to use the production store, click the button **Use Production**; to use the specification in the patch store, click the button **Use Patch**.

   > **Important Note:** The decision that you make in this step may imply necessary changes to other artifacts. These changes, necessary to preserve data consistency, are called *dependencies*.
   >
   > Oracle Authorization Policy Manager displays the dependencies that a decision implies and requests your confirmation before setting the value.

The decision value set for a change or conflict can be reset at any time. To any change or conflict left unresolved, Oracle Authorization Policy Manager sets one of the following default values:

- For a change, Use Patch.
- For a conflict, Use Production.

7.6 Applying a Patch

The procedure in this section assumes that:

- All changes and conflicts reported in the Patch Checklist of the Patch Details tab have been resolved (manually or by default).
- The prerequisites stated in Prerequisites to Patching Policies are met.

To apply a patch, proceed as follows:

1. Click the button **Apply Patch** in the application's patching tab to initiate the patching process, which will modify the application policy stripe in the domain LDAP store.
2. Once the application of the patch is completed, you are ready to deploy the new version of the application.

   Make sure that when deploying it, *the automatic migration of policies is turned off* so that the just patched application policies are not modified when the application is deployed.

For details about how to manage the migration of policies when the application is deployed with Oracle Enterprise Manager Fusion Middleware Control, see *Oracle Fusion Middleware Application Security Guide*

8 Customizing the User Interface

This chapter explains several customizations available in Oracle Authorization Policy Manager in the following sections:

- Customizing Oracle Authorization Policy Manager
- Customizing Headers, Footers, and Logo
- Customizing Color Schemes
- Customizing the Login Page

8.1 Customizing Oracle Authorization Policy Manager

All customizations described in this chapter require modifying data in the following files:

```
$ORACLE_HOME$/apm/modules/oracle.security.apm_11.1.1/oracle.security.apm.ear
$ORACLE_HOME$/apm/modules/oracle.security.apm_
11.1.1/oracle.security.apm.core.view.war
```

Customizations applied to a version of Oracle Authorization Policy Manager need to be specified anew every time a new version of the tool is installed.

Before you begin customizing Oracle Authorization Policy Manager, it is recommended that you backup the tool's EAR and the view WAR files listed above.

To customize Oracle Authorization Policy Manager, proceed as follows:

1. Unzip the tool's EAR and WAR files, and the view WAR file, as illustrated by the following commands:

   ```
   $ unzip -d $tempDir/ear $ORACLE_HOME$/apm/modules/oracle.security.apm_
   11.1.1/oracle.security.apm.ear
   $ unzip -d $tempDir/war $tempDir/ear/oracle.security.apm.war
   $ unzip -d $tempDir/viewWar $ORACLE_HOME$/apm/modules/oracle.security.apm_
   11.1.1/oracle.security.apm.core.view.war
   ```

2. Modify one or more unzipped files, as explained in the remaining sections of this chapter.

3. Zip anew the tool's EAR and WAR files, and the view WAR file, as illustrated by the following commands:

   ```
   $ zip $tempDir/ear/oracle.security.apm.war $tempDir/war/*
   $ zip $ORACLE_HOME$/apm/modules/oracle.security.apm_
   11.1.1/oracle.security.apm.ear $tempDir/ear/*
   $ zip $ORACLE_HOME$/apm/modules/oracle.security.apm_
   11.1.1/oracle.security.apm.core.view.war $temp/viewWar/*
   ```

4. Redeploy Oracle Authorization Policy Manager.

8.2 Customizing Headers, Footers, and Logo

To customize headers, footers, and logo, proceed as follows:

1. Unzip the view WAR file. For details, see Customizing Oracle Authorization Policy Manager.
2. Open for edit the file `AuthPolicyMgr.jspx` and apply any of the following modifications, as appropriate.
3. To specify a new branding title, modify the `branding` facet as illustrated in the following snippet:

```
<f:facet name="branding">
 <af:outputText value="My Custom Application Title" noWrap="true" id="ot1"/>
</f:facet>
```

4. To specify a new footer, modify the `appAbout` and `appCopyright` facets as illustrated in the following snippet:

```
<f:facet name="appAbout">
  <af:outputText value="My Custom Footer at Right" noWrap="true" id="ot2"/>
</f:facet>
<f:facet name="appCopyright">
  <af:outputText value="My Custom Footer at Left"  noWrap="true" id="ot3"/>
</f:facet>
```

5. To specify a new logo image, proceed as follows:
   1. Insert your resource in the `metaContainer` facet as illustrated in the following snippet (leave all other content inside the facet as is):

   ```
   <f:facet name="metaContainer">
   ....
     <af:resource type="css">
               .MyCustomBrandingLogo {
                   background-image:url(/apm/images/world_36x20.png);
                   background-position:center;
                   background-repeat:no-repeat; display:block;
                   height:2.5em; width:119px;
                 }
     </af:resource>
   ...
   </f:facet>
   ```

   2. Specify that style class name as the input attribute to the `pageTemplate` tag, as illustrated in the following snippet (leave all other content inside the tag as is):

   ```
   <af:pageTemplate viewId="/templates/IdmShell.jspx"
                          value="#{bindings.pageTemplateBinding}" id="pt1">
   ...
     <f:attribute name="brandingLogoCls" value="MyCustomBrandingLogo"/>
   ...
   ```

8.3 Customizing Color Schemes

Assuming that you have a new skin available, to customize the color scheme, proceed as follows:

1. Unzip the tool's EAR and WAR files. For details, see Customizing Oracle Authorization Policy Manager.

2. Open for edit the file `Trinidad-config.xml`, typically located in the folder `WAR/WEB-INF.`

3. In that file, specify the value of the new skin in the `skin-family` tag, as illustrated in the following snippet:

```
<trinidad-config xmlns="http://myfaces.apache.org/trinidad/config">
...
  <skin-family>MyCustomSkin</skin-family>
...
</trinidad-config>
```

8.4 Customizing the Login Page

To customize the login page and login error page, proceed as follows:

1. Unzip the tool's EAR file. For details, see Customizing Oracle Authorization Policy Manager.

2. Open for edit the file `web.xml`, typically located in the folder `EAR/WEB-INF.`

3. In that file, specify the appropriate values for the `form-login-page` and `form-error-page`, under the element `form-login-config`, as illustrated in the following snippet:

```
<login-config>
  <form-login-config>
    <form-login-page>/MyCustomLoginPage.html</form-login-page>
    <form-error-page> MyCustomLoginErrorPage.html </form-error-page>
  </form-login-config>
</login-config>
```

9 Internationalization

Oracle Authorization Policy Manager uses Globalization Support to handle data in one of several languages. Globalization Support allows Oracle Authorization Policy Manager to display text, such as role and user names, in a one of those languages.

9.1 Language Support

Oracle Authorization Policy Manager determines the language in which text is displayed from the setting of the browser locale.

Oracle Authorization Policy Manager supports the following standard administrator languages: English, Portuguese, French, German, Italian, Japanese, Korean, Spanish, and Chinese.

When your browser locale is set to one of the above supported administrator languages, then the text that Oracle Authorization Policy Manager displays is in that language. In this way, an administrator can specify the language in which pages are displayed.

10

Oracle Fusion Applications Data Role Templates

The information in this chapter is specific to Oracle Fusion Applications only.

This chapter describes what data role templates are and the procedures to create, run, and maintain them, in the following sections:

- Prerequisites for Using Templates
- Template Overview
- Creating a Template
- Running a Template
- Updating a Template
- Importing and Exporting a Template

10.1 Prerequisites for Using Templates

In addition to the data source listed in Chapter 1.1, "Audience and Prerequisites," the use of templates requires two other data sources as described in Table 10–1:

Table 10–1 Data Sources Required by Templates

Data Source Name	JNDI Name	Description
ApmRgxDimDBDS	jdbc/ApmRgxDimDBDS	Used by role templates to execute dimension SQLs.
ApplicationDB	jdbc/ApplicationDBDS	Stores role template records to create security artifacts.

All data sources can be configured with the WebLogic Console by navigating to **JDBC > Data Sources**. The data source ApmRgxDimDBDS must be created with a credential that includes the database writing privilege.

10.2 Template Overview

A template or data role template specifies key characteristics of external roles and data security policies. When run, it generates all the external roles and the data security policies that satisfy the values in the template. The external roles generated (by a template run) are stored in the domain identity store; the data security policies generated are stored in the data security store; templates are stored in the metadata storage (MDS).

The basic principle behind the generation of external roles and data policies is that given:

- A set of base external roles
- A set of dimension values
- A set of naming rules

one can take the cross product of the first two sets (external roles times dimension values) to obtain a set of external roles named according to the naming rules, and associate them with a set of permissions, for a given data stripe, in data security policies.

The external roles and the data security policies that a template run generates are specified as a set of external roles and a set of dimensions (rows or attributes returned by an SQL query). Each dimension attribute is associated with an alias, which is used (by the naming conventions) to generate names for the roles and data security policies generated.

A dimension attribute can be the attribute return by an SQL query, such as, the following:

```
where territory=US, business unit=Finance, and legal entity=North America
```

The number of external roles generated equals the number of specified external roles times the number of rows returned by the query (or number of dimensions). Each external role generated inherits from the corresponding specified external role.

For example, a template specifying the external roles Employee-Role and Manager-Role, the dimensions US and UK, and the naming rule [external role]:[dimension code name] would generate the following four external roles:

Employee-Role:US, Employee-Role:UK, Manager-Role:US, Manager-Role:UK

Each of the four generated role inherits from one of the specified external roles, Employee-Role or Manager-Role.

The list of external roles and data security policies that a template run generates can be previewed, that is, displayed *before* the actual creation of roles and associated data security policies takes place.

10.3 Creating a Template

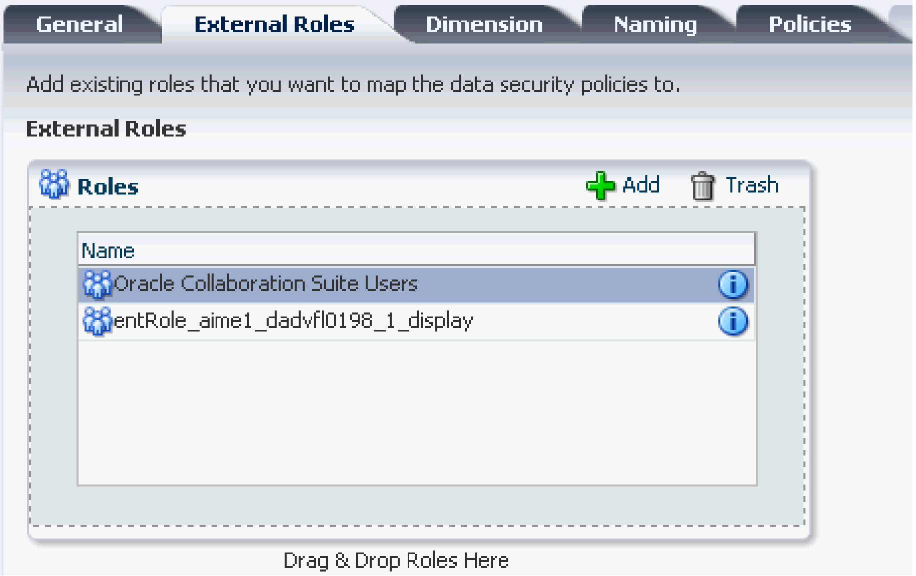
To create a new template, proceed as follows:

1. Select **Global > Role Templates**, in the left panel, and then click **New** to display an Untitled page in the right panel containing six tabs: General, External Roles, Dimension, Naming, Policies, and Summary.
2. In the **General** tab, enter the following data for the template being created:
    - A display name (required)
    - A name (required)
    - A description (optional)
    - A template group (optional) - This attribute allows searching templates by group and running simultaneously the set of templates in a group.
3. In the **External Roles** tab, specify the external roles for the template in one of the following ways:

- Click **Add**, at the top of the Roles area, to display bring up the **Add External Role** dialog where you can search for external roles matching a given pattern; then select roles from the results of the query and click Add. The role(s) selected are displayed in the **Roles** table.
- Perform a regular search for external roles and drag-and-drop the desired roles from the Search Results list into the **Roles** table.

Figure 10–1 illustrates the Roles table in the External Roles tab after two external roles have been added to the table. When the mouse hoovers the blue icon, at the right of a role row, the following information about the role is displayed: the role code, the role name, and the role description; these three attributes can always be used in the Naming tab to specify the names of generated roles.

Figure 10–1 Creating a Template - Specifying External Roles



Add existing roles that you want to map the data security policies to.

External Roles

Name
Oracle Collaboration Suite Users
entRole_aime1_dadvfl0198_1_display

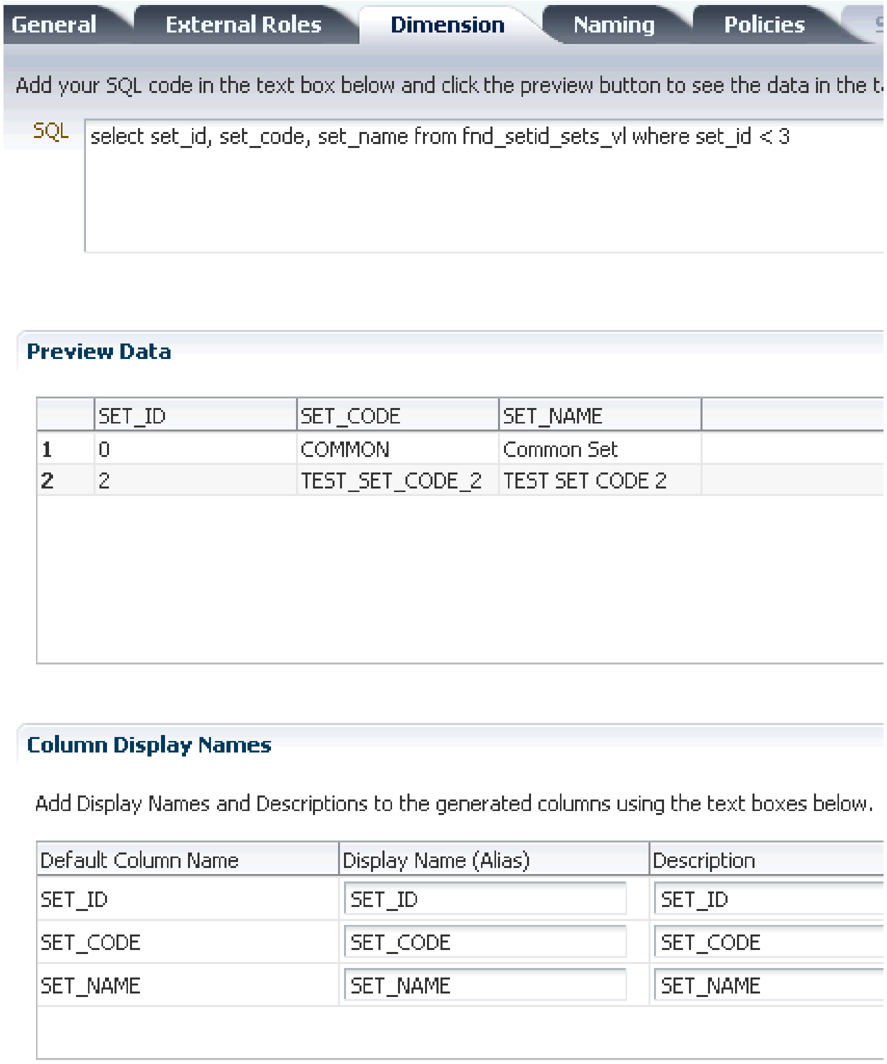
Drag & Drop Roles Here

4. In the **Dimension** tab, specify the SQL that identifies the dimensions of the template. The data returned by that SQL is displayed in the **Preview Data** table. Optionally, enter aliases for the column names of the returned data in the **Column Display Names** table, at the bottom of the page.

   The user must have access privilege to the data queried.

   Figure 10–2 illustrates the Dimension tab with an SQL query, the data returned by it, and display name aliases; the attributes SET_ID, SET_CODE, and SET_NAME can be used in the Naming tab to specify the names of generated roles.

Figure 10–2 Creating a Template - Specifying Dimensions



Add your SQL code in the text box below and click the preview button to see the data in the t

SQL select set_id, set_code, set_name from fnd_setid_sets_vl where set_id < 3

Preview Data

	SET_ID	SET_CODE	SET_NAME
1	0	COMMON	Common Set
2	2	TEST_SET_CODE_2	TEST SET CODE 2

Column Display Names

Add Display Names and Descriptions to the generated columns using the text boxes below.

Default Column Name	Display Name (Alias)	Description
SET_ID	SET_ID	SET_ID
SET_CODE	SET_CODE	SET_CODE
SET_NAME	SET_NAME	SET_NAME

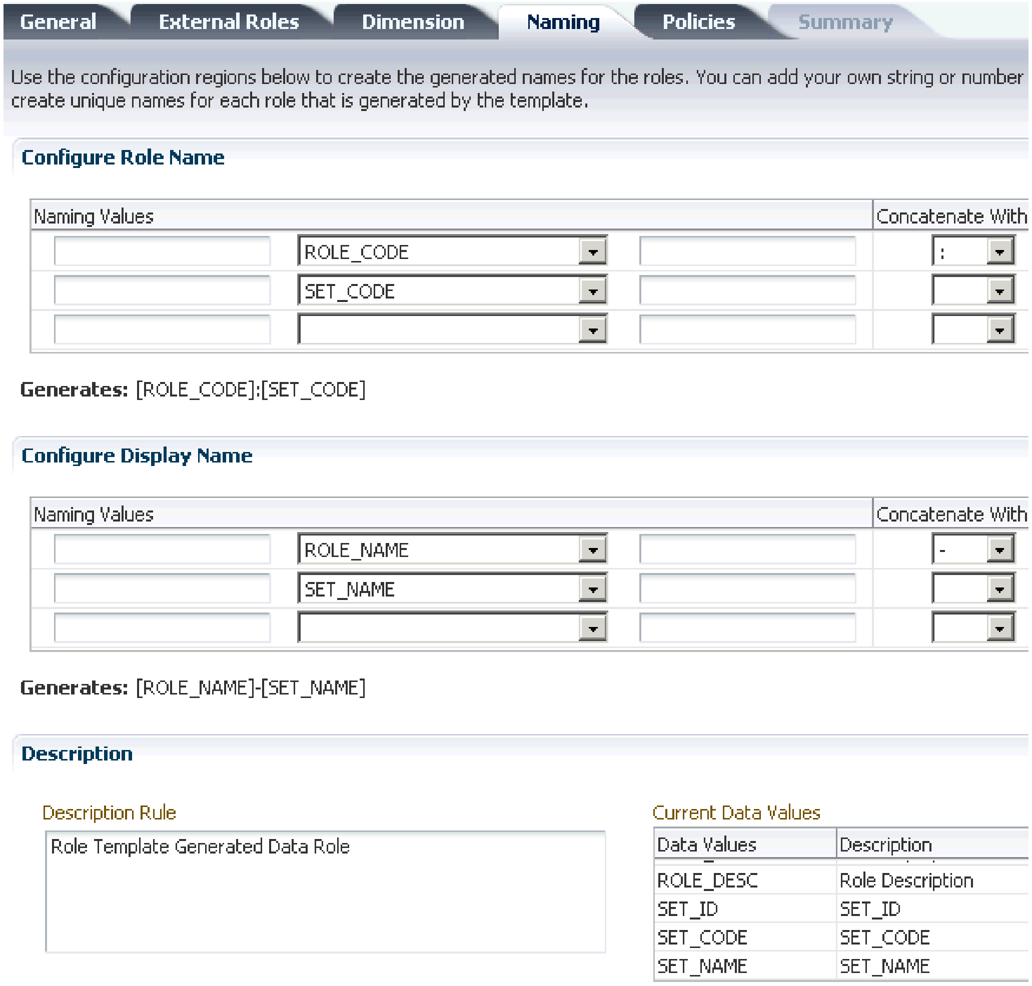
5. In the **Naming** tab, specify the rule to follow to generate names of the data roles created by the template. These names are put together by concatenating several strings that you specify in the area **Configure Role Name**. Typically, one chooses an attribute of the base role and an attribute of the dimension (such as SET_ID, SET_CODE, or SET_NAME in Figure 10–2); the role attributes Role_Code, Role_Name, and Role_Descrip are available by default. The resulting names must be unique.

   Similarly, specify the rule to follow to generated display names for the data roles created by the template. These names are put together by concatenating several strings that you specify in the area **Configure Display Name**. The resulting names need not be unique, but it is recommended that you specify enough attributes to make them unique too.

   Optionally, enter a description for the roles generated in the area **Description**.

   Figure 10–3 illustrates a portion of a Naming tab with naming values for the names and the display names for the external roles generated by the template. Note the following points: (a) the pattern of the concatenation is shown at the bottom of each area after the heading **Generates**; (b) the use of square brackets in the description to refer to data values.

Figure 10–3 Creating a Template - Specifying Role Naming Rules



Use the configuration regions below to create the generated names for the roles. You can add your own string or number create unique names for each role that is generated by the template.

Configure Role Name

Naming Values			Concatenate With
	ROLE_CODE		:
	SET_CODE		

Generates: [ROLE_CODE]:[SET_CODE]

Configure Display Name

Naming Values			Concatenate With
	ROLE_NAME		-
	SET_NAME		

Generates: [ROLE_NAME]-[SET_NAME]

Description

Description Rule

Role Template Generated Data Role

Current Data Values

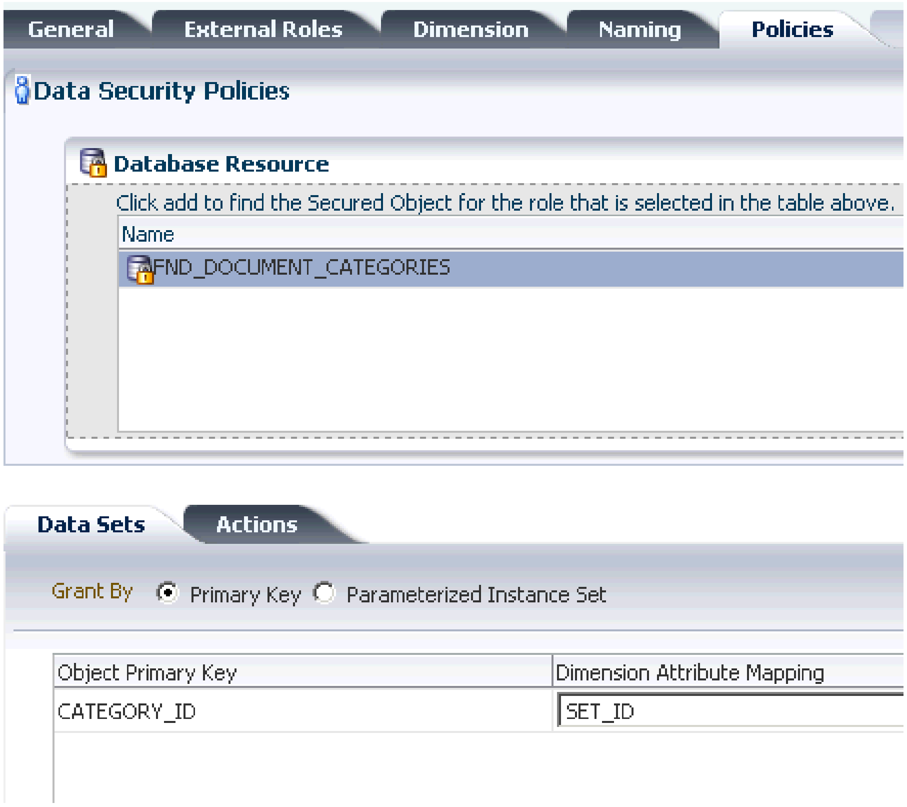
Data Values	Description
ROLE_DESC	Role Description
SET_ID	SET_ID
SET_CODE	SET_CODE
SET_NAME	SET_NAME

6. In the **Policies** tab, specify the rules to create data set grants, as follows:

   - In the **Database Resource** area, use the button **Add** to add a database resource, that is, the object to be secured by the generated data security grants.
   - In the **Data Sets** tab, specify wether the grant is using a **Primary Key** or an **Instance Set** (the instance set is selected from the available instance sets associated with the resource, which are defined at resource creation), and how the data set is mapped to a dimension attribute.
   - In the **Actions** tab, specify the actions allowed on the database resource.

   Figure 10–4 illustrates the specification of a data set by a primary key and the corresponding mapping to a dimension attribute; Figure 10–5 illustrates the specification of a data set by an instance set and the corresponding mapping to dimension attributes; and Figure 10–6 illustrates the selection of actions allowed on the database resource.

Figure 10–4 Creating a Template - Spedifying a Data Set by a Primary Key



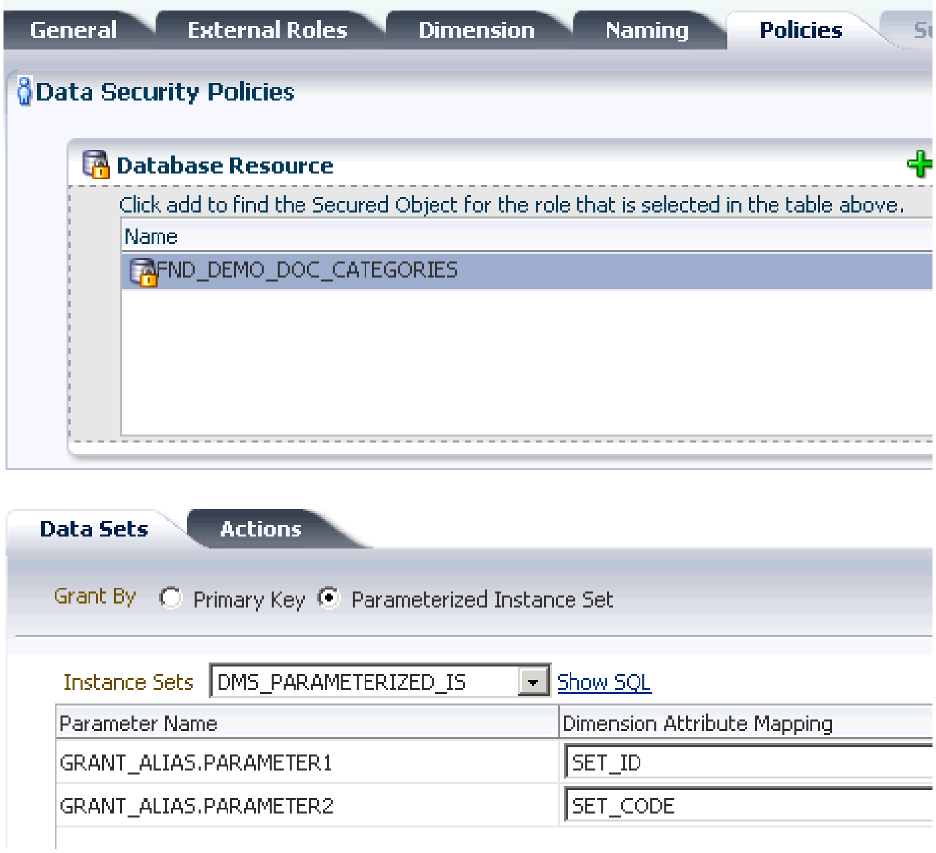
Click add to find the Secured Object for the role that is selected in the table above.

Name
FND_DOCUMENT_CATEGORIES

Grant By ● Primary Key ○ Parameterized Instance Set

Object Primary Key	Dimension Attribute Mapping
CATEGORY_ID	SET_ID

Figure 10–5 Creating a Template - Specifying a Data Set by an Instance Set



Data Security Policies

Database Resource

Click add to find the Secured Object for the role that is selected in the table above.

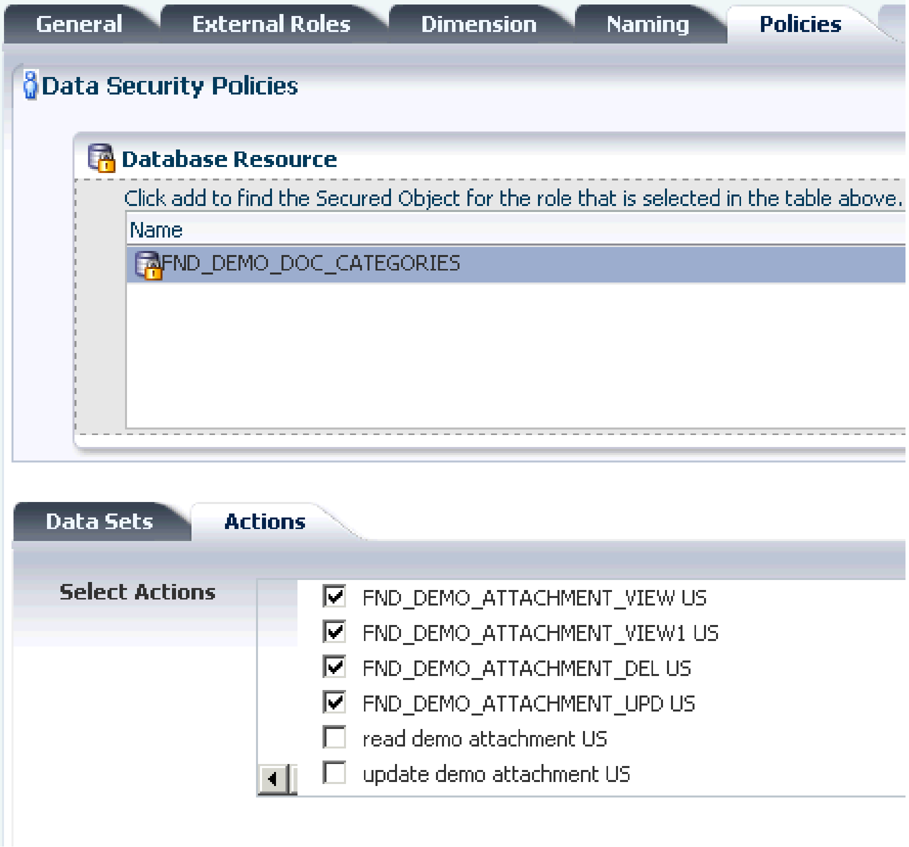
Name
FND_DEMO_DOC_CATEGORIES

Grant By ○ Primary Key ● Parameterized Instance Set

Instance Sets DMS_PARAMETERIZED_IS Show SQL

Parameter Name	Dimension Attribute Mapping
GRANT_ALIAS.PARAMETER1	SET_ID
GRANT_ALIAS.PARAMETER2	SET_CODE

Figure 10–6 Creating a Template - Specifying Actions



Click add to find the Secured Object for the role that is selected in the table above.

Name
FND_DEMO_DOC_CATEGORIES

Select Actions

- ☑ FND_DEMO_ATTACHMENT_VIEW US
- ☑ FND_DEMO_ATTACHMENT_VIEW1 US
- ☑ FND_DEMO_ATTACHMENT_DEL US
- ☑ FND_DEMO_ATTACHMENT_UPD US
- ☐ read demo attachment US
- ☐ update demo attachment US

7. Click **Save**. Oracle Authorization Policy Manager validates the information supplied and, if all data passes validation, the template is saved and the tab **Summary** becomes available.

10.4 Running a Template

The roles that a template run generates can be previewed *before* the creation of security artifacts takes place. The procedures in this section assume that the template (mentioned in the procedures) has been created and saved.

A template or a set of templates can also be run programmatically via web-services. For details see Running Templates Programmatically.

To preview the external roles that a template run would generate, proceed as follows:

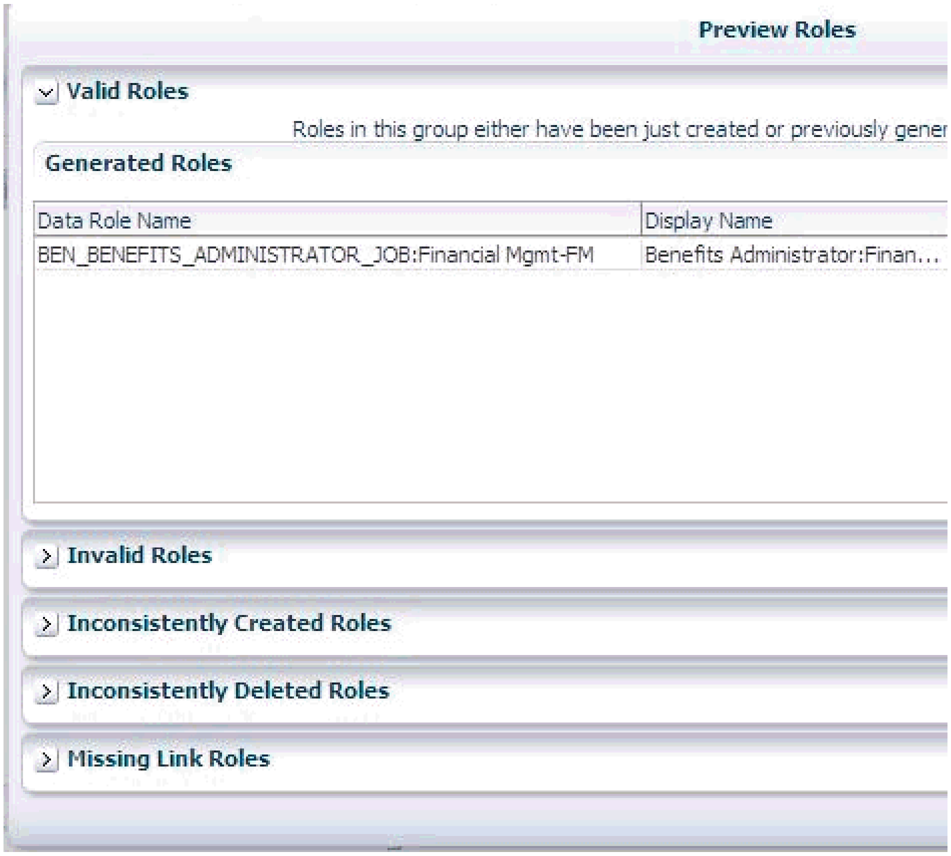
1. Open the template and bring the **Summary** tab to the foreground (this tab is available since the template has been saved).
2. Click the button **Preview Roles**, near the top of the page, to display the **Preview Roles** dialog, where the external roles that would be generated by an actual template run are grouped in the following five disjoint categories:
   - **Valid Roles** - Set of roles with no issues.
   - **Invalid Roles** - Set of roles with no base role in the identity store.
   - **Inconsistently Created Roles** - Set of roles with identical names to existing roles in the identity store. These roles, typically, get to be included in this

category because of a change or deletion in records from where the dimensions are computed.

- **Inconsistently Deleted Roles** - Set of roles that have been deleted from the identity store.
- **Missing Link Roles** - Set of roles that are missing the link to the parent base role.

Figure 10–7 illustrates a portion of the Preview Roles dialog with the category Valid Roles expanded.

Figure 10–7 Previewing Roles - The Five Categories



Roles in this group either have been just created or previously gener

Data Role Name	Display Name
BEN_BENEFITS_ADMINISTRATOR_JOB:Financial Mgmt-FM	Benefits Administrator:Finan...

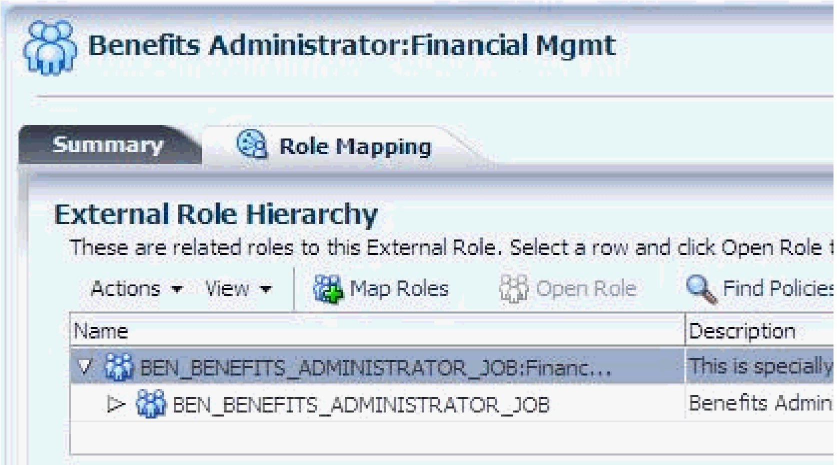
To run a template, proceed as follows:

1. Open the template and bring the **Summary** tab to the foreground (this tab is available since the template has been saved).
2. Click the button **Generate Roles**. The roles generated are displayed in the five disjoint categories mentioned in the preceding procedure. Each external role generated by the run inherits from the corresponding parent external role.
3. Reconcile roles in the following four categories, as appropriate:
   - Invalid Roles - A role in this category is a role for which the base role is not found in the identity store. Delete or allow roles in this set; deleting an invalid role:
     – Removes the role, if it is not being used by any policy.
     – Removes the data security generated for the role.

- Inconsistently Created Roles - A role in this category is a role with a name identical the name of some other role already in the identity store. Typically, these roles show up because of a change or deletion in records from where the dimensions are computed. Delete or reuse roles in this set; reusing an inconsistently created role:
  - Overwrites the existing role with the generated one.
  - Adds a link between the base role and the role.
  - Refreshes the role's display name and description.
  - Adds the data security for the role.
  - Does not affect data securities defined by other templates.
- Inconsistently Deleted Roles - Delete or recreate roles in this set; recreating an inconsistently deleted role:
  - Creates the role in the identity store using the template's naming definition.
  - Adds the data security for the role.
  - Adds a link between the base role and the role, if it was not already in place.
- Missing Link Roles - A role in this category is missing the required link to a base role. Relink roles in this set; relinking a missing link:
  - Adds a link between the base role and the role.
  - Updates the grant associated with the role.

Once external roles and data policy grants have been generated, you can verify that they have been properly created by searching and opening a particular role or policy. Figure 10–8 illustrates how the generated external role *Benefits Administrator:Finalcial Mgnt* inherits, as expected, from the base external role *Benefits Administrator* (the names displayed in the External Role Hierarchy table are the role display names, not role names):

Figure 10–8 A Generated Role Inheriting from a Based Role



Benefits Administrator:Financial Mgmt

External Role Hierarchy

These are related roles to this External Role. Select a row and click Open Role t

Name	Description
▽ BEN_BENEFITS_ADMINISTRATOR_JOB:Financ...	This is specially
▷ BEN_BENEFITS_ADMINISTRATOR_JOB	Benefits Admin

10.4.1 Running Templates Programmatically

The following two functions support running a single template or the collection of templates with a given group id via web-services:

```
public String executeTemplate(String TemplateName)
public String executeTemplateByGroupId(String GroupId)
```

The string returned by either of them describes the status of the run. If succesful, it identifies the template(s) that were run; otherwise, it identifies the error that was encountered.

10.5 Updating a Template

There are rather rigorous restrictions on how a template can be changed once it has been run.

The name of a template cannot be updated.

The SQL that defines the template dimensions cannot be changed. The data that this SQL accesses, however, can change and, therefore, a new template run may return a different set of dimensions than those returned by the last run.

When a dimension is added (to the set of dimensions of the last run), then the template run creates external roles for the added dimension only.

When a dimension is deleted (from the set of dimensions of the last run), then the administrator can either deactivate the external roles involving the deleted dimension or left them unchanged.

After execution, the template's naming cannot be updated.

On the other hand, external roles can be added or deleted from a template at any time.

When an external role is added to a template, a template run creates external roles for the added role and each of the dimensions.

When an external role is deleted from a template, then the administrator can either deactivate the external roles involving the deleted role or left them unchanged.

To update a template, proceed as follows:

1. Locate the template to update by performing a regular search or an advanced search. For details on template advanced search, see Section 4.7, "Searching Data Role Templates."
2. Click **Edit**, to open the template for editing in the right panel.
3. Modify fields as appropriate and as allowed in the page tabs.
4. Click the button **Apply**, at the top of the page, to save changes.

10.6 Importing and Exporting a Template

A data role template can be imported to or exported from the Oracle Authorization Policy Manager environment with the use of the following two utilities: `importMetadata` and `exportMetadata`. Both of them are online, that is, they require establishing a connection to the Oracle WebLogic server before they can be used.

The following line illustrates how to establish a connection to a WebLogic server:

```
> connect ('aUser','aPassword','t5://localhost:7133')
```

where the first argument is the user name, the second one is the password for that user, and the third one is the connection URL to the server. The connection so established is terminated with the command `exit()`.

To import one or several data role templates, proceed as follows:

1. Connect to the server.
2. Execute the utility `importMetadata`, as illustrated in the following sample (the arguments are listed in different lines only for clarity of exposition):

```
> importMetadata(application='oracle.security.apm',
                 server='AdminServer',
                 fromLocation='/myLocation/myRoleTemplates',
                 docs='/oracle/apps/apm/**',
                 restrictCustTo='site')
```

   The meaning of the arguments is as follows:

   - `application` specifies the owner of the data role template to be imported.
   - `server` specifies the name of the WebLogic server to which one is connected.
   - `fromLocation` specifies the directory where the data role template to be imported is located.
   - `docs` specifies the template in the directory `fromLocation` to be imported. To import all tempates (including template subdirectories) in the specified directory, use **, as illustrated in the example above.
   - `restrictCustTo` is an argument that should always be set to `site`.

To export a data role template, proceed as follows:

1. Connect to the server.
2. Execute the utility `exportMetadata`, as illustrated in the following sample (the arguments are listed in different lines only for clarity of exposition):

```
> exportMetadata(application='oracle.security.apm',
                 server='AdminServer',
                 toLocation='/myLocation/myRoleTemplates',
                 docs='/oracle/apps/apm/**',
                 restrictCustTo='site')
```

   The meaning of the arguments is identical to those used for importing, except for `toLocation`, which specifies the location where the data role template(s) should be downladed.

11

Managing Oracle Fusion Applications Data Security Policies

The information in this chapter is specific to Oracle Fusion Applications only.

This chapter describes the procedures an administrator follows to manage security policies on database resources, and it is divided into the following sections:

11.1 Database Resources and Policies Overview

Data security policies determine who can do what on which set of data. A data security policy defines the enterprise or application roles that provides members of those roles access rights to specific data.

The Oracle Fusion security reference implementation provides enterprise roles and access to data through a comprehensive set of predefined data security policies applicable to application roles that are members of those enterprise roles.

Data security consists of privileges conditionally granted to a role, and these grants are used to control access to instance sets of a business object. A privilege is a single action corresponding to an operation on a single business object. Instance sets are rows of a database resource returned by a user-defined SQL WHERE clause; instance sets may be a single row of data, multiple rows of a single table, or all rows of a single table. A data security policy is, therefore, a set of privileges to a principal on a business object for a given instance set.

The security administrator uses Oracle Authorization Policy Manager to create and administer data security policies. A data security policy involves the following security artifacts:

- A database resource that references a primary key corresponding to the database table or view of the business object to be secured
- A role that has been provisioned with the users who can perform the granted actions
- A rule (also known as a condition) to define the available row instances in the form of an SQL predicate or simple filter (stored as XML) defined on the rows of the database resource

- One or more actions (such as view, edit, or delete) performed on database records that correspond to the operations supported by the business object, and which may include custom operations

By default, when a business object is registered as a database resource in Oracle Authorization Policy Manager, users are denied access to all data of that business object. A data security policy makes data available to users based on the roles they are members of according to the actions and conditions specified in the policy:

- Actions determine whether the user has the right to perform a given operation.
- Condition evaluation for actions (and their corresponding operations) specify the set of rows on which those operations can be applied.

11.1.1 Prerequisites and Best Practices for Creating Data Security Policies

Data security policies secure the database resources of an enterprise. The Oracle Fusion security reference implementation provides a comprehensive set of predefined data security policies for database resources that involve database tables and views that correspond to business objects; it is recommended that these database resources not be changed.

In cases where custom database resources must be secured, the security administrator can manage the predefined database resources or create new data security policies. Before modifying any data security policy, it is important to understand the predefined data security policies provided by the security reference implementation. As a general guideline, security policies assigned to duty roles of the reference implementation should not be changed, only their participation in role hierarchies. Details about the Oracle Fusion security reference implementation can be found in the Oracle Fusion Security Reference Manual and are also available for review Oracle Authorization Policy Manager.

> **Important:** Review but do not modify data security policies from the Oracle Fusion security reference implementation in Oracle Authorization Policy Manager except as a custom implementation to create data security policies.

For example, in the security reference implementation, the `IT Security Manager` job role hierarchy includes the `Application Data Security Administration Duty` duty role, which is entitled to manage data security policies (the entitlement is `Manage Data Security Policy`). This entitlement provides necessary privileges to perform the **Manage Data Security Policies** task in Oracle Authorization Policy Manager.

Before creating a data security policy with Oracle Authorization Policy Manager, the security administrator should collect the following information for custom security policies:

- The actions corresponding to the operations that the business object to be secured defines; these actions can be obtained from the developer who implemented the business function.
- The primary key of the database table or view that the business object represents; this key can be obtained from the developer who implemented the business function.

- The application roles for which the policy is created; these roles can be obtained from an Oracle Identity Manager administrator, or they can be queried with Oracle Authorization Policy Manager.

11.1.2 Process Overview for Creating Data Security Policies

To define an Oracle Fusion Data Security policy, proceed as follows:

1. Identify the business object that you want to secure and register its backend database table or view as a database resource.

   A table or view is registered by its primary key columns.

2. Identify and define all of the conditions that you want to make available on the registered database resource.

   Conditions define an instance set of rows specified either by simple filters (XML defined) or complex SQL queries whose values can be parameterized. No condition definition is needed in the case of a single row instance or all row instances.

3. Identify and register the actions that you want to secure for this database resource.

   Action names should match the names of the operations the business object supports (for example, view_US_ONLY, edit_US_ONLY, delete_US_ONLY for custom operations).

4. Identify the Oracle Platform Security Services (OPSS) role for which you want to create the policy.

   OPSS roles and the role inheritance hierarchy are managed by Oracle Identity Manager.

5. Define a rule to specify the values (data) that you want to make available on the registered database resource for a particular role.

   A rule can be a row instance of the database resource (when a single value is desired), the entire resource (when all values are desired), or a condition that had been defined for the resource (when multiple values are needed).

6. Grant one or more actions on the database resource to the role for the specified rule.

   Available actions will be limited to the actions that had been defined for the database resource.

11.2 Searching Database Resources and Policies

Data security policies are displayed in Oracle Authorization Policy Manager by the database resource they secure, as explained in the following sections:

- Searching Database Resources
- Locating Policies Associated with a Database Resource

11.2.1 Searching Database Resources

Database resources can be queried with a simple or an advanced search.

To specify a simple search, proceed as follows:

1. Select **Global** from the pull-down list at the top of the navigation panel.

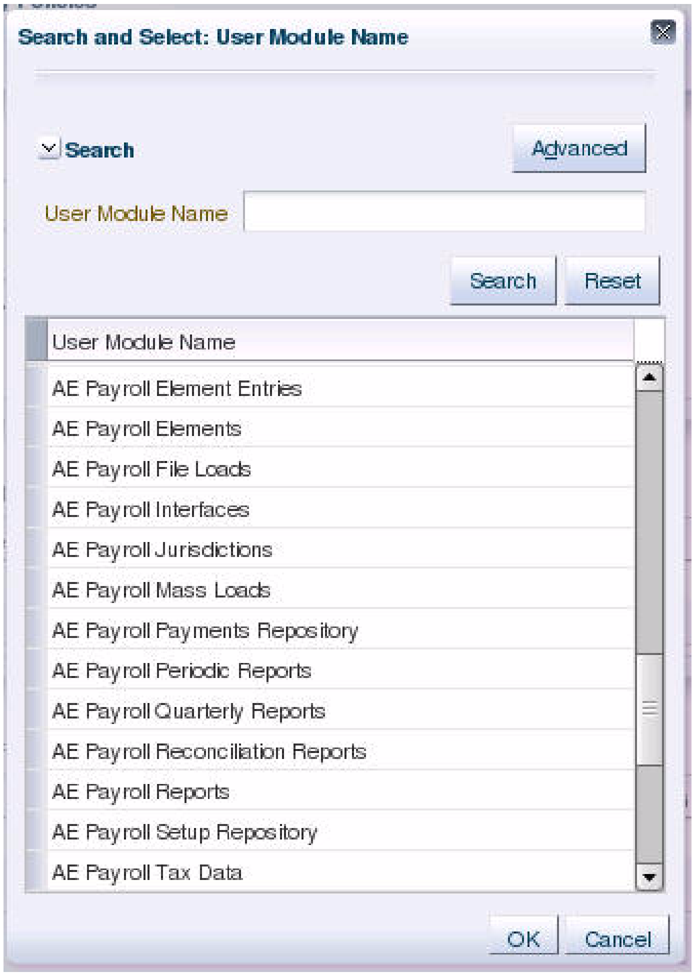
2. Select **Database Resources** from the pull-down list second from the top.
3. Enter a string to match in the text box, possibly using the wildcard characters % or * (the wild character matches any character in the pattern).

   The search returns all names and display names of database resources that match the specified string; leave this box empty to obtain the list of all objects of the specified type.
4. Click the Go button to trigger the search and to display the results in the tab **Search Results**, which is automatically brought to the foreground when the search is completed. Positioning the cursor on the blue information button next to an item displays the item details. The Search Results tab shows at most the first 200 matches found by the search.
5. Once an item is selected in the Search Results, it can be opened or edited by clicking **Open** or **Edit** at the top of the table.

To specify a database resource advanced search, proceed as follows:

1. Expand the hierarchy it to expose all nodes in the hierarchy.
2. Double-click **Database Resources** under the Global node to display the **Manage Database Resources and Policies** tab.
3. In the Search area of that tab, enter the query parameters as follows:
   - In the **Object Name** box, enter the string to match the database resource name, possibly including the wildcard characters % or * (the wild character matches any character in the pattern). To match all strings, leave the box empty.
   - In the **Display Name** box, enter the string to match the database resource display name, possibly including the wildcard characters % or * (the wild character matches any character in the pattern). To match all strings, leave the box empty.
   - In the **User Module Name** pull-down box, select a module where to look for database resources. To locate a module, optionally select the Search item (at the bottom of the pull-down list) to bring up the **Search and Select: User Module Name** dialog, illustrated in Figure 11–1. In **User Module Name** box in that dialog, enter the string to match module and select one from the result list returned and then click OK.
   - Optionally, click **Reset** to set the parameter values to the values they had before you entered the current values.

Figure 11–1 Searching for a User Module



Search and Select: User Module Name

User Module Name
AE Payroll Element Entries
AE Payroll Elements
AE Payroll File Loads
AE Payroll Interfaces
AE Payroll Jurisdictions
AE Payroll Mass Loads
AE Payroll Payments Repository
AE Payroll Periodic Reports
AE Payroll Quarterly Reports
AE Payroll Reconciliation Reports
AE Payroll Reports
AE Payroll Setup Repository
AE Payroll Tax Data

4. Optionally, click **Save...** to save the current query parameters. The name of the saved collection then appears in the pull-down list **Saved Search**. Selecting a saved search from this pull-down list fills in the query parameters automatically with the saved values.

5. Click **Search** to trigger the search. All database resources matching the entered specifications are displayed in the table **Search Results**.

   The actions at the top of this table allow:

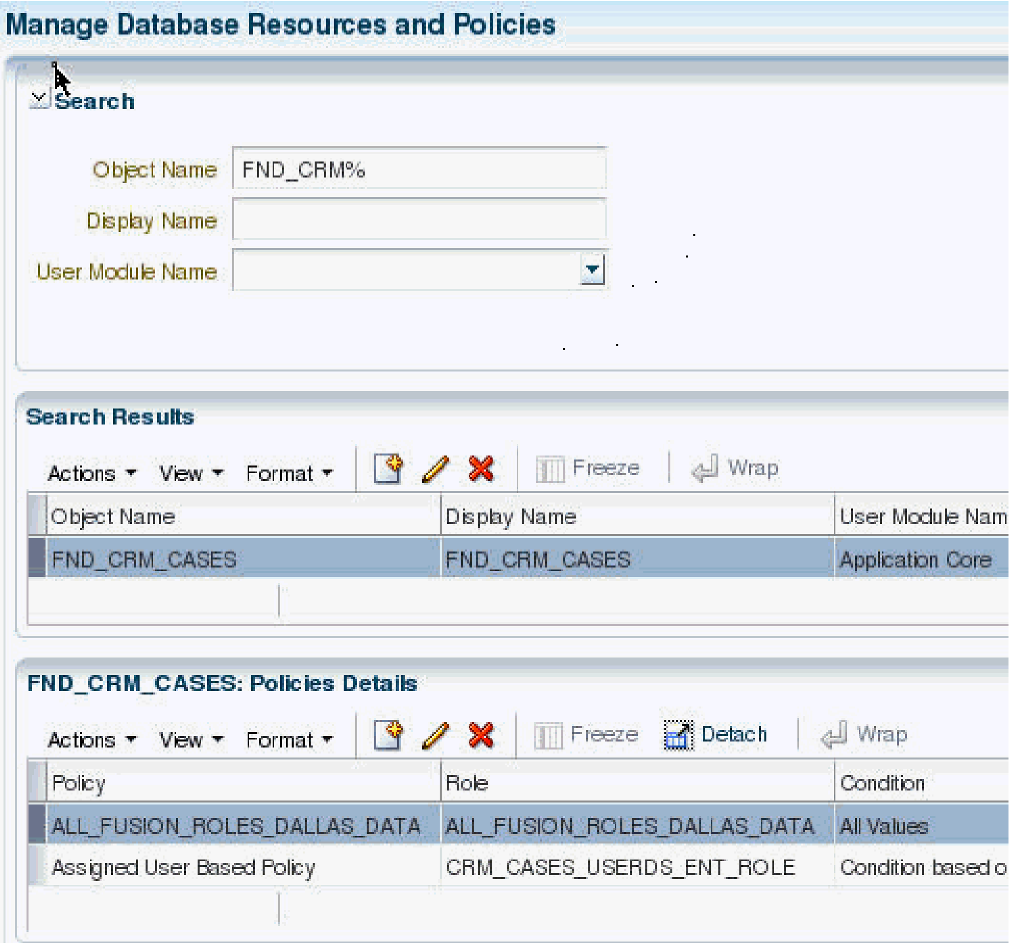
   - Creating a database resource
   - Editing a database resource
   - Deleting a database resource

   In addition, the table below the Search Results area, displays the list of policies associated with a database resource selected in the Search Results table.

Figure 11–2 illustrates the results of an advanced search on database resources and the policies associated with a database resource selected from the Search Results table.

The button Follow is used send out notifications about the activity stream. For details about Activity Stream, see *Oracle Fusion Applications Developer's Guide*.

Figure 11–2 Manage Database Resources and Policies Tab



Object Name: FND_CRM%

Display Name:

User Module Name:

Object Name	Display Name	User Module Nam
FND_CRM_CASES	FND_CRM_CASES	Application Core

Policy	Role	Condition
ALL_FUSION_ROLES_DALLAS_DATA	ALL_FUSION_ROLES_DALLAS_DATA	All Values
Assigned User Based Policy	CRM_CASES_USERDS_ENT_ROLE	Condition based o

11.2.2 Locating Policies Associated with a Database Resource

To locate a policy (global or associated with an application) associated with a database resource, first identify the database resource with a search as described in section Searching Database Resources, and then inspect the list of policies associated with the database resource in the **Policies Details** table. Figure 11–2 illustrates the policies associated with a database resource FND_CRM_CASES.

For alternative ways to locate policies, see Section 4.6, "Searching Application Policies," and Section 3.4, "Finding Artifacts with a Simple Search."

11.3 Managing Database Resources

The following sections describe how to specify what portion of the database resource is secured by a data security policy:

- Specifying Database Resource Column Details
- Managing Database Resource Conditions
- Managing Database Resource Actions

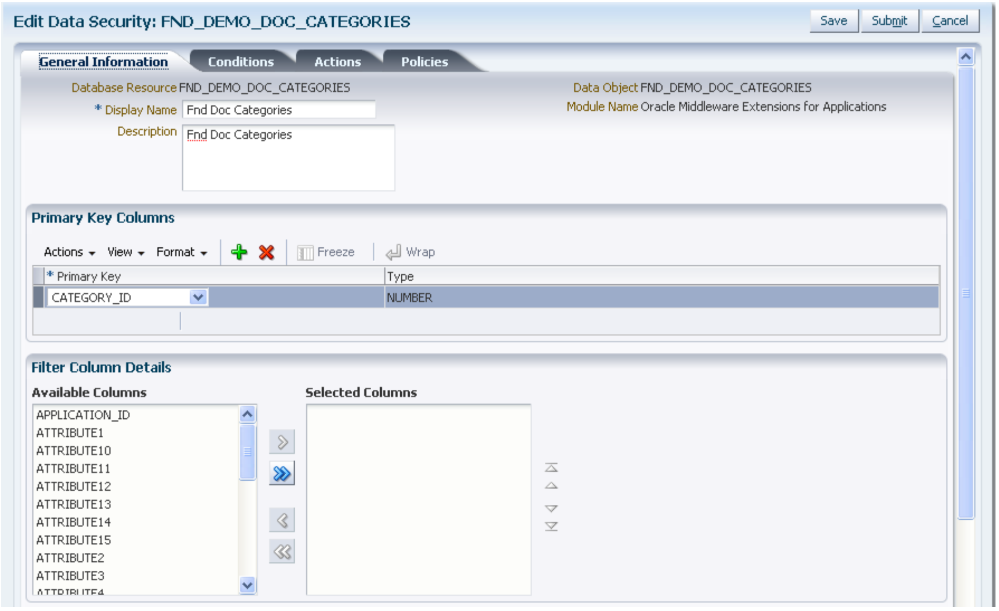
11.3.1 Specifying Database Resource Column Details

The following sections describe how to manage the available columns of a database resource for which security policies may be defined:

- Specifying the Primary Key Columns of the Policy's Database Resource
- Filtering Columns of the Policy's Database Resource

Figure 11–3 illustrates the **General Information** tab in the Edit Data Security page after the `FND_DOC_CATEGORIES` table has been registered as a database resource with the primary key `CATEGORY_ID` and no columns filtered.

Figure 11–3 Creating a Database Resource - Specifying the Primary Key Columns



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Database Resource FND_DEMO_DOC_CATEGORIES

* Display Name Fnd Doc Categories

Description Fnd Doc Categories

Data Object FND_DEMO_DOC_CATEGORIES

Module Name Oracle Middleware Extensions for Applications

Primary Key Columns

* Primary Key	Type
CATEGORY_ID	NUMBER

Filter Column Details

Available Columns

APPLICATION_ID
ATTRIBUTE1
ATTRIBUTE10
ATTRIBUTE11
ATTRIBUTE12
ATTRIBUTE13
ATTRIBUTE14
ATTRIBUTE15
ATTRIBUTE2
ATTRIBUTE3
ATTRIBUTE4

Selected Columns

11.3.1.1 Specifying the Primary Key Columns of the Policy's Database Resource

The database resource is a database table or view. You use the table or view's primary key column(s) to register it as a database resource.

To specify the primary key of the database resource, proceed as follows:

1. Identify the database resource by matching the name of the database resource that the policy will secure. For details, see Section 11.2.1, "Searching Database Resources."
2. In the **General Information** tab, click **Add** and choose the database resource's primary key from the dropdown list. You can add additional key columns when more than one key column is defined by the resource.
3. Click **Save** to complete the specification of the primary key.

11.3.1.2 Filtering Columns of the Policy's Database Resource

You can filter columns at the level of the database resource when you want to exclude columns from the row instance sets defined by data security policies. Additionally, the data from filtered columns will not be accessible by the user.

To filter the list of columns that the database resource defines, proceed as follows:

1. Identify the database resource by matching the name of the database resource that the policy will secure. For details, see Section 11.2.1, "Searching Database Resources."
2. In the **General Information** tab, move available columns to the **Selected Column** list when you want to exclude that column from the database resource.

   Excluded columns will not be available when defining database resource conditions and the data of these columns will not be accessible to any user.
3. Click **Save** to complete the filtering the list of columns.

11.3.2 Managing Database Resource Conditions

You define conditions on the database resource to specify what portions of the database resource may be secured by data security policies. A condition is a group of row instances that are determined by a simple XML filter or an SQL predicate (`WHERE` clause) that queries the attributes of the resource itself. Conditions are always defined on a single table or view.

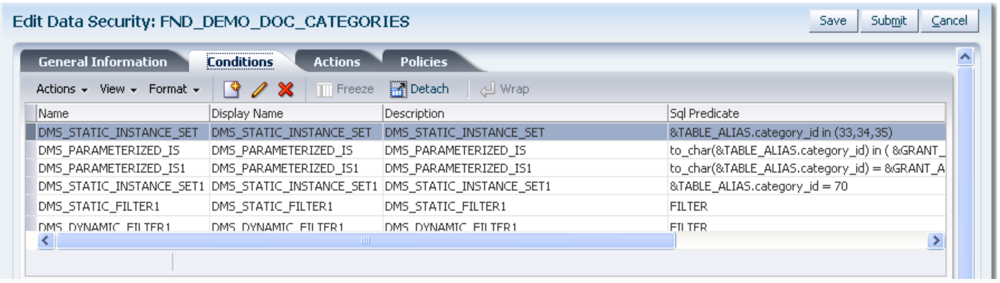
You can define a condition to specify multiple row instance sets using a parameterized SQL WHERE clause. For example, the condition may be defined by the predicate `REGION=&PARAM` where the parameter `PARAM` is associated with different regions. When an action is granted for a condition, it may be done for a particular value of the parameter, such as a "sales manager" in the West region may have an action granted for a **Region** condition with the parameter value `West`.

You do not need to define a condition for single row instance condition (single value) or for all row instances conditions (all values). Both the single-value case and the all-values case may be easily defined when you create the data security policy. Internally, Oracle Authorization Policy Manager will save these as conditions with the appropriate SQL query clause.

Figure 11–4 illustrates the **Conditions** tab in the Edit Data Security page after several row instance sets have been defined as conditions of the database resource. You can perform these operations using the **Conditions** tab:

- Click **New** to define a new condition.
- Select an existing condition and click **Edit** to edit the condition details.
- Select an existing condition and click **Delete** to delete the condition.

Figure 11–4 Creating a Database Resource - Adding to the Available Conditions List



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Name	Display Name	Description	Sql Predicate
DMS_STATIC_INSTANCE_SET	DMS_STATIC_INSTANCE_SET	DMS_STATIC_INSTANCE_SET	&TABLE_ALIAS.category_id in (33,34,35)
DMS_PARAMETERIZED_IS	DMS_PARAMETERIZED_IS	DMS_PARAMETERIZED_IS	to_char(&TABLE_ALIAS.category_id) in (&GRANT_
DMS_PARAMETERIZED_IS1	DMS_PARAMETERIZED_IS1	DMS_PARAMETERIZED_IS1	to_char(&TABLE_ALIAS.category_id) = &GRANT_A
DMS_STATIC_INSTANCE_SET1	DMS_STATIC_INSTANCE_SET1	DMS_STATIC_INSTANCE_SET1	&TABLE_ALIAS.category_id = 70
DMS_STATIC_FILTER1	DMS_STATIC_FILTER1	DMS_STATIC_FILTER1	FILTER
DMS_DYNAMIC_FILTER1	DMS_DYNAMIC_FILTER1	DMS_DYNAMIC_FILTER1	FILTER

To define a new database resource condition, proceed as follows:

1. Identify the database resource to secure by matching the name of the database resource that the policy secures. For details, see Section 11.2.1, "Searching Database Resources."

2. In the **Conditions** tab, click **New** and define what portions of the database resource may be secured by data security policies. For details, see Section 11.3.2, "Managing Database Resource Conditions."

3. In the **Create Database Resource Condition** dialog, enter the following information:

   - A name (required)
   - A display name (required)
   - A description (optional)
   - A condition type (required)
     - When you what to use the attribute tree picker user interface to define a simple condition, choose **Filter**.
     - When you know the attributes names of your condition and you want to define an SQL WHERE clause, for example to specify a dynamic condition, using a parameterized SQL predicate, choose **SQL Predicate**.

4. If you chose a **Filter** condition type, then define the condition as follows:

   a. Click **Add** and choose the column name from the dropdown list that you want to define the filter on.

   b. Choose the tree operator for the selected column.

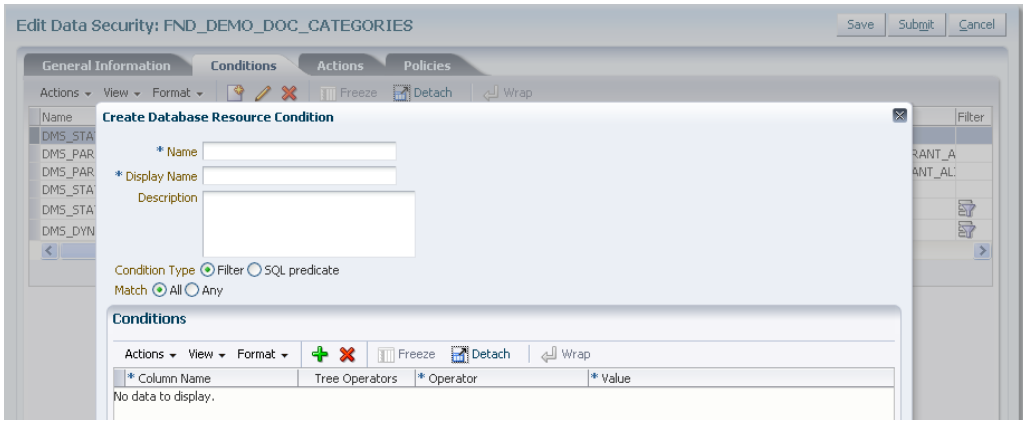
   c. Enter a value as the test for the operator.

   d. Add additional columns as needed.

   e. Select **Match All** or **Match Any** depending on whether you want the filter conditions to be ANDed (match all) or ORed (match any).

   Figure 11–5 illustrates the **Create Database Resources Condition** dialog in the Edit Data Security page when creating an XML filter condition.

Figure 11–5 Creating a Database Resource Condition - Defining an XML Filter Condition



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Create Database Resource Condition

* Name

* Display Name

Description

Condition Type ● Filter ○ SQL predicate

Match ● All ○ Any

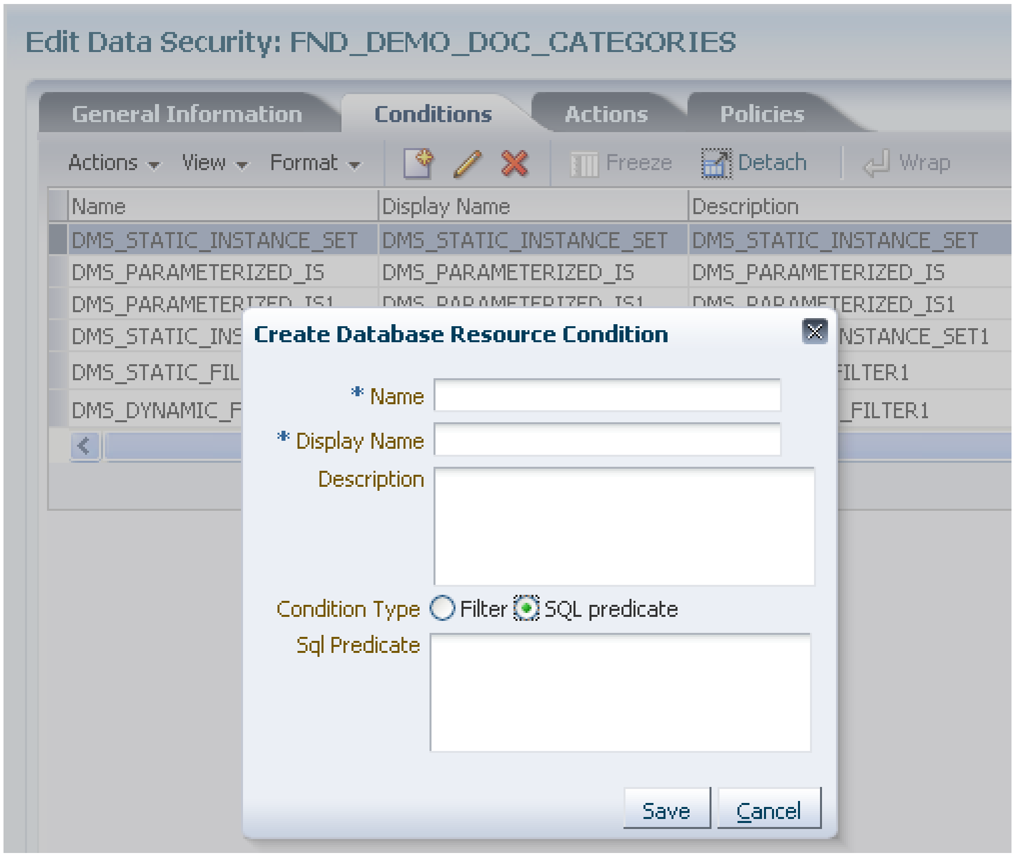
Conditions

* Column Name	Tree Operators	* Operator	* Value
No data to display.			

5. If you chose a **SQL Predicate** condition type, then enter the SQL predicate consisting of a query on the table or view named by the database resource.

   Figure 11–6 illustrates the **Create Database Resources Condition** dialog in the Edit Data Security page where you enter an SQL predicate condition.

Figure 11–6 Creating a Database Resource Condition



Name	Display Name	Description
DMS_STATIC_INSTANCE_SET	DMS_STATIC_INSTANCE_SET	DMS_STATIC_INSTANCE_SET
DMS_PARAMETERIZED_IS	DMS_PARAMETERIZED_IS	DMS_PARAMETERIZED_IS
DMS_PARAMETERIZED_IS1	DMS_PARAMETERIZED_IS1	DMS_PARAMETERIZED_IS1
DMS_STATIC_INS		NSTANCE_SET1
DMS_STATIC_FIL		FILTER1
DMS_DYNAMIC_F		_FILTER1

Create Database Resource Condition

* Name

* Display Name

Description

Condition Type ○ Filter ● SQL predicate

Sql Predicate

6. Click **Save** to complete the creation of a database source condition.

11.3.3 Managing Database Resource Actions

You define actions on the database resource to specify what kind of access data security policies will secure on a business object. For example, you can specify whether a user might have read, update, or delete access by naming actions for each of these and granting them in a data security policy to a particular role.

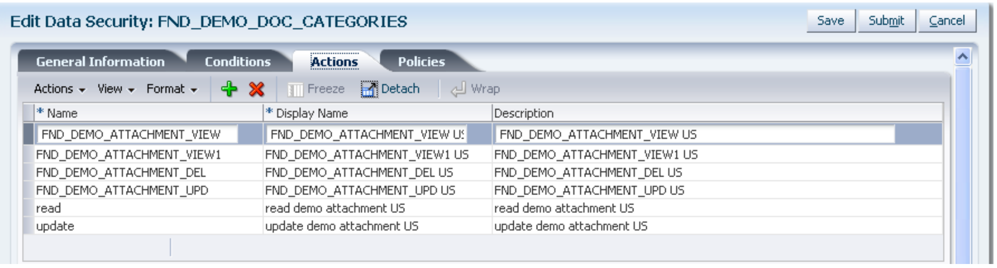
An action corresponds one to one with an operation that the business object implements. Action names must match the corresponding business object operation names established by the business object developer. Actions may correspond to either standard operations or custom operations. For example, a business object might define custom read operations based on the regions West and East, which allows you to create the corresponding actions **read_WEST** and **read_EAST**. Alternatively, actions that you define, such as **read** and **update**, may correspond to the standard read and update operations of the same business object, when no region is specified.

Actions act on the row instance sets of the database resource conditions that you define in a data security policy. When the user invokes an operation on the business object, the system will act on the row set instances defined by the condition and the corresponding action of the security policy in effect for that business object. The system will perform the operation only if the policy grants the user a privilege for the corresponding action.

Figure 11–7 illustrates the **Actions** tab in the Edit Data Security page after several actions have been defined on the database resource. You can perform these operations using the **Actions** tab:

- Click **Add** to define a new action.
- Click in any field of an existing action and edit the details; do not change the name of an action unless the name of the corresponding business object operation should be changed too.
- Select an existing action and click **Delete** to delete the action.

Figure 11–7 Creating a Database Resource - Adding to the Available Actions List



Edit Data Security: FND_DEMO_DOC_CATEGORIES

* Name	* Display Name	Description
FND_DEMO_ATTACHMENT_VIEW	FND_DEMO_ATTACHMENT_VIEW US	FND_DEMO_ATTACHMENT_VIEW US
FND_DEMO_ATTACHMENT_VIEW1	FND_DEMO_ATTACHMENT_VIEW1 US	FND_DEMO_ATTACHMENT_VIEW1 US
FND_DEMO_ATTACHMENT_DEL	FND_DEMO_ATTACHMENT_DEL US	FND_DEMO_ATTACHMENT_DEL US
FND_DEMO_ATTACHMENT_UPD	FND_DEMO_ATTACHMENT_UPD US	FND_DEMO_ATTACHMENT_UPD US
read	read demo attachment US	read demo attachment US
update	update demo attachment US	update demo attachment US

To define a new database resource action, proceed as follows:

1. Identify the database resource to secure by matching the name of the database resource that the policy secures. For details, see Section 11.2.1, "Searching Database Resources."
2. In the **Actions** tab, click **New** and enter the following information in the list of actions table:
   - An action name (required) - the name must match the corresponding operation of the business object. When defining actions for custom operations, consult the developer for the names of the operations.
   - A display name (required)
   - A description (optional)
3. Click **Save**.

11.4 Managing Data Security Policies

The following sections describe how to determine the roles that can access a database resource and the type of actions that those roles may perform on the data:

- Creating a Data Security Policy
- Modifying a Custom Data Security Policy

11.4.1 Creating a Data Security Policy

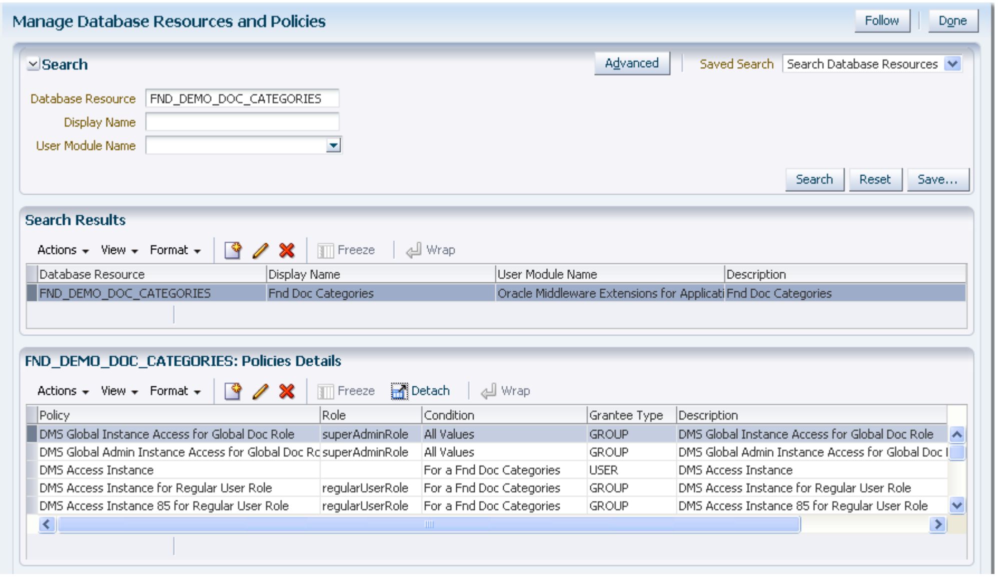
When you register a new business object as a database resource, users will initially be prevented from invoking the operations of the business object. They will also be prevented from accessing the data of the resource. You define data security policies to make data of a custom business object available to the users of the application.

Figure 11–8 illustrates the **Policies Details** tab in the Manage Database Resources and Polices page after several data security policies have been created for the database resource. You can perform these operations using the **Policies** tab:

- Click **New** to define a new policy.
- Select an existing policy and click **Edit** to edit the details in the **Details** tab.
- Select an existing policy and click **Delete** to delete the policy.

  Important: Duty roles in security policies in the Oracle Fusion reference implementation should not be edited or deleted; only their role hierarchies should be modified.

Figure 11–8 Creating a Data Security Policy - Adding to the Policy List



Database Resource: FND_DEMO_DOC_CATEGORIES
Display Name:
User Module Name:

Search Results

Database Resource	Display Name	User Module Name	Description
FND_DEMO_DOC_CATEGORIES	Fnd Doc Categories	Oracle Middleware Extensions for Applicati	Fnd Doc Categories

FND_DEMO_DOC_CATEGORIES: Policies Details

Policy	Role	Condition	Grantee Type	Description
DMS Global Instance Access for Global Doc Role	superAdminRole	All Values	GROUP	DMS Global Instance Access for Global Doc Role
DMS Global Admin Instance Access for Global Doc Rc	superAdminRole	All Values	GROUP	DMS Global Admin Instance Access for Global Doc I
DMS Access Instance		For a Fnd Doc Categories	USER	DMS Access Instance
DMS Access Instance for Regular User Role	regularUserRole	For a Fnd Doc Categories	GROUP	DMS Access Instance for Regular User Role
DMS Access Instance 85 for Regular User Role	regularUserRole	For a Fnd Doc Categories	GROUP	DMS Access Instance 85 for Regular User Role

Before you begin

Before you create a data security policy, perform the following tasks:

1. Register the business object as a database resource, as described in Section 11.3, "Managing Database Resources."
2. Define the conditions that you want to apply for specific actions of the policy, as described in Section 11.3.2, "Managing Database Resource Conditions." Conditions determine the row instance set available to a user for a given operation.
3. Define the actions to grant to the role, as described in Section 11.3.3, "Managing Database Resource Actions." Actions correspond to the operations of the business object that the user may invoke.
4. Obtain the name of the application role or enterprise role for which you want to create the policy.

To create a new data security policy, proceed as follows:

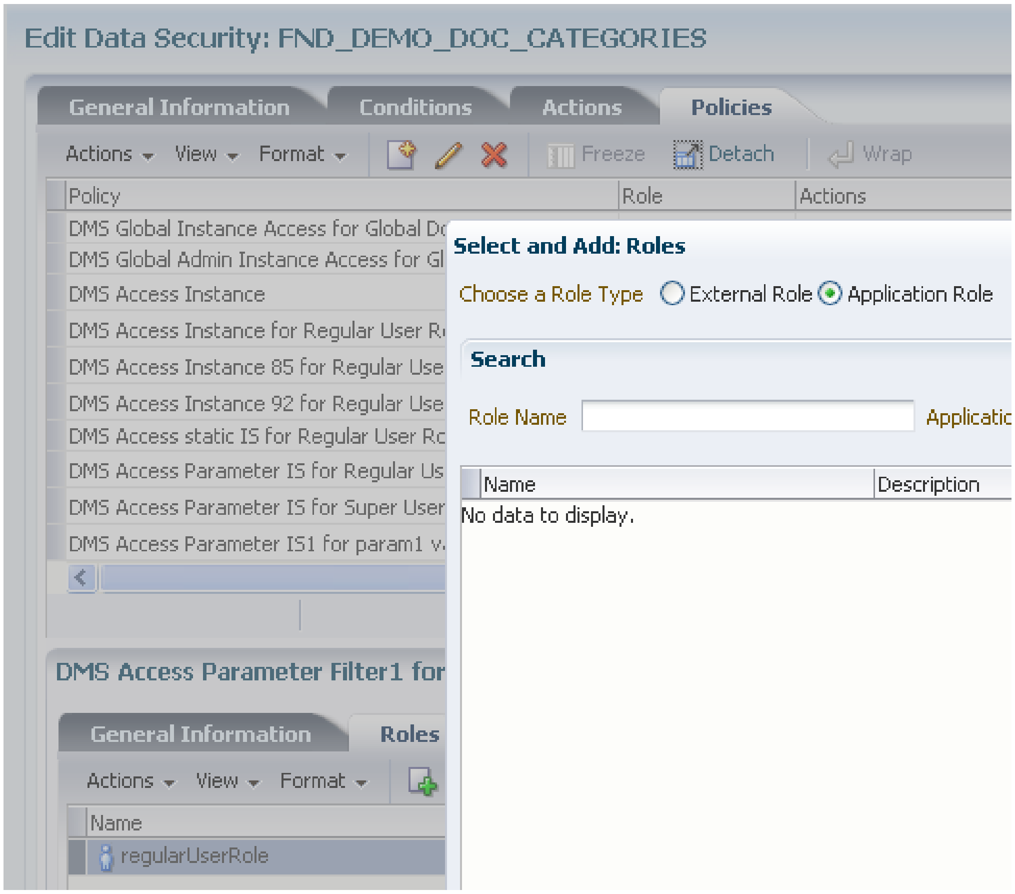
1. Identify the database resource to secure by matching the name of the database resource that the policy secures. For details, see Section 11.2.1, "Searching Database Resources."
2. In the **Policies** tab, click **New**.
3. In the **General Information** tab of the **Details** section, enter the following information for the data security policy being created:
   - A name (required)

- A module (required)
- A start date for the policy to become effective (required)
- An end date for the policy to cease to be effective (optional)
- A description (optional)

4. In the **Roles** tab of the **Details** section, select the role to which the policy grants access. The roles you add entitle all users assigned to those roles with access to the data.

   Figure 11–9 illustrates the **Select and Add: Roles** dialog in the Edit Data Security page.

Figure 11–9 Creating a Data Security Policy - Selecting a Role



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Policy	Role	Actions
DMS Global Instance Access for Global Dc		
DMS Global Admin Instance Access for Gl		
DMS Access Instance		
DMS Access Instance for Regular User Ri		
DMS Access Instance 85 for Regular Use		
DMS Access Instance 92 for Regular Use		
DMS Access static IS for Regular User Rc		
DMS Access Parameter IS for Regular Us		
DMS Access Parameter IS for Super User		
DMS Access Parameter IS1 for param1 v		

Select and Add: Roles

Choose a Role Type ○ External Role ● Application Role

Search

Role Name [ ] Applicatic

Name	Description
No data to display.	

DMS Access Parameter Filter1 for

Name
regularUserRole

5. In the **Rule** tab of the **Details** section, specify the rows of the database resource on which the policy applies in the following ways:

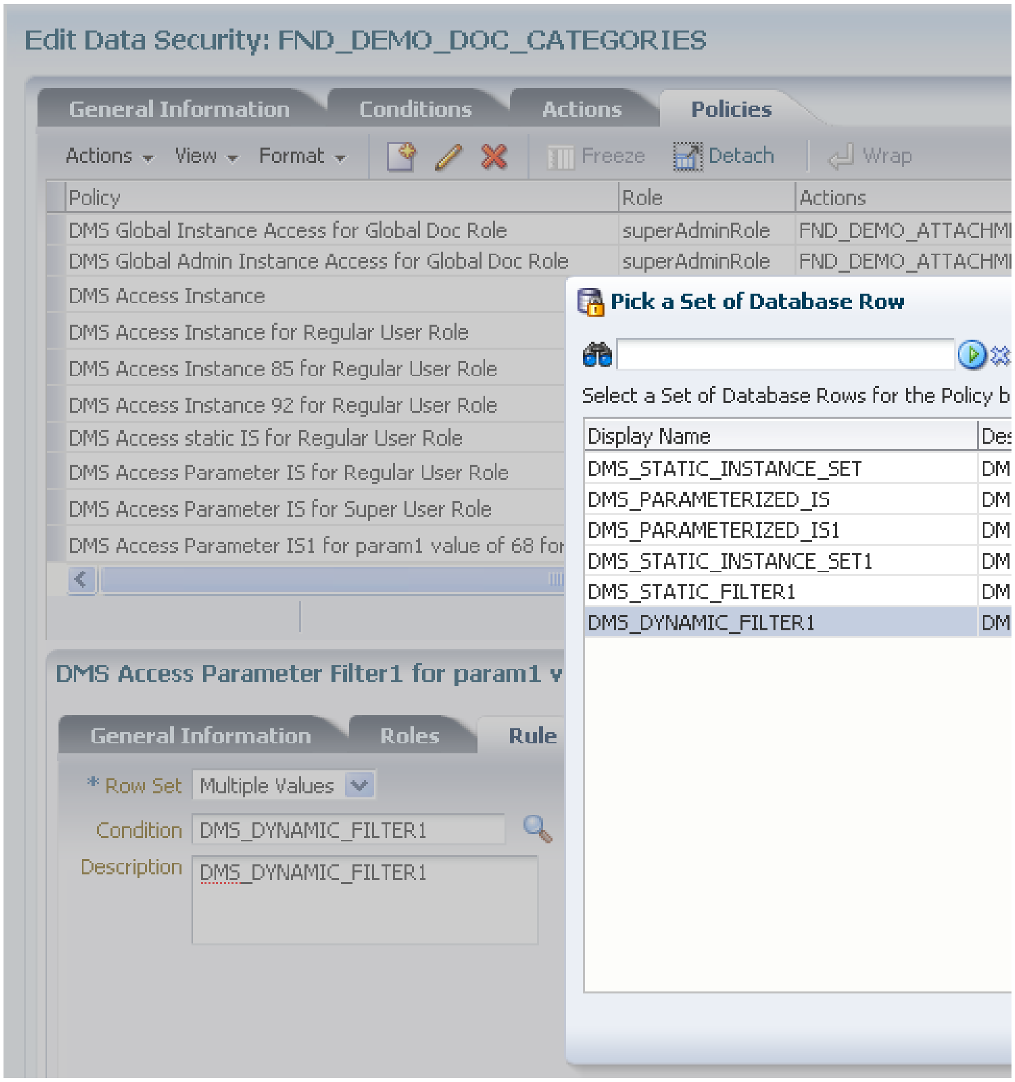
   – When you want to secure a specific row, select **Single Value**.

   – When you want to secure all rows, select **All Values**.

   – When you want to change the condition in order to change the secured rows of the database resource, select **Multiple Values** and click the **Search** icon and choose the desired condition. To create a new condition, see Section 11.3.2, "Managing Database Resource Conditions."

Figure 11–10 illustrates the **Pick a Set of Database Row** dialog in the Edit Data Security page after several conditions have been selected from the list of available conditions.

Figure 11–10 Creating a Data Security Policy - Selecting a Rule



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Policy	Role	Actions
DMS Global Instance Access for Global Doc Role	superAdminRole	FND_DEMO_ATTACHM
DMS Global Admin Instance Access for Global Doc Role	superAdminRole	FND_DEMO_ATTACHM
DMS Access Instance		
DMS Access Instance for Regular User Role		
DMS Access Instance 85 for Regular User Role		
DMS Access Instance 92 for Regular User Role		
DMS Access static IS for Regular User Role		
DMS Access Parameter IS for Regular User Role		
DMS Access Parameter IS for Super User Role		
DMS Access Parameter IS1 for param1 value of 68 for		

DMS Access Parameter Filter1 for param1 v

* Row Set: Multiple Values

Condition: DMS_DYNAMIC_FILTER1

Description: DMS_DYNAMIC_FILTER1

Pick a Set of Database Row

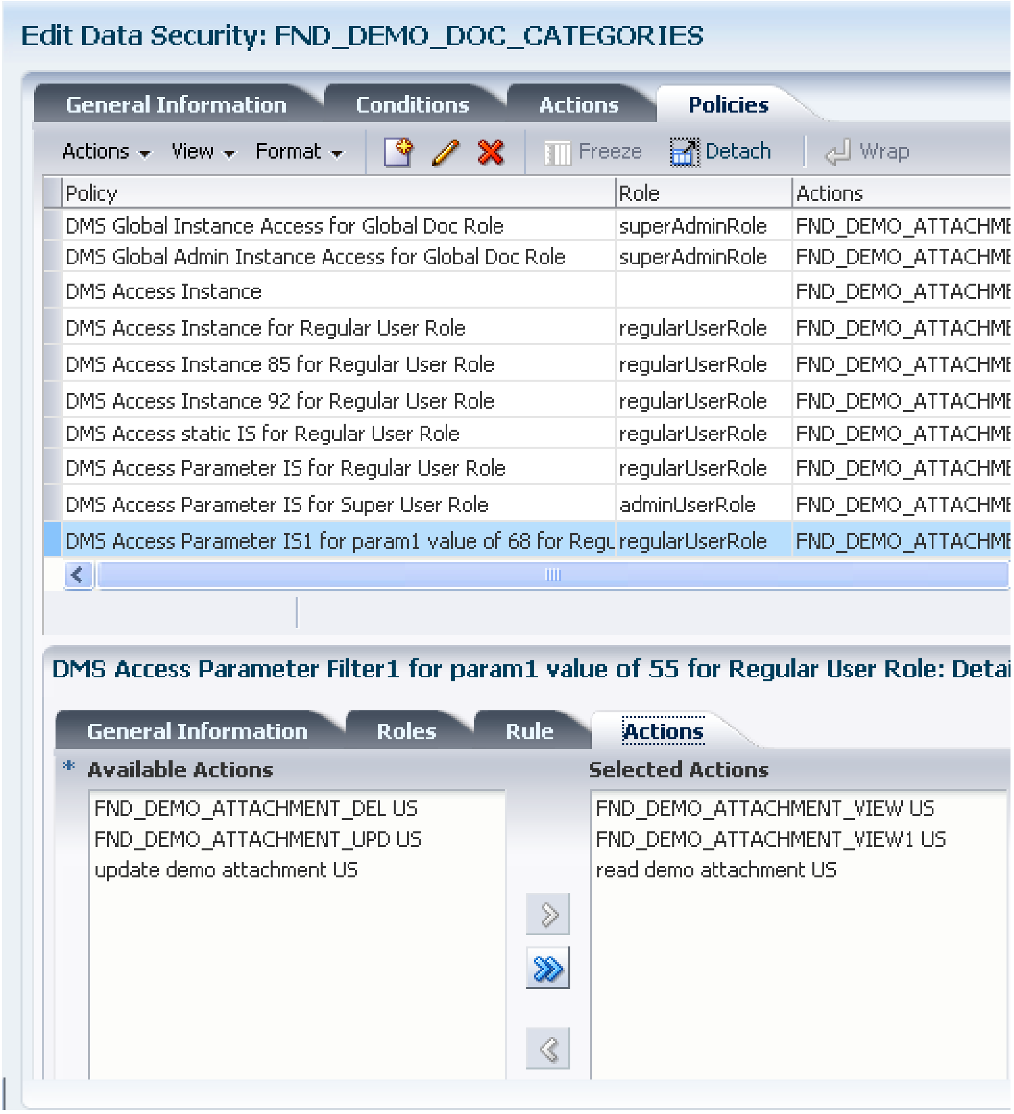
Select a Set of Database Rows for the Policy b

Display Name	Des
DMS_STATIC_INSTANCE_SET	DM
DMS_PARAMETERIZED_IS	DM
DMS_PARAMETERIZED_IS1	DM
DMS_STATIC_INSTANCE_SET1	DM
DMS_STATIC_FILTER1	DM
DMS_DYNAMIC_FILTER1	DM

6. In the **Action** tab of the **Details** section, click **New** and specify what kind of access data security policies will secure on the database resource. For details, see Section 11.3.3, "Managing Database Resource Actions."

   Figure 11–11 illustrates the **Actions** tab in the Edit Data Security page after several actions have been selected.

Figure 11–11 Creating a Data Security Policy - Selecting Actions



Edit Data Security: FND_DEMO_DOC_CATEGORIES

Policy	Role	Actions
DMS Global Instance Access for Global Doc Role	superAdminRole	FND_DEMO_ATTACHME
DMS Global Admin Instance Access for Global Doc Role	superAdminRole	FND_DEMO_ATTACHME
DMS Access Instance		FND_DEMO_ATTACHME
DMS Access Instance for Regular User Role	regularUserRole	FND_DEMO_ATTACHME
DMS Access Instance 85 for Regular User Role	regularUserRole	FND_DEMO_ATTACHME
DMS Access Instance 92 for Regular User Role	regularUserRole	FND_DEMO_ATTACHME
DMS Access static IS for Regular User Role	regularUserRole	FND_DEMO_ATTACHME
DMS Access Parameter IS for Regular User Role	regularUserRole	FND_DEMO_ATTACHME
DMS Access Parameter IS for Super User Role	adminUserRole	FND_DEMO_ATTACHME
DMS Access Parameter IS1 for param1 value of 68 for Regu	regularUserRole	FND_DEMO_ATTACHME

DMS Access Parameter Filter1 for param1 value of 55 for Regular User Role: Detai

* Available Actions	Selected Actions
FND_DEMO_ATTACHMENT_DEL US	FND_DEMO_ATTACHMENT_VIEW US
FND_DEMO_ATTACHMENT_UPD US	FND_DEMO_ATTACHMENT_VIEW1 US
update demo attachment US	read demo attachment US

7. Click **Save** to compete the creation of the data security policy.

11.4.2 Modifying a Custom Data Security Policy

Data security policies provided in the Oracle Fusion security reference implementation can be viewed but it is recommended that they not be modified; other data security policies, that is, those created with Oracle Authorization Policy Manager, can be modifed.

To modify a data security policy, proceed as follows:

1. Identify the data security policy to modify or view in either of the following ways:

   - By matching the name of the policy. For details, see Section 11.2.2, "Locating Policies Associated with a Database Resource."

   - By matching the name of the database resource that the policy secures. For details, see Section 11.2.1, "Searching Database Resources."

2. In the **Policies** tab, select the policy to modify from the **Policy** list and modify the following details for the data security policy:

   a. In the **General Information** tab, you can modify the policy start and end dates, as well as change the name of the policy and its description.

   b. In the **Roles** tab, you can change the roles to which the policy grants access. You can add a new role to the policy when you want to entitle all users who belong to that role with access to the data. You can also remove an existing role from the policy.

   c. In the **Rule** tab, you can change the rows of the database resource on which the policy applies in the following ways:

      – When you want to secure a specific row, select **Single Value**.

      – When you want to secure all rows, select **All Values**.

      – When you want to change the condition in order to change the secured rows of the database resource, select **Multiple Values** and click the **Search** icon and choose the desired condition. To create a new condition, see Section 11.3.2, "Managing Database Resource Conditions."

   d. In the **Actions** tab, you can change the actions on the database resource’s records secured by the policy. To create a new action, see Section 11.3.3, "Managing Database Resource Actions."

3. Click **Save** to complete the modification of the data security policy.

A

Using an OpenLDAP Identity Store

This appendix describes the special set up required in case the domain APM is running uses an OpenLDAP 2.2 identity store.

A.1 Using an OpenLDAP Identity Store

To use OpenLDAP 2.2 as a domain identity store with Oracle Authorization Policy Manager, proceed as follows:

1. Use the WebLogic Server administration console to create a new authenticator provider. For this new provider:
   - Select OpenLDAPAuthenticator from the list of authenticators.
   - Set the control flag of the OpenLDAPAuthenticator to SUFFICIENT.
   - Set the control flag of the DefaultAuthenticator to SUFFICIENT.
   - Change the order of authenticators to make the OpenLDAPAuthenticator the first in the list.
   - In the Provider Specific page for the OpenLDAPAuthenticator, enter User Base DN and Group Base DN, and set the value of the objectclass in the Group From Name Filter to something other than groupofnames.
2. From the Home directory of the OpenLDAP installation:
   - Open the file `slapd.conf` for edit.
   - In that file, insert the following line in the "include" section at the top:

     ```
     include ./schema/inetorgperson.schema
     ```

   - Save the file, and restart the OpenLDAP.

The above settings make possible adding the object class `inetorgperson` to every new external role you create in the OpenLDAP; this object class is required to map the external role to an application role.

B

Troubleshooting Oracle Authorization Policy Manager

This appendix describes common problems that you may encounter when configuring and using Oracle Authorization Policy Manager and explains how to solve them.

B.1 Unable to Login

This section explains one of the reasons why logging in Oracle Authorization Policy Manager may fail.

Symptom

Oracle Authorization Policy Manager logging in fails and the system outputs a message that contains a line similar to the following:

```
Cannot obtain connection: driverURL = jdbc:weblogic:pool:mds-ApplicationMDSDB,
props = {EmulateTwoPhaseCommit=false, connectionPoolID=mds-ApplicationMDSDB,
jdbcTxDataSource=true, LoggingLastResource=false,
dataSourceName=mds-ApplicationMDSDB}.
```

Diagnosis

The above message indicates that Oracle Authorization Policy Manager cannot establish a connection with the database mds-ApplicationMDSBD. Oracle Authorization Policy Manager requires that this database be present for a successful logging in.

For the list of databases required by APM, see Section 1.1, "Audience and Prerequisites."

Solution

Verify that referenced database is up, running, and available; then retry logging in.

B.2 Need Further Help?

You can find more solutions on My Oracle Support (formerly MetaLink) at `http://myoraclesupport.oracle.com`. If you do not find a solution to your problem, log a service request.

Index