

Oracle® Fusion Middleware

Administrator's Guide for Oracle Entitlements Server

11g Release 2 (11.1.2.2)

E27153-17

August 2015

This guide provides information on system configuration administration and management of policy objects using the Oracle Entitlements Server Administration Console. Manual configuration is also covered.

Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server, 11g Release 2 (11.1.2.2)

E27153-17

Copyright © 2011, 2015, Oracle and/or its affiliates. All rights reserved.

Primary Author: Priscilla Lee

Contributing Author: Michael Teger

Contributor: Oracle Entitlements Server Team

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

| | |
|---|------|
| Preface | xxv |
| Audience | xxv |
| Documentation Accessibility | xxv |
| Related Documents | xxv |
| Conventions | xxvi |
| | |
| 1 Introducing Oracle Entitlements Server | |
| 1.1 About Access Control | 1-1 |
| 1.2 Overview of Oracle Entitlements Server | 1-2 |
| 1.2.1 Understanding Oracle Entitlements Server Releases | 1-2 |
| 1.2.2 Using the Authorization Policy Manager Console | 1-2 |
| 1.2.3 Features of Oracle Entitlements Server 11gR2 | 1-3 |
| 1.3 Overview of the Oracle Entitlements Server Architecture | 1-3 |
| 1.3.1 The Policy Administration Point | 1-4 |
| 1.3.2 The Policy Decision Point and the Policy Enforcement Point | 1-5 |
| 1.3.2.1 Security Module as PDP | 1-5 |
| 1.3.2.2 Security Module as Combination PDP / PEP | 1-6 |
| 1.3.2.3 Understanding the Types of Security Modules | 1-7 |
| 1.3.3 The Policy Information Point | 1-8 |
| 1.4 How Oracle Entitlements Server Processes Authorization Policies | 1-8 |
| 1.5 About the Supported Access Control Standards | 1-9 |
| 1.5.1 Role-based Access Control (RBAC) | 1-10 |
| 1.5.2 Attribute-Based Access Control (ABAC) | 1-10 |
| 1.5.3 Java Permissions | 1-10 |
| 1.5.4 XACML | 1-10 |
| 1.5.5 PEP API | 1-11 |
| | |
| 2 Understanding the Policy Model | |
| 2.1 Understanding Oracle Entitlements Server Policies | 2-1 |
| 2.1.1 Understanding the Authorization Policy | 2-1 |
| 2.1.2 Understanding Role Assignments and the Role Mapping Policy | 2-2 |
| 2.2 How Oracle Entitlements Server Evaluates Policies | 2-4 |
| 2.3 The Policy Object Glossary | 2-4 |
| 2.4 Implementing a Policy Use Case | 2-7 |
| 2.4.1 Protecting Software Components | 2-8 |

| | | |
|-------|-----------------------------------|------|
| 2.4.2 | Protecting Business Objects | 2-10 |
|-------|-----------------------------------|------|

3 Getting Started

| | | |
|---------|---|------|
| 3.1 | Before You Begin..... | 3-1 |
| 3.2 | Understanding The Graphical Interface | 3-4 |
| 3.2.1 | Assigning Oracle Entitlements Server Administrators | 3-4 |
| 3.2.2 | Using the Identity Store | 3-4 |
| 3.2.3 | Accessing the Policy Store | 3-5 |
| 3.2.4 | Displaying Oracle Platform Security Services Application Grants | 3-5 |
| 3.3 | Accessing the Administration Console..... | 3-5 |
| 3.3.1 | Signing In to the Administration Console | 3-5 |
| 3.3.2 | Signing Out of the Administration Console | 3-6 |
| 3.4 | Navigating the Administration Console | 3-7 |
| 3.4.1 | Understanding the Main Tabs | 3-7 |
| 3.4.1.1 | Authorization Management Tab | 3-8 |
| 3.4.1.2 | System Configuration Tab..... | 3-8 |
| 3.4.2 | Using The Navigation Panel | 3-8 |
| 3.4.3 | Using the Home Tab..... | 3-10 |
| 3.4.4 | Accessing Help..... | 3-11 |
| 3.5 | Upgrading from Oracle Entitlements Server Basic | 3-11 |
| 3.5.1 | Changing From Basic to Advanced Policy Authorization..... | 3-12 |
| 3.6 | Accessing Oracle Entitlements Server Examples | 3-13 |

4 Managing Policies and Policy Objects

| | | |
|---------|---|------|
| 4.1 | Introducing Policy and Policy Object Management | 4-1 |
| 4.2 | Defining an Authorization Policy And Its Components..... | 4-2 |
| 4.3 | Adding Fine-Grained Elements to an Authorization Policy | 4-3 |
| 4.4 | Implementing An Authorization Policy Step by Step | 4-5 |
| 4.5 | Managing Policy Objects in An Application..... | 4-5 |
| 4.5.1 | Managing Applications..... | 4-6 |
| 4.5.1.1 | Creating an Application | 4-6 |
| 4.5.1.2 | Modifying an Application | 4-7 |
| 4.5.1.3 | Deleting an Application..... | 4-7 |
| 4.5.2 | Managing Resource Types | 4-7 |
| 4.5.2.1 | Creating a Resource Type..... | 4-8 |
| 4.5.2.2 | Modifying a Resource Type | 4-10 |
| 4.5.2.3 | Deleting a Resource Type..... | 4-10 |
| 4.5.3 | Managing Resources | 4-10 |
| 4.5.3.1 | Creating a Resource..... | 4-11 |
| 4.5.3.2 | Modifying a Resource | 4-12 |
| 4.5.3.3 | Deleting a Resource | 4-12 |
| 4.5.4 | Managing Entitlements..... | 4-13 |
| 4.5.4.1 | Creating an Entitlement..... | 4-13 |
| 4.5.4.2 | Modifying an Entitlement | 4-15 |
| 4.5.4.3 | Deleting an Entitlement..... | 4-15 |
| 4.5.5 | Managing Authorization Policies..... | 4-16 |
| 4.5.5.1 | Creating an Authorization Policy | 4-16 |

| | | |
|---------|---|------|
| 4.5.5.2 | Modifying an Authorization Policy | 4-19 |
| 4.5.5.3 | Deleting an Authorization Policy | 4-20 |
| 4.5.6 | Managing Application Roles in the Role Catalog..... | 4-21 |
| 4.5.6.1 | Creating an Application Role | 4-22 |
| 4.5.6.2 | Modifying an Application Role..... | 4-23 |
| 4.5.6.3 | Mapping External Roles to an Application Role..... | 4-23 |
| 4.5.6.4 | Mapping an External User to an Application Role..... | 4-24 |
| 4.5.6.5 | Deleting an Application Role or Removing External Role Mappings | 4-25 |
| 4.5.6.6 | Removing External User Mappings..... | 4-25 |
| 4.5.7 | Managing Role Mapping Policies..... | 4-25 |
| 4.5.7.1 | Creating a Role Mapping Policy..... | 4-26 |
| 4.5.7.2 | Modifying a Role Mapping Policy | 4-28 |
| 4.5.7.3 | Deleting a Role Mapping Policy | 4-28 |
| 4.5.8 | Managing a Role Category | 4-28 |
| 4.5.9 | Managing Attributes and Functions as Extensions | 4-29 |
| 4.5.9.1 | Creating an Attribute | 4-30 |
| 4.5.9.2 | Modifying an Attribute..... | 4-31 |
| 4.5.9.3 | Deleting an Attribute | 4-31 |
| 4.5.9.4 | Creating a Function | 4-31 |
| 4.5.9.5 | Modifying a Function..... | 4-32 |
| 4.5.9.6 | Deleting a Function | 4-32 |
| 4.6 | Using the Condition Builder | 4-33 |
| 4.6.1 | Building a Complex Expression | 4-36 |
| 4.6.2 | Passing Parameters to Functions..... | 4-36 |

5 Querying Security Objects

| | | |
|--------|--|------|
| 5.1 | Searching with the Administration Console..... | 5-1 |
| 5.2 | Finding Objects with a Simple Search..... | 5-2 |
| 5.3 | Finding Objects with an Advanced Search | 5-3 |
| 5.3.1 | Searching External Roles | 5-4 |
| 5.3.2 | Searching Applications | 5-4 |
| 5.3.3 | Searching Resource Types | 5-5 |
| 5.3.4 | Searching Application Roles | 5-6 |
| 5.3.5 | Searching Role Mapping Policies | 5-6 |
| 5.3.6 | Searching Resources | 5-7 |
| 5.3.7 | Searching Entitlements | 5-8 |
| 5.3.8 | Searching Authorization Policies | 5-9 |
| 5.3.9 | Searching Attributes | 5-11 |
| 5.3.10 | Searching Functions | 5-12 |
| 5.3.11 | Searching for Users..... | 5-12 |
| 5.4 | Understanding Case Sensitivity in Object Names | 5-13 |

6 Managing Policy Distribution

| | | |
|-------|-----------------------------------|-----|
| 6.1 | Defining Distribution Modes | 6-1 |
| 6.1.1 | Controlled Distribution..... | 6-1 |
| 6.1.2 | Non-controlled Distribution | 6-2 |

| | | |
|---------|--|------|
| 6.2 | Understanding Policy Distribution | 6-2 |
| 6.2.1 | Using a Central Policy Distribution Component | 6-3 |
| 6.2.2 | Using a Local Policy Distribution Component..... | 6-3 |
| 6.3 | Distributing Policies | 6-4 |
| 6.3.1 | Distributing Policies Using the Administration Console | 6-4 |
| 6.4 | Using Default or Third Party Digital Certificates | 6-5 |
| 6.4.1 | Configuring Oracle Entitlements Server Security Module (Client) When Third Party Certificate is Used in Administration Server 6-6 | |
| 6.4.1.1 | Configuring the WebLogic Security Module if a Third Party Digital Certificate Is Used On the Administration Side 6-6 | |
| 6.4.1.2 | Configuring the Web Services or Java Security Module if a Third Party Digital Certificate Is Used On the Administration Side 6-7 | |
| 6.4.1.3 | Configuring the IBM WebSphere Application Server Security Module if a Third Party Digital Certificate Is Used On the Administration Side 6-7 | |
| 6.4.2 | Adding Signer if Third Party Certificate Is Used in a Security Module with an IBM Websphere Administration Side 6-9 | |
| 6.4.3 | Adding Signer if Third Party Certificate Is Used in a Security Module with a WebLogic Administration Side 6-10 | |
| 6.4.4 | Using a Third Party Certificate with a WebLogic Server Security Module | 6-10 |
| 6.4.5 | Using a Third Party Certificate with a Web Services or Java Security Module..... | 6-12 |
| 6.4.6 | Using a Third Party Certificate with a WebSphere Application Server Security Module 6-13 | |
| 6.4.7 | Using a Third Party Certificate with a Tomcat or JBoss Security Module | 6-15 |
| 6.5 | Debugging Policy Distribution | 6-15 |

7 Deploying the Policy Decision Point

| | | |
|-------|---|-----|
| 7.1 | Understanding the PDP Deployment Models | 7-1 |
| 7.1.1 | Embedding the PDP Locally | 7-2 |
| 7.1.2 | Locating the PDP Remotely | 7-2 |
| 7.2 | Using the Security Module Proxy Mode | 7-3 |
| 7.3 | Using the XACML Gateway..... | 7-3 |

8 Managing Security Module Configurations

| | | |
|-------|--|------|
| 8.1 | Before You Begin..... | 8-1 |
| 8.2 | Starting the SMConfig UI..... | 8-2 |
| 8.3 | Modifying Security Module Configurations..... | 8-4 |
| 8.4 | Configuring Security Modules Post-Instantiation | 8-4 |
| 8.4.1 | Configuring the Java Security Module | 8-5 |
| 8.4.2 | Configuring the RMI Security Module..... | 8-10 |
| 8.4.3 | Configuring the Web Services Security Module | 8-10 |
| 8.4.4 | Configuring the WebLogic Server Security Module | 8-11 |
| 8.4.5 | Configuring the SharePoint Server (MOSS) Security Module | 8-12 |
| 8.4.6 | Configuring the .NET Security Module | 8-12 |
| 8.4.7 | Configuring the WebSphere, Tomcat and JBoss Security Modules | 8-12 |
| 8.4.8 | Configuring the Oracle Service Bus Security Module..... | 8-13 |
| 8.5 | Configuring the PDP Proxy Client for RMI or Web Services..... | 8-14 |

9 Securing Environment Specific Resources

| | | |
|---------|---|------|
| 9.1 | Choosing a Security Module Type | 9-1 |
| 9.2 | Securing Microsoft Office SharePoint Server Resources | 9-3 |
| 9.2.1 | Protecting SharePoint Resources | 9-3 |
| 9.2.1.1 | Protecting Web Sites and Web Pages | 9-4 |
| 9.2.1.2 | Protecting Web Parts | 9-5 |
| 9.2.1.3 | Protecting Lists | 9-5 |
| 9.2.1.4 | Protecting Sensitive Content Within Web Pages | 9-6 |
| 9.2.2 | Instantiating the MOSS and Web Services Security Modules | 9-6 |
| 9.2.3 | Integrating and Disintegrating the MOSS Security Module | 9-7 |
| 9.2.4 | Configuring for SharePoint Security | 9-7 |
| 9.3 | Securing Oracle Service Bus Resources | 9-13 |
| 9.3.1 | Examining the OSB Resource Object | 9-13 |
| 9.3.2 | Mapping Message Level OSB Resources to Oracle Entitlements Server | 9-14 |
| 9.3.3 | Mapping Transport Level OSB Resources to Oracle Entitlements Server | 9-14 |
| 9.3.4 | Enabling the WebLogic Server Providers | 9-15 |
| 9.4 | Securing WebLogic Server Resources | 9-15 |
| 9.4.1 | Integrating with WebLogic Server | 9-16 |
| 9.4.2 | Discovering WebLogic Server Resources | 9-16 |
| 9.4.2.1 | Enabling Discovery Mode | 9-17 |
| 9.4.2.2 | Loading Discovered Resources | 9-17 |
| 9.4.3 | Converting WebLogic Server Resources | 9-18 |
| 9.4.4 | Mapping WebLogic Server Resources to Policy Objects | 9-19 |
| 9.4.4.1 | Enterprise Java Bean Resources | 9-19 |
| 9.4.4.2 | Java Naming and Directory Interface Resources | 9-20 |
| 9.4.4.3 | URL Resources | 9-21 |
| 9.4.4.4 | JDBC Resources | 9-25 |
| 9.4.4.5 | JMS Resources | 9-27 |
| 9.4.4.6 | Web Services Resources | 9-29 |
| 9.4.4.7 | Server Resources | 9-31 |
| 9.5 | Securing Oracle WebCenter Content Resources | 9-33 |
| 9.5.1 | About the Oracle WebCenter Content and Oracle Entitlements Server Integration | 9-33 |
| 9.5.2 | Terminology for Oracle WebCenter Content and Oracle Entitlements Server Directories | 9-35 |
| 9.5.3 | Integration Roadmap | 9-35 |
| 9.5.4 | Prerequisites | 9-37 |
| 9.5.4.1 | Reviewing System Requirements and Certification | 9-37 |
| 9.5.4.2 | Installing the Oracle Database | 9-37 |
| 9.5.4.3 | Installing the Oracle WebLogic Server and Creating the Oracle Middleware Home | 9-38 |
| 9.5.4.4 | Installing Oracle Identity and Access Management Suite 11g R2PS2 in the WebLogic Home | 9-38 |
| 9.5.4.5 | Obtaining Oracle Entitlements Server Client Software | 9-38 |
| 9.5.4.6 | Installing Oracle Entitlements Server Client | 9-38 |
| 9.5.5 | Oracle WebCenter Content Base Installation | 9-38 |
| 9.5.5.1 | Installing Oracle WebCenter Content | 9-39 |

| | | |
|----------|---|------|
| 9.5.5.2 | Creating the Oracle WebCenter Content Schema..... | 9-40 |
| 9.5.5.3 | Creating the WebCenter Domain | 9-41 |
| 9.5.5.4 | Starting the Servers in the WebCenter Domain | 9-43 |
| 9.5.5.5 | Configuring WebCenter Content | 9-44 |
| 9.5.6 | Configuring Oracle Entitlements Server | 9-44 |
| 9.5.6.1 | Running RCU to Create the OPSS Schema | 9-44 |
| 9.5.6.2 | Creating the OES Domain using the IDM Configuration Wizard | 9-45 |
| 9.5.7 | Configuring the OES Security Store using the Security Store Configuration Tool. | 9-45 |
| 9.5.8 | Integrating WebCenter Content with OES..... | 9-46 |
| 9.5.8.1 | Creating a Data Source in Oracle WebCenter Content Domain..... | 9-46 |
| 9.5.8.2 | Reassociating Oracle WebCenter Content Domain Security Store | 9-47 |
| 9.5.8.3 | Updating the config.cfg File of the WCC Domain..... | 9-48 |
| 9.5.8.4 | Adding Permission in JRE for WebCenter Content Version is 11.1.1.7.0 or Lower.... | 9-48 |
| 9.5.8.5 | Installing the WCC-OES Connector..... | 9-48 |
| 9.5.9 | Creating the Application, Resource Types, Resources, and Policies | 9-49 |
| 9.5.9.1 | Creating a New Application | 9-49 |
| 9.5.9.2 | Creating the UCM Pre-Search Query Resource Type | 9-50 |
| 9.5.9.3 | Creating the UCM CRUD Operation Resource Type..... | 9-50 |
| 9.5.9.4 | Creating a Resource..... | 9-50 |
| 9.5.9.5 | Creating Policies | 9-51 |
| 9.5.10 | Verification and Troubleshooting | 9-52 |
| 9.5.10.1 | Verifying Oracle WebCenter Content Is Working..... | 9-52 |
| 9.5.10.2 | Troubleshooting Tips | 9-53 |
| 9.5.11 | Post-Integration Set Up (Example)..... | 9-54 |
| 9.5.11.1 | Creating Users in the OES Domain (oes_domain)..... | 9-54 |
| 9.5.11.2 | Creating Users in the WebCenter Content Domain (wcc_domain) | 9-54 |
| 9.5.11.3 | Adding Metadata Values Using the Configuration Manager in WebCenter Content | 9-54 |
| 9.5.11.4 | Checking In Documents | 9-55 |

10 Managing System Configurations

| | | |
|--------|---|------|
| 10.1 | Delegating With Administrators | 10-1 |
| 10.2 | Configuring Security Module Definitions..... | 10-1 |
| 10.2.1 | Creating a Security Module Definition..... | 10-2 |
| 10.2.2 | Binding an Application to a Security Module | 10-2 |
| 10.2.3 | Unbinding an Application From a Security Module..... | 10-3 |
| 10.2.4 | Deleting a Security Module Definition..... | 10-3 |
| 10.3 | Configuring Identity Directory Service Profiles..... | 10-3 |
| 10.3.1 | Creating an Identity Directory Service Profile | 10-4 |
| 10.3.2 | Binding an Application to an Identity Directory Service Profile..... | 10-6 |
| 10.3.3 | Unbinding an Application From an Identity Directory Service Profile | 10-7 |
| 10.3.4 | Deleting an Identity Directory Service Profile..... | 10-7 |

11 Delegating With Administrator Roles

| | | |
|------|---|------|
| 11.1 | About Delegated Administrators | 11-1 |
| 11.2 | Delegating Using Scope and Granularity..... | 11-2 |

| | | |
|--------|---|-------|
| 11.3 | Delegating Application Administration..... | 11-3 |
| 11.3.1 | Adding a Delegated Administrator for An Application..... | 11-3 |
| 11.3.2 | Modifying or Deleting an Application's Delegated Administrator | 11-5 |
| 11.4 | Using Policy Domains to Delegate..... | 11-5 |
| 11.4.1 | Creating a Policy Domain..... | 11-6 |
| 11.4.2 | Modifying a Policy Domain | 11-6 |
| 11.4.3 | Deleting a Policy Domain..... | 11-6 |
| 11.5 | Delegating Policy Domain Administration..... | 11-7 |
| 11.5.1 | Adding a Delegated Administrator to a Policy Domain | 11-7 |
| 11.5.2 | Modifying or Deleting a Policy Domain's Delegated Administrator | 11-8 |
| 11.6 | Managing System Administrators Using Administrator Roles..... | 11-8 |
| 11.6.1 | Creating a New Administrator Role..... | 11-9 |
| 11.6.2 | Assigning Privileges to an Administrator Role..... | 11-9 |
| 11.6.3 | Modifying Administrator Role Membership..... | 11-10 |
| 11.6.4 | Deleting an Administrator Role..... | 11-10 |

12 Customizing the Administration Console

| | | |
|------|---|------|
| 12.1 | Customizing Authorization Policy Manager..... | 12-1 |
| 12.2 | Customizing Headers, Footers, and Logo..... | 12-2 |
| 12.3 | Customizing Color Schemes | 12-3 |
| 12.4 | Customizing the Login Page | 12-3 |

13 Management Tasks

| | | |
|----------|---|-------|
| 13.1 | Moving from a Test Environment to Production (T2P)..... | 13-1 |
| 13.2 | Using the Policy Simulator..... | 13-1 |
| 13.2.1 | Understanding Policy Simulation..... | 13-2 |
| 13.2.2 | Choosing the Policy Simulation Mode..... | 13-2 |
| 13.2.3 | Running the Policy Simulator..... | 13-3 |
| 13.2.3.1 | Running the Policy Simulator in Simple Mode..... | 13-3 |
| 13.2.3.2 | Running the Policy Simulator in Advanced Mode..... | 13-4 |
| 13.3 | Using FIPS-compliant Security Providers..... | 13-6 |
| 13.3.1 | Installing the JCE Provider..... | 13-6 |
| 13.3.2 | Configuring JCE..... | 13-6 |
| 13.4 | Managing Audit Tasks..... | 13-6 |
| 13.4.1 | Auditing Oracle Entitlements Server Events..... | 13-7 |
| 13.4.2 | Enabling Audit | 13-8 |
| 13.4.3 | Loading the Audit Log to a Database..... | 13-9 |
| 13.4.3.1 | Creating the Audit View Schema using RCU..... | 13-9 |
| 13.4.3.2 | Extending the OES Domain using the IDM Configuration Wizard | 13-10 |
| 13.4.3.3 | Configuring Audit Settings..... | 13-10 |
| 13.4.4 | Configuring Oracle Entitlements Server Security Modules for Auditing..... | 13-11 |
| 13.4.4.1 | Configuring the WebLogic Server Security Module..... | 13-11 |
| 13.4.4.2 | Configuring Other Security Modules..... | 13-12 |
| 13.4.5 | Additional Auditing Information..... | 13-13 |
| 13.5 | Migrating Policies..... | 13-13 |
| 13.5.1 | Migrating From XML to LDAP..... | 13-13 |

| | | |
|----------|--|-------|
| 13.5.2 | Migrating From LDAP to XML..... | 13-15 |
| 13.5.3 | Migrating From XML to Database | 13-17 |
| 13.5.4 | Migrating From Database to XML | 13-20 |
| 13.6 | Configuring Cache..... | 13-22 |
| 13.6.1 | Configuring Decision Caching..... | 13-22 |
| 13.6.2 | Configuring Attribute Caching..... | 13-23 |
| 13.7 | Logging..... | 13-23 |
| 13.8 | Debugging..... | 13-25 |
| 13.8.1 | Enabling Debugging By Defining Parameters | 13-26 |
| 13.8.1.1 | Configuring Logging for Debugging..... | 13-26 |
| 13.8.1.2 | Searching Logs to Debug Authorization Policies | 13-27 |
| 13.8.2 | Enabling Debugging Using Methods | 13-32 |
| 13.8.3 | Debugging Policy Distribution..... | 13-32 |

14 Configuring a Disaster Recovery Solution

| | | |
|---------|---|-------|
| 14.1 | Overview of a Multi-Site Deployment..... | 14-1 |
| 14.2 | Multi-Site Deployment Topology..... | 14-2 |
| 14.3 | Task Roadmap | 14-3 |
| 14.4 | Prerequisites..... | 14-5 |
| 14.5 | Configuring Disaster Recovery for Oracle Entitlements Server | 14-5 |
| 14.5.1 | Setting Up the Primary Server | 14-6 |
| 14.5.2 | Setting Up the Standby Server (Duplicate) | 14-8 |
| 14.5.3 | Test Log Transfer | 14-10 |
| 14.5.4 | Configuring the Oracle Data Guard Broker..... | 14-10 |
| 14.5.5 | Testing Failover and Switchover | 14-11 |
| 14.5.6 | Configuring a Virtual Device for Oracle ASM | 14-12 |
| 14.5.7 | Installing Oracle Grid Infrastructure for a Standalone Server | 14-13 |
| 14.5.8 | Configuring Oracle Restart | 14-13 |
| 14.5.9 | Installing OPSS Schema | 14-14 |
| 14.5.10 | Installing the Primary Administration Server..... | 14-14 |
| 14.5.11 | Installing the Secondary Administration Server..... | 14-15 |
| 14.5.12 | Configuring the Security Module..... | 14-16 |

15 Configuring an Oracle RAC Disaster Recovery Solution

| | | |
|--------|--|------|
| 15.1 | Multi-Site Oracle Data Guard with Oracle RAC Database Deployment Topology..... | 15-1 |
| 15.2 | Oracle RAC Primary to Oracle RAC Standby Data Guard..... | 15-3 |
| 15.2.1 | Installing Oracle Clusterware | 15-3 |
| 15.2.2 | Installing Oracle Real Application Clusters..... | 15-3 |
| 15.3 | Setting Up Data Guard for Oracle RAC Databases..... | 15-4 |
| 15.3.1 | Preparing the Primary Database for Standby Database Creation | 15-4 |
| 15.3.2 | Creating a Physical Standby Database | 15-5 |
| 15.3.3 | Configuring the Oracle Data Guard Broker..... | 15-6 |
| 15.3.4 | Performing Switchover and Failover Operations with Data Guard Broker | 15-6 |
| 15.4 | Configuring Oracle Entitlements Server for High Availability Disaster Recovery | 15-6 |
| 15.4.1 | Oracle Entitlements Server High Availability Disaster Recovery Configuration Roadmap | 15-6 |
| 15.4.2 | Prerequisites for Installing Oracle Entitlements Server | 15-7 |

| | | |
|----------|---|-------|
| 15.4.3 | Installing OPSS Schema | 15-7 |
| 15.4.4 | Installing Oracle Entitlements Server Administration Server Cluster on Master Policy Store on OESHOST1 | 15-7 |
| 15.4.4.1 | Install Oracle Entitlements Server Administration Server with Primary Oracle RAC Database | 15-7 |
| 15.4.4.2 | Create the Oracle Entitlements Server Administration Server Domain with WebLogic Server Cluster | 15-7 |
| 15.4.4.3 | Configuring Security Store for Oracle Entitlements Server Administration Server... | 15-9 |
| 15.4.4.4 | Configuring Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP Request Distribution | 15-10 |
| 15.4.4.5 | Access the Oracle Entitlements Server Administration Console..... | 15-10 |
| 15.4.5 | Installing Oracle Entitlements Server Client in High Availability Environment.. | 15-10 |
| 15.4.6 | Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Master Oracle RAC Database Policy Store | 15-10 |
| 15.4.7 | Installing Oracle Entitlements Server Administration Server Cluster..... | 15-12 |
| 15.4.7.1 | Install Oracle Entitlements Server Administration Server with Secondary Oracle RAC Database | 15-12 |
| 15.4.7.2 | Create the Oracle Entitlements Server Administration Server Domain with WebLogic Server Cluster | 15-12 |
| 15.4.7.3 | Export Encryption Key from Primary Domain..... | 15-14 |
| 15.4.7.4 | Configuring Security Store for Oracle Entitlements Server Administration Server... | 15-14 |
| 15.4.7.5 | Configuring Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP Request Distribution | 15-15 |
| 15.4.7.6 | Access the Oracle Entitlements Server Administration Console..... | 15-15 |
| 15.4.8 | Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Secondary Oracle RAC Database Policy Store | 15-15 |

16 Tuning Performance and Monitoring Components

| | | |
|----------|--|-------|
| 16.1 | Understanding Key Concepts and Components in Oracle Entitlements Server Deployment | 16-1 |
| 16.2 | Oracle Entitlements Server Performance Planning..... | 16-1 |
| 16.2.1 | Define Your Performance Objectives and Requirements | 16-2 |
| 16.2.1.1 | Understand Performance Constraints..... | 16-2 |
| 16.2.1.2 | Define Operational Requirements | 16-3 |
| 16.2.1.3 | Identify Performance Goals | 16-3 |
| 16.2.1.4 | Conduct Performance Evaluations | 16-3 |
| 16.2.2 | Design Authorization for Applications..... | 16-3 |
| 16.2.2.1 | Policy Design..... | 16-3 |
| 16.2.2.2 | Best Practices for Designing Application Authorization..... | 16-5 |
| 16.3 | Performance Tuning Considerations for Oracle Entitlements Server..... | 16-6 |
| 16.3.1 | Tuning the OES Policy Store | 16-6 |
| 16.3.1.1 | Oracle Database System Parameters Tuning..... | 16-6 |
| 16.3.1.2 | Oracle Database REDO Log and UNDO Tablespace Tuning | 16-9 |
| 16.3.1.3 | Tablespaces Tuning | 16-10 |
| 16.3.1.4 | Schema Statistics Gathering..... | 16-11 |
| 16.3.1.5 | EclipseLink Tuning | 16-12 |

| | | |
|----------|--|-------|
| 16.3.2 | Tuning of OES Administration Server..... | 16-13 |
| 16.3.2.1 | WLST Tuning | 16-13 |
| 16.3.2.2 | OES Administration Server Tuning..... | 16-13 |
| 16.3.3 | Tuning OES Security Modules..... | 16-14 |
| 16.3.3.1 | OES Security Module Memory Sizing | 16-15 |
| 16.3.3.2 | WebLogic Security Module..... | 16-17 |
| 16.3.3.3 | Java Security Module | 16-17 |
| 16.3.3.4 | Web Service Security Module..... | 16-18 |
| 16.3.3.5 | Tomcat Security Module | 16-18 |
| 16.3.4 | Tuning OES Distribution Service | 16-18 |
| 16.3.5 | Tuning OES Attribute Retrievers | 16-19 |
| 16.3.6 | Tuning OES Cache..... | 16-19 |
| 16.3.7 | Tuning Resource Intensive Operations | 16-20 |
| 16.3.8 | Enabling Logging..... | 16-20 |
| 16.3.8.1 | Enable Logging for Performance Measurement | 16-20 |
| 16.3.8.2 | Enable Logging for Snapshot Generation Measurement..... | 16-21 |
| 16.3.8.3 | Enable Logging for Migration Performance Measurement | 16-21 |

A Installation and Configuration Parameters

| | | |
|---------|--|------|
| A.1 | Policy Distribution Configuration..... | A-1 |
| A.1.1 | Policy Distribution Component Server Configuration | A-1 |
| A.1.2 | Policy Distribution Component Client Configuration..... | A-2 |
| A.1.2.1 | Policy Distribution Component Client Java Standard Edition Configuration (Controlled Push Mode) A-2 | |
| A.1.2.2 | Policy Distribution Component Client Java Enterprise Edition Container Configuration (Controlled Push Mode) A-6 | |
| A.1.2.3 | Policy Distribution Client Configuration (Controlled-Pull Mode) | A-9 |
| A.1.2.4 | Policy Distribution Client Configuration (Non-controlled Mode)..... | A-13 |
| A.1.2.5 | Policy Distribution Client Configuration (Mixed Mode) | A-13 |
| A.2 | Security Module Configuration | A-17 |
| A.2.1 | Java Security Module | A-17 |
| A.2.2 | Web Services Security Module | A-21 |
| A.2.3 | Web Services Security Module on WebLogic Server | A-23 |
| A.2.4 | RMI Security Module | A-25 |
| A.2.5 | WebLogic Server Security Module..... | A-26 |
| A.2.6 | WebLogic Server Security Module Discovery Mode | A-26 |
| A.3 | PDP Proxy Client Configuration | A-27 |
| A.3.1 | Web Services Security Module PDP Proxy Client | A-27 |
| A.3.2 | RMI Security Module PDP Proxy Client..... | A-29 |
| A.4 | Policy Store Service Configuration..... | A-30 |

B Configuring Attribute Retrievers

| | | |
|-------|--|-----|
| B.1 | Understanding Predefined Attribute Retrievers..... | B-1 |
| B.2 | Configuring the Attribute Retrievers Using SMConfig UI..... | B-1 |
| B.2.1 | Prerequisites | B-2 |
| B.2.2 | Running the SMConfig UI to Edit the jps-config.xml File..... | B-2 |
| B.2.3 | Adding, Editing, or Deleting Attribute Retrievers | B-2 |

| | | |
|---------|--|------|
| B.2.4 | Adding, Editing, or Deleting Attributes in Attribute Retriever Configuration | B-5 |
| B.3 | Configuring the Predefined Attribute Retrievers Manually | B-6 |
| B.3.1 | Roadmap | B-6 |
| B.3.2 | Configuring Individual Attribute Values | B-7 |
| B.3.3 | Declaring the PIP Service Provider | B-8 |
| B.3.4 | Configuring Repository Connection..... | B-8 |
| B.3.4.1 | Configuring the LDAP Repository Attribute Retriever Parameters..... | B-9 |
| B.3.4.2 | Configuring the Database Repository Attribute Retriever Parameters..... | B-10 |
| B.3.4.3 | Setting Up PIP Connection Credentials | B-12 |
| B.3.4.4 | Updating the Database Password | B-13 |
| B.3.5 | Declaring the Predefined Attribute Retriever Reference in jpsContexts Section | B-13 |
| B.3.6 | Configuring Cache and Failover | B-14 |
| B.3.7 | Sample jps-config.xml File..... | B-15 |
| B.4 | Configuring the Custom Attribute Retrievers Manually | B-20 |
| B.4.1 | Configuring the jps-config.xml Configuration File | B-20 |
| B.4.2 | Implementing Custom PIP Interface | B-21 |

C Configuring an Oracle Service Bus 12.1.3 Domain to Take Use of an OSB Security Module from OES 11.1.2.2

| | | |
|-----|--|-----|
| C.1 | Configuring an Oracle Service Bus 12.1.3 Domain to Take Use of an OSB Security Module from Oracle Entitlements Server 11.1.2.2 C-1 | |
| C.2 | Configuring OSB Security..... | C-3 |

D Configuring Enterprise Role Based Authorization for Oracle API Gateway and OES Integration

| | | |
|-------|--|-----|
| D.1 | Configure LDAP Identity Store | D-1 |
| D.1.1 | Add LDAP Identity Store Instance | D-1 |
| D.1.2 | Add idstore.oid Instance into Default Context | D-2 |
| D.1.3 | Add LDAP Principal to Bootstrap Credential Store..... | D-2 |
| D.2 | Use Username in String as SubjectObj for PepRequest..... | D-2 |

E Managing Advanced Policies with WLST

| | | |
|--------|---|-----|
| E.1 | Using the WebLogic Scripting Tool with Oracle Entitlements Server | E-1 |
| E.2 | Using the WLST Commands..... | E-1 |
| E.2.1 | createApplicationPolicy | E-2 |
| E.2.2 | updateResourceType..... | E-2 |
| E.2.3 | updateResource..... | E-3 |
| E.2.4 | createPolicy | E-4 |
| E.2.5 | updatePolicy | E-5 |
| E.2.6 | deletePolicy..... | E-7 |
| E.2.7 | listPolicies | E-7 |
| E.2.8 | createAttribute..... | E-7 |
| E.2.9 | updateAttribute..... | E-8 |
| E.2.10 | deleteAttribute | E-8 |
| E.2.11 | listAttributes | E-9 |
| E.2.12 | createFunction | E-9 |

| | | |
|--------|------------------------------------|------|
| E.2.13 | updateFunction | E-10 |
| E.2.14 | deleteFunction..... | E-10 |
| E.2.15 | listFunctions..... | E-11 |
| E.2.16 | getFunction | E-11 |
| E.2.17 | listAppRoles | E-11 |
| E.2.18 | getResourceType..... | E-12 |
| E.2.19 | getResource..... | E-12 |
| E.3 | Creating Policy with a Script..... | E-12 |

Index

List of Tables

| | | |
|------|---|-------|
| 6-1 | Web Services or Java Security Module Parameters | 6-6 |
| 6-2 | IBM WebSphere Security Module Parameter | 6-8 |
| 6-3 | Storing and Managing Certificate Options | 6-11 |
| 6-4 | Using the Identity Keystore Attributes..... | 6-11 |
| 6-5 | Using Trust Keystore Attributes..... | 6-11 |
| 8-1 | Security Modules with Supported Policy Distribution Modes | 8-2 |
| 8-2 | Java Security Module Controlled-Push Client Configuration | 8-5 |
| 8-3 | Java Security Module Controlled-Pull Client and Store Configuration | 8-6 |
| 8-4 | Java Security Module Non-controlled Policy Store Configuration | 8-6 |
| 8-5 | Java Security Module Advanced Properties | 8-7 |
| 8-6 | Java Security Module PIP Parameters (Attribute Retrievers) | 8-8 |
| 8-7 | Java Security Module PIP Parameters (Attributes)..... | 8-9 |
| 9-1 | General Protection Security Module Types | 9-1 |
| 9-2 | Environment Specific Security Module Types | 9-3 |
| 9-3 | appSettings Properties for the MOSS Application..... | 9-9 |
| 9-4 | WebLogic Server Authorization Policy Objects | 9-18 |
| 9-5 | Mapping EJB Definitions to Policy Objects..... | 9-19 |
| 9-6 | Mapping JNDI Definitions to Policy Objects | 9-20 |
| 9-7 | URL Resource Values Mapped to Oracle Entitlements Server Objects | 9-21 |
| 9-8 | Dynamic Attributes Supported by URL Resources | 9-23 |
| 9-9 | JDBC Values Mapped to Oracle Entitlements Server Objects | 9-25 |
| 9-10 | JDBC Resource Action Options..... | 9-26 |
| 9-11 | Dynamic Attributes Supported by JDBC Resources..... | 9-27 |
| 9-12 | JMS Values Mapped to Oracle Entitlements Server Objects | 9-27 |
| 9-13 | JMS Resource Action Options | 9-29 |
| 9-14 | Dynamic Attributes Supported by JMS Resources | 9-29 |
| 9-15 | Web Services Values Mapped to Oracle Entitlements Server Objects | 9-30 |
| 9-16 | Dynamic Attributes Supported by Web Services Resources..... | 9-31 |
| 9-17 | Server Resource Values Mapped to Oracle Entitlements Server Objects | 9-32 |
| 9-18 | Server Resource Action Options | 9-33 |
| 9-19 | Dynamic Attributes Supported by Server Resource..... | 9-33 |
| 9-20 | Supported Oracle WebCenter Content Document Operations..... | 9-34 |
| 9-21 | Integration Roadmap..... | 9-35 |
| 9-22 | Action Comparison..... | 9-52 |
| 13-1 | Events Audited in Oracle Entitlements Server | 13-7 |
| 13-2 | Auditing Parameters in jps-config.xml..... | 13-11 |
| 13-3 | Decision Caching Parameters..... | 13-23 |
| 13-4 | Logging Server Issues..... | 13-24 |
| 14-1 | Configuration Flow for Disaster Recovery Solution..... | 14-4 |
| 15-1 | Oracle Entitlements Server Disaster Recovery Configuration Flow | 15-6 |
| 16-1 | Oracle Database System Parameters Tuning | 16-7 |
| 16-2 | Specifying the Tablespace to Edit..... | 16-10 |
| 16-3 | Specifying the Size of a Datafile..... | 16-11 |
| 16-4 | EclipseLink Tuning | 16-12 |
| 16-5 | Security Module Tuning Attributes | 16-14 |
| 16-6 | Policy Artifacts | 16-16 |
| 16-7 | Web Service Security Module Parameters | 16-18 |
| 16-8 | Tuning OES Cache Example Configuration | 16-19 |
| A-1 | Policy Distribution Server Configuration..... | A-1 |
| A-2 | Policy Distribution Client Configuration, JSE, Controlled Push Mode | A-2 |
| A-3 | Policy Distribution Client Configuration, JEE, Controlled Push Mode..... | A-6 |
| A-4 | Policy Distribution Client Configuration, Controlled-Pull Mode | A-9 |
| A-5 | Policy Distribution Client Configuration, Non-controlled Mode..... | A-13 |

| | | |
|------|---|------|
| A-6 | Policy Distribution Client Configuration, Mixed Mode..... | A-13 |
| A-7 | Java Security Module Configuration Parameters..... | A-17 |
| A-8 | Web Services Security Module Configuration Parameters..... | A-21 |
| A-9 | Web Services Security Module on WebLogic Configuration Parameters | A-23 |
| A-10 | RMI Security Module Configuration Parameters | A-25 |
| A-11 | WebLogic Server Security Module Configuration Parameters | A-26 |
| A-12 | WebLogic Server Discovery Mode Parameters | A-27 |
| A-13 | Web Services Proxy Client Configuration Parameters..... | A-28 |
| A-14 | PDP RMI Proxy Client Configuration Parameters..... | A-29 |
| A-15 | Policy Store Service Configuration Parameters..... | A-30 |
| B-1 | Configuration Roadmap | B-6 |
| B-2 | Configure Attributes to be Retrieved..... | B-7 |
| B-3 | LDAP Attribute Retriever Parameters | B-9 |
| B-4 | RDBMS Attribute Retriever Parameters..... | B-11 |

List of Figures

| | | |
|------|--|------|
| 1-1 | Components of Oracle Entitlements Server | 1-4 |
| 1-2 | Oracle Entitlements Server PAP Architecture | 1-4 |
| 1-3 | Application Acting as PEP Requests Decision from PDP | 1-6 |
| 1-4 | Agent Acting as PEP Intercepts Request and Makes Decision | 1-6 |
| 1-5 | Security Module as PDP and PEP | 1-7 |
| 1-6 | Security Module Architecture | 1-7 |
| 1-7 | How Data Flows in the Policy Authorization Process | 1-9 |
| 2-1 | Policy Components Mapped to Authorization Policy Objects | 2-2 |
| 2-2 | Policy Components Mapped to Role Mapping Policy Objects | 2-3 |
| 2-3 | Use Case for Software Components and Business Objects | 2-8 |
| 3-1 | The Authentication Provider Tab | 3-2 |
| 3-2 | SUFFICIENT Control Flag | 3-2 |
| 3-3 | DefaultAuthenticator Tab in WebLogic Server Console | 3-3 |
| 3-4 | OPSS Application Grants Display Screen | 3-5 |
| 3-5 | Administration Console Sign In Page | 3-6 |
| 3-6 | Administration Console Sign Out Link | 3-7 |
| 3-7 | Oracle Entitlements Server Administration Console | 3-7 |
| 3-8 | Authorization Management Tab | 3-8 |
| 3-9 | System Configuration Tab | 3-8 |
| 3-10 | Navigation Panel Browse Tab With Nodes Expanded | 3-9 |
| 3-11 | Navigation Panel Search Tab | 3-10 |
| 3-12 | The Home Tab | 3-11 |
| 4-1 | Add Default Roles Pop Up | 4-17 |
| 4-2 | OPSS Application Grants Display Screen | 4-20 |
| 4-3 | The Condition Builder | 4-34 |
| 4-4 | Operand Value Tabs | 4-34 |
| 4-5 | Adding a Literal to the Condition | 4-35 |
| 4-6 | Adding a Function | 4-37 |
| 5-1 | Pop-up Search Box | 5-2 |
| 5-2 | Simple Search Fields and Results Tab in Navigation Panel | 5-2 |
| 5-3 | Searching for Resource Types | 5-5 |
| 5-4 | Resource Type Search Results | 5-5 |
| 5-5 | Searching for Application Roles in a Role Catalog | 5-6 |
| 5-6 | Application Role Search Results | 5-6 |
| 5-7 | Searching for Role Mapping Policies | 5-7 |
| 5-8 | Role Mapping Policy Search Results | 5-7 |
| 5-9 | Searching for Resources | 5-8 |
| 5-10 | Searching for Entitlements | 5-8 |
| 5-11 | Searching Policies | 5-9 |
| 5-12 | Searching Polices by Target | 5-10 |
| 5-13 | Searching Polices by Principal | 5-10 |
| 5-14 | OPSS Application Grants Display Screen | 5-11 |
| 6-1 | Using Oracle Entitlements Server Policy Distribution Component | 6-3 |
| 6-2 | Using Security Module Policy Distribution Component | 6-4 |
| 7-1 | Embedded PDP Deployment | 7-2 |
| 7-2 | Remote PDP Deployment | 7-2 |
| 7-3 | Proxy Mode Deployment | 7-3 |
| 7-4 | XACML Gateway Deployment | 7-3 |
| 8-1 | SMConfig UI for Java Security Module | 8-3 |
| 9-1 | Adding Providers to the WebLogic Server Domain's Realm | 9-16 |
| 10-1 | Security Modules in Home Area | 10-2 |
| 10-2 | IDS Profiles in Home Area | 10-5 |
| 10-3 | Create Identity Store Profile Page | 10-5 |
| 11-1 | Edit Admin Role Pop Up Screen | 11-4 |

| | | |
|------|--|------|
| 13-1 | Policy Simulator User Interface in Simple Mode | 13-3 |
| 13-2 | Policy Simulator User Interface in Advanced Mode | 13-4 |
| 14-1 | Multi-Site Deployment Topology..... | 14-3 |
| 15-1 | Multi-Site Deployment Topology..... | 15-2 |

List of Examples

| | | |
|-------|---|-------|
| 9-1 | appSettings Section of Sharepoint web.config File | 9-8 |
| 9-2 | SafeControl Assembly Entries..... | 9-9 |
| 9-3 | add assembly Entry | 9-10 |
| 9-4 | add name Entry | 9-10 |
| 9-5 | PageParserPaths Entry | 9-10 |
| 9-6 | MOSS PortalSiteMapProvider..... | 9-10 |
| 9-7 | Oracle Entitlements Server PortalSiteMapProvider | 9-11 |
| 9-8 | Sample File Of Discovered Resources..... | 9-17 |
| 9-9 | Defining an EJB Resource in ejb-jar.xml | 9-19 |
| 9-10 | Defining a JNDI Resource in weblogic-ejb-jar.xml | 9-20 |
| 9-11 | Defining a JDBC Resource in config.xml | 9-25 |
| 9-12 | Initiating Authorization on JDBC Resource..... | 9-26 |
| 9-13 | Defining a JMS Queue Resource in config.xml..... | 9-27 |
| 9-14 | JMS Client Example | 9-28 |
| 9-15 | Web Application Configuration | 9-29 |
| 9-16 | Web Application Context Configuration | 9-30 |
| 9-17 | Web Service Configuration..... | 9-30 |
| 9-18 | Client Code For Accessing WSDL | 9-30 |
| 9-19 | Configuration of WebLogic Server Instance | 9-32 |
| 13-1 | XML to LDAP serviceInstances for Source and Destination Policy Stores | 13-14 |
| 13-2 | XML to LDAP serviceInstance for Bootstrap Credential | 13-14 |
| 13-3 | XML to LDAP jpsContext for Source and Destination Policy Stores | 13-14 |
| 13-4 | LDAP to XML serviceInstances for Source and Destination Policy Stores | 13-16 |
| 13-5 | LDAP to XML serviceInstance for Bootstrap Credential | 13-16 |
| 13-6 | LDAP to XML jpsContext for Source and Destination Policy Stores | 13-16 |
| 13-7 | XML to Database serviceInstances for Source and Destination Policy Stores | 13-18 |
| 13-8 | XML to Database serviceInstance for Bootstrap Credential | 13-18 |
| 13-9 | XML to Database jpsContext for Source and Destination Policy Stores | 13-18 |
| 13-10 | Database to XML serviceInstances for Source and Destination Policy Stores | 13-20 |
| 13-11 | Database to XML serviceInstance for Bootstrap Credential | 13-20 |
| 13-12 | Database to XML jpsContext for Source and Destination Policy Stores | 13-20 |
| 13-13 | XML To Configure Decision Caching..... | 13-22 |
| 13-14 | XML To Configure Attribute Caching..... | 13-23 |
| 13-15 | Default logging.properties Configuration File | 13-24 |
| 13-16 | Configuration for Administration Console Logging..... | 13-27 |
| 13-17 | Configuration for File Logging | 13-27 |
| 13-18 | DebugStore Sample Logging Output..... | 13-28 |
| 13-19 | Sample Output for Cache Configuration Parameters Search..... | 13-30 |
| 13-20 | Sample Output for Principal Search..... | 13-30 |
| 13-21 | Sample Output for Resource and Action Search..... | 13-31 |
| 13-22 | Sample Output for the Value of an Attribute Search..... | 13-31 |
| 13-23 | Sample Output for Authorization Decision Search | 13-31 |
| 13-24 | Sample Output for Obligation Value Search | 13-31 |
| 13-25 | Sample Output for Static Role Search | 13-32 |
| B-1 | Attribute Query Information Defined for LDAP Attribute Retriever..... | B-8 |
| B-2 | Attribute Query Information Defined for the RDBMS Attribute Retriever | B-8 |
| B-3 | Declaring the Predefined Attribute Retriever..... | B-8 |
| B-4 | Using the Predefined LDAP Attribute Retriever | B-10 |
| B-5 | Using the Predefined RDBMS Attribute Retriever with JDBC | B-12 |
| B-6 | Using the Predefined RDBMS Attribute Retriever with Data Source..... | B-12 |
| B-7 | Declaring the Predefined Attribute Retriever in jpsContext | B-14 |
| B-8 | Enabling an Attribute's Cache..... | B-14 |
| B-9 | Configuring LDAP Failover | B-14 |
| B-10 | Sample jps-config.xml File..... | B-15 |

| | | |
|------|---|------|
| B-11 | Declaring Custom Attribute Retriever Service Provider | B-20 |
| B-12 | Specifying Custom Attribute Retriever Type and Classnames..... | B-20 |
| B-13 | Declaring Custom Attribute Retriever Reference in jpsContext..... | B-21 |
| B-14 | Implementing Custom PIP Interface..... | B-21 |
| E-1 | Sample Script For Policy Creation..... | E-12 |

Preface

The *Oracle Fusion Middleware Administrator's Guide for Oracle Entitlements Server* provides information on system configuration administration and management of policy objects using the Oracle Entitlements Server Administration Console. Manual configuration using files is also covered.

Audience

The intended audience of this guide is security administrators.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

For more information, see the following documents:

- *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*
- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Quick Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Third-Party Application Server Guide for Oracle Identity and Access Management*

Conventions

The following text conventions are used in this document:

| Convention | Meaning |
|-------------------|--|
| boldface | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| <i>italic</i> | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| monospace | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

Introducing Oracle Entitlements Server

This chapter contains an overview of the features and architecture of Oracle Entitlements Server. It contains the following sections.

- Section 1.1, "About Access Control"
- Section 1.2, "Overview of Oracle Entitlements Server"
- Section 1.3, "Overview of the Oracle Entitlements Server Architecture"
- Section 1.4, "How Oracle Entitlements Server Processes Authorization Policies"
- Section 1.5, "About the Supported Access Control Standards"

1.1 About Access Control

Access control refers to a system used to grant or deny access to an enterprise's information, systems or resources. For the purposes of this documentation, the entity that is being protected is referred to as the protected *resource* while the entity to which access is granted or denied is referred to as the *subject* or *principal* (most often a real person). An *authorization policy* matches a subject with a set of *operations* that determine what the subject is allowed to see and do within the protected resource. The operations are dependent on the type of resource. For example, the operations attached to a text file (read, modify, delete) are different from those that can be attached to a banking application (view account, transfer money, modify profile).

Access control assures that only authorized subjects can access protected resources thus preventing the resources from unauthorized or inadvertent modification. Authorization of a subject typically occurs after authentication. In general, an access control system may comprise two types of authorization:

- Coarse grained authorization is perimeter authorization that uses technology principally focused on "keeping the bad guys out." Generally, it is performed by interceptors outside the application making the authorization call. It takes into account a URL and the policies regarding the subject requester.
- Fine grained authorization is more detailed, and primarily controlled by the application making the authorization call. It takes into account the URL of the protected resource and its configured policies as well as information that may include resource-specific or user-specific attributes and the context of the request. For example, granting an employee access to a portal during normal business hours and denying this access during the weekend hours would call for fine grained authorization.

Thus, an access control system must support a policy model that is easy to administer yet allows for complex sets of conditions under which access can be granted (or denied). Oracle Entitlements Server is a product that provides centralized policy

management with centralized *or* distributed access control enforcement for all types of resources including software components and application business objects.

1.2 Overview of Oracle Entitlements Server

Oracle Entitlements Server is a fine-grained authorization product that allows an organization to protect its resources by defining and managing policies that control access to, and usage of, these resources. Access privileges are defined in a policy by specifying who can do what to which resource, when it can be done, and how. The policy can enforce controls on all types of resources including software components (URLs, Java Server Pages, Enterprise JavaBeans, methods, servlets and the like used to construct an application) and business objects (representations of user accounts, personal profiles and contracts such as bank accounts in a banking application, patient records in a health care application, or anything used to define a business relationship).

Oracle Entitlements Server supports the creation of Role Mapping Policies and Authorization Policies. A *Role Mapping Policy* defines constraints regarding which users are assigned roles and can map Application Roles in the Policy Store to external groups in the Identity Store. This mapping allows users in external groups to access resources as specified by the Application Roles. The mapping is allowed to be many-to-many. An *Authorization Policy* defines access to the protected software components and business objects. The following sections contain information on the previous releases of Oracle Entitlements Server and the features developed for this release of Oracle Entitlements Server.

- [Section 1.2.1, "Understanding Oracle Entitlements Server Releases"](#)
- [Section 1.2.2, "Using the Authorization Policy Manager Console"](#)
- [Section 1.2.3, "Features of Oracle Entitlements Server 11gR2"](#)

1.2.1 Understanding Oracle Entitlements Server Releases

Oracle Entitlements Server 11g represents a consolidation of Oracle Platform Security Services with Oracle Entitlements Server 10g (formerly BEA AquaLogic Enterprise Security). While Oracle Platform Security Services (OPSS) is a Java Authentication and Authorization Services (JAAS) security provider that offers coarse-grained authorization, Oracle Entitlements Server 11g is an end-to-end enterprise solution that includes multiple technologies including Java Standard Edition (SE) and Enterprise Edition (EE), service-oriented architecture (SOA) and .NET. Oracle Entitlements Server 11g offers fine-grained authorization in which a context for the authorization request may be provided and access is granted or denied based on this. The Oracle Entitlements Server 11g architecture is based on the interaction model described in the core eXtensible Access Control Markup Language (XACML) specifications. See [Section 1.3, "Overview of the Oracle Entitlements Server Architecture"](#) for details.

1.2.2 Using the Authorization Policy Manager Console

Authorization Policy Manager is the administration console for Oracle Entitlements Server. For purposes of the Oracle Entitlements Server documentation set, *Authorization Policy Manager* and variations of the *Oracle Entitlements Server Administration Console* (Administration Console, Console and the like) may be used interchangeably. See [Chapter 3, "Getting Started"](#) for more information on the Administration Console.

Note: Oracle Entitlements Server is not meant to contain the functionality of the product released as Oracle Authorization Policy Manager product. When referred to in this documentation set, Authorization Policy Manager is simply the Administration Console.

1.2.3 Features of Oracle Entitlements Server 11gR2

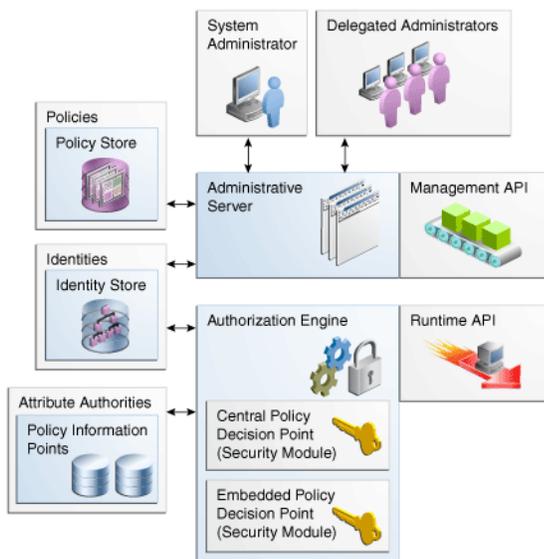
Oracle Entitlements Server 11gR2 offers fine-grained authorization and centralized entitlements management across heterogeneous application environments. Additionally, this release of Oracle Entitlements Server 11gR2 offers:

- Support for all data types and functions as defined in the XACML 3.0 specifications
- Support for viewing and modification of Oracle Platform Security Services created Application Grants (application policies)
- Logging enhancements to simplify policy evaluation analysis
- Policy Simulator
- Debugging enhancements
- Support for permission based advanced policies
- Enhanced PEP API query requests
- Administration Console support for plugging in multiple identity stores
- SMConfig UI, the Security Module configuration interface
- Support for .NET resources
- Security Modules for Java containers, Web Services (on WebLogic Server), Oracle Service Bus, Microsoft Sharepoint, JBoss, and Tomcat

1.3 Overview of the Oracle Entitlements Server Architecture

From a high-level, Oracle Entitlements Server (OES) comprises centralized policy management with centralized *or* distributed policy decision making. The architecture of Oracle Entitlements Server is based on the interaction model of entities discussed in the XACML specifications. This model defines entities that provide a flexible architecture that can adapt to many components and deployments. [Figure 1-1](#) illustrates the components of the Oracle Entitlements Server. Each of these components corresponds to one of the XACML entities.

Figure 1–1 Components of Oracle Entitlements Server



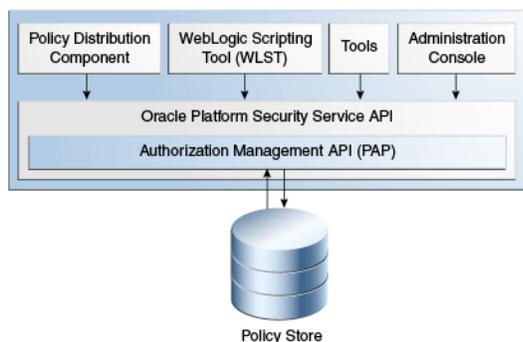
The following sections contain information on the Oracle Entitlements Server components and how they conform with the XACML entities.

- Section 1.3.1, "The Policy Administration Point"
- Section 1.3.2, "The Policy Decision Point and the Policy Enforcement Point"
- Section 1.3.3, "The Policy Information Point"

1.3.1 The Policy Administration Point

The Policy Administration Point (PAP) is where policies used to protect a specified protected resource are created and managed. The PAP makes these rules available to the Policy Decision Point in order for that entity to reach a *grant* or *deny* decision for a request to access the protected resource. The Oracle Entitlements Server PAP is comprised of the authorization management application programming interfaces (API). (In Figure 1–1, Administrative Server and Management API represent the PAP.) Access to (and use of) the PAP can be achieved with the Administration Console, the WebLogic Scripting Tool (WLST), the Policy Distribution Component or various other tools (including `migrateSecurityStore` and those for reassociation). Figure 1–2 illustrates the architecture.

Figure 1–2 Oracle Entitlements Server PAP Architecture



1.3.2 The Policy Decision Point and the Policy Enforcement Point

When Oracle Entitlements Server is deployed, a Policy Decision Point (PDP) receives a request for authorization, evaluates it based on applicable policies, reaches a decision and returns the decision to the Policy Enforcement Point (PEP), the entity which first made the authorization call. The PEP then enforces the decision.

Note: The PDP can retrieve additional subject, resource, action and environment attributes from a Policy Information Point to add context to the request. See [Section 1.3.3, "The Policy Information Point"](#) for more information.

The PEP doesn't intercept authorization requests; it intercepts a request for access sent to an application and authorizes the request by forming an authorization request and sending it to the PDP. Upon receipt, it enforces the *grant* or *deny* decision returned by the PDP. The PEP is a software component that can be the protected application itself or a Security Module.

Note: The PDP may also return information with the decision - referred to as an *obligation* - that allows the decision to be enforced within a particular context. The application is not forced to act upon these obligations. See [Chapter 2, "Understanding the Policy Model"](#) for more information.

Oracle Entitlements Server offers two types of Security Modules. One type was developed to act purely as a PDP by receiving requests and reaching decisions. The other type combines this PDP functionality with that of the PEP; thus, this Security Module type receives requests, reaches authorization decisions and enforces the decision. [Chapter 7, "Deploying the Policy Decision Point"](#) contains information on how the Security Module may be deployed. The following sections illustrate how the Security Modules work.

- [Section 1.3.2.1, "Security Module as PDP"](#)
- [Section 1.3.2.2, "Security Module as Combination PDP / PEP"](#)
- [Section 1.3.2.3, "Understanding the Types of Security Modules"](#)

Note: A Security Module is referred to as the *OES Client* before and during its installation process.

1.3.2.1 Security Module as PDP

When a Security Module acts purely as a PDP, its only functionality is decision making. It receives an authorization request and returns its decision to the PEP that originally made the authorization call. With the Security Module acting solely as the PDP, an external entity must act as the PEP - make the authorization call (using the Oracle Entitlements Server authorization API) and enforce the returned decision.

[Figure 1–3](#) illustrates the process when the PEP entity making the call is the resource (application) itself. It receives the request for access, initiates authorization (through communication with the Security Module) and enforces the returned decision.

Figure 1-3 Application Acting as PEP Requests Decision from PDP

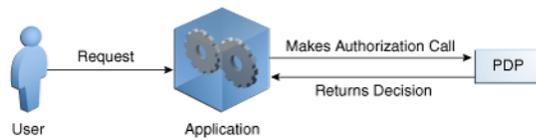
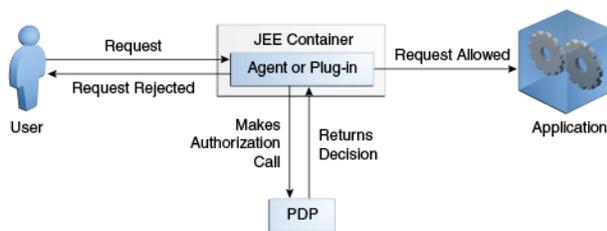


Figure 1-4 illustrates the process when the PEP entity is an agent or a plug-in (or similar software component) that intercepts the request before it reaches the application. The software component intercepts the request for access, initiates authorization (through communication with the Security Module) and forwards the decision returned from the Security Module to the application.

Figure 1-4 Agent Acting as PEP Intercepts Request and Makes Decision



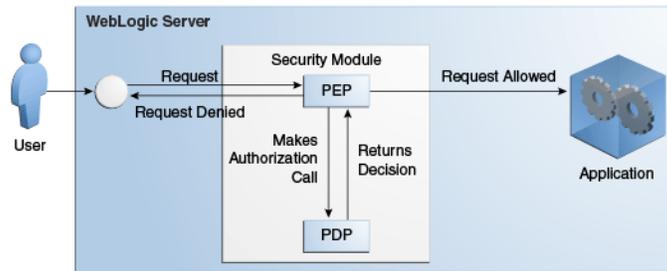
Working together, these scenarios can offer a flexible authorization service. For example, the intermediary Web Services/XML gateway can request an authorization decision for a subject to access a portal. Assuming this primary decision is granted, the Web Services/XML gateway itself can then request secondary authorization decisions used to personalize the portal for the user that has been granted access.

1.3.2.2 Security Module as Combination PDP / PEP

When a Security Module acts in tandem as a PDP and a PEP, it intercepts authorization requests, makes a decision, and enforces the decision. With this release of Oracle Entitlements Server, the WebLogic Server, Oracle Service Bus and Microsoft SharePoint Security Modules work in this manner.

For example, the WebLogic Server Security Module plugs directly into an Oracle WebLogic Server container that executes the protected application and will automatically request an authorization. In this scenario, a subject-initiated request to the application is intercepted by the WebLogic Server for authorization. The WebLogic Server, after successful authentication, attempts to authorize the request by making a call to a set of authorization providers configured during the Security Module's installation.

The Role Mapping and Authorization Proxy providers communicate with the Oracle Entitlements Server authorization engine (calling the PEP API which, in turn, calls the PDP). The PDP computes a decision and returns the decision to the PEP which returns an appropriate response to the WebLogic Server. (Optionally, the PDP may return an obligation with the decision.) If access is denied, the WebLogic Server throws a security exception and prevents access. If access is permitted, the WebLogic Server allows access. Figure 1-5 illustrates this scenario.

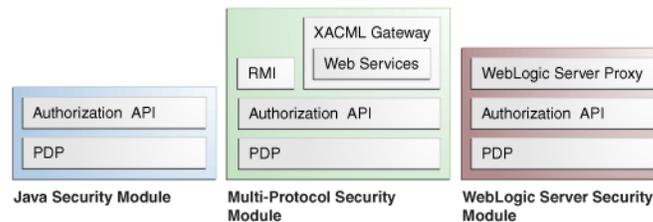
Figure 1–5 Security Module as PDP and PEP

The benefit of using the providers is fine-grained component level authorization. For example, you can use the providers to protect access to a servlet URL while allowing the servlet itself to make additional PEP API calls to decide which elements should be rendered on the returned page (as illustrated by [Figure 1–3, "Application Acting as PEP Requests Decision from PDP"](#)). By default, the Role Mapping and Authorization Proxy providers are not enabled.

Note: See [Section 9.4, "Securing WebLogic Server Resources"](#) for the procedure to enable the authorization providers using the WebLogic Server console. Post-configuration parameters are documented in [Section A.2.5, "WebLogic Server Security Module."](#)

1.3.2.3 Understanding the Types of Security Modules

[Figure 1–6](#) illustrates how the various types of Security Modules have been developed.

Figure 1–6 Security Module Architecture

Based on this topology, the services of a Security Module can be invoked in several ways.

- The Java Security Module is a generic PDP that provides authorization decisions using Java or .NET API. This Security Module is supported on the following containers:
 - Java, Standard Edition (JSE)
 - WebSphere
 - JBoss
 - Tomcat
 - Microsoft Sharepoint Server
- The Multi-Protocol Security Module is an authorization service (based on service-oriented architecture principles) wrapped around a generic Java Security

Module. It provides authorization decisions using RMI, Web Services and XACML (request and response). The Multi-Protocol Security Module can be co-located with the protected application or deployed on a central server.

Note: Figure 1–4, "Agent Acting as PEP Intercepts Request and Makes Decision" works similarly to the Multi-Protocol Security Module with an XML gateway; it intercepts requests and forces authorization before sending them to on to the destination.

- The WebLogic, Oracle Service Bus (OSB) and Sharepoint Security Modules are Security Modules that include both a PDP and a PEP. They can receive requests directly from the container without the need for explicit authorization API calls.

Caution: Security Modules deployed centrally are supported for RMI, Web Services or XACML calls but Oracle Entitlements Server and the Security Modules cannot be in the same WebLogic Server domain. For more information on the deployment models, see Chapter 7, "Deploying the Policy Decision Point."

See *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* for more information on requesting authorization decision and how Security Modules get updated policy information using the Policy Distribution Service. See Chapter 8, "Managing Security Module Configurations" and Chapter 9, "Securing Environment Specific Resources" for details on configuring and using Security Modules.

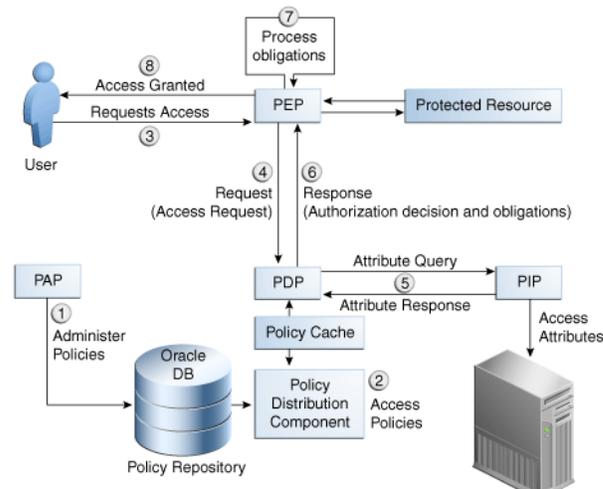
1.3.3 The Policy Information Point

The Policy Information Point (PIP) is a data repository - a source from which information can be retrieved for use when evaluating policies for an authorization decision. This allows policies to be data-driven in that the value of an attribute can impact the access decision. For example, if access to transfer money from a bank account is based on how much money is currently in the account, an attribute retriever can be used to get a value for the current balance.

In an Oracle Entitlements Server deployment, *attribute retrievers* serve the PIP thus, the terms PIP and attribute retriever may be used interchangeably in this documentation. The Attribute Authorities component illustrated in Figure 1–1, "Components of Oracle Entitlements Server" would be considered the PIP. Out of the box, an attribute retriever is available for both, LDAP and relational database data sources. See *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* and Appendix B, "Configuring Attribute Retrievers" for more information on attribute retrievers.

1.4 How Oracle Entitlements Server Processes Authorization Policies

The Oracle Entitlements Server authorization process involves the components described in Section 1.3, "Overview of the Oracle Entitlements Server Architecture". When a policy decision is requested, the PDP evaluates all policies related to the request and returns a *grant* or *deny* decision to the calling application. Figure 1–7 illustrates how the data flows during the policy authorization process.

Figure 1–7 How Data Flows in the Policy Authorization Process

1. Oracle Entitlements Server (acting as a PAP) is used to create and manage policies to protect a particular resource.
2. Policies in the policy repository are pushed to a policy cache, local to the PDP, by the Policy Distribution Service. The PDP reads policies from this cache. See *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* for more information.
3. A request for a resource is received by the PEP protecting it. The PEP can be the application itself or a Security Module - whichever makes the authorization call to Oracle Entitlements Server.
4. The PEP makes an authorization call to the PDP.
5. The Security Module PDP queries for additional subject, resource, action and environment attributes from the appropriate data source PIP.
6. The Security Module PDP evaluates the request and returns a response (and applicable obligations) to the PEP in the form of an authorization decision to grant or deny access.
7. The PEP fulfills any obligations, if applicable. An *obligation* is information returned with the decision upon which the PEP may or may not act. For example, an obligation may contain additional information concerning a decision to deny. The PEP entity is responsible for obligation fulfillment based on its settings. Oracle Entitlements Server is only responsible for forwarding the obligation based on policy configuration.
8. If access is permitted, the PEP grants the requester access to the resource; otherwise, access is denied.

Section 2.2, "How Oracle Entitlements Server Evaluates Policies" contains more details.

1.5 About the Supported Access Control Standards

Oracle Entitlements Server supports a number of access control models. Many access control products support only one of these models but Oracle Entitlements Server has implemented a policy model with the flexibility to support many of them. You can deploy strictly based on one model or mix and match pieces of different models. The following sections contain information on the access control models.

- Section 1.5.1, "Role-based Access Control (RBAC)."
- Section 1.5.2, "Attribute-Based Access Control (ABAC)."
- Section 1.5.3, "Java Permissions."
- Section 1.5.4, "XACML"
- Section 1.5.5, "PEP API"

1.5.1 Role-based Access Control (RBAC)

The Role-Based Access Control (RBAC) authorization model uses *roles* to define the privileges of a user. First, roles are created. Following, *permissions* to perform certain operations are assigned to the roles and, finally, *users* or *external groups* are assigned to the roles. Through role assignment, the assignee acquires the right to perform the assigned operations. Thus, RBAC makes management of individual permissions simply a matter of assigning the appropriate roles to the appropriate entity. Roles can also be combined in a hierarchy where higher-level roles subsume permissions owned by sub-roles. This model is useful for more coarse-grain authorization; for example, when your authorization requirements are not complex. Application Roles are used for modeling Oracle Entitlements Server deployments based on RBAC.

1.5.2 Attribute-Based Access Control (ABAC)

Attribute-Based Access Control (ABAC) provides the capability to define fine grained authorization using attributes. Roles need not be created. An ABAC policy specifies one or more *claims* that need to be satisfied before a user is granted access; for example, the user must be a certain age. If the user can prove this claim, access is granted. Conditions are used when modeling Oracle Entitlements Server deployments based on ABAC. For more information, see [Section 4.6, "Using the Condition Builder."](#)

1.5.3 Java Permissions

Oracle Entitlements Server is built as an extension of Oracle Platform Security Services (OPSS). The OPSS security model is based on Java Authentication and Authorization Service (JAAS) security. JAAS institutes a permission based authorization system that implements Java-based security standards to support principal based and code based policies. A Java `Permission` object represents permission to access a resource. For example, the following code creates a `FilePermission` object representing read access to a file named `abc` in the `/tmp` directory.

```
perm = new java.io.FilePermission("/tmp/abc", "read");
```

Oracle Entitlements Server supports the Java Development Kit developer version 1.6 on either the Standard Edition or Enterprise Edition platforms. For more information, see the Java documentation at

<http://www.oracle.com/technetwork/indexes/documentation/index.html>.

1.5.4 XACML

The eXtensible Access Control Markup Language (XACML) is an access control model that describes how to interpret policies, and an access control policy language (written using XML). Oracle Entitlements Server implements the XACML request and response standard as well as the architecture model (described in [Section 1.3, "Overview of the Oracle Entitlements Server Architecture."](#)) It also implements how XACML defines policies as a collection of principals, resources, actions and attributes. For more

information, see the XACML specifications at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

Note: Only support for XACML 3.0 data types and functions has been added to this release of Oracle Entitlements Server.

1.5.5 PEP API

Oracle Entitlements Server has implemented the PEP API, a part of the Open Az framework (<http://www.openliberty.org>). The `org.openliberty.openaz.azapi` package provides access from a PEP to a remote or embedded PDP. The `org.openliberty.openaz.azapi.pep` package (PEP API) has been implemented by Oracle Entitlements Server to be used by the PEP to issue authorization requests to a PDP. More information on the Open Az API can be found at <http://openaz.sourceforge.net>. More information on the PEP API implementation can be found in *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

Note: As implemented by Oracle Entitlements Server, the PEP API do not support authorization decisions for resources protected by Java permissions.

Understanding the Policy Model

A *policy* is a set of criteria that, when evaluated by Oracle Entitlements Server, specifies whether a user will be granted access to a particular protected resource or assignment to a particular role. This chapter contains an overview of the Oracle Entitlements Server policy model, the elements that comprise a policy and how the elements are organized in the policy store. It contains the following sections.

- [Section 2.1, "Understanding Oracle Entitlements Server Policies"](#)
- [Section 2.2, "How Oracle Entitlements Server Evaluates Policies"](#)
- [Section 2.3, "The Policy Object Glossary"](#)
- [Section 2.4, "Implementing a Policy Use Case"](#)

2.1 Understanding Oracle Entitlements Server Policies

Oracle Entitlements Server supports the creation of the following types of policies. The referenced sections contain detailed information regarding these policy types including how they are used.

- An *Authorization Policy* defines the criteria that control access to an organization's protected resources. See [Section 2.1.1, "Understanding the Authorization Policy."](#)

Note: Resources may include software components or business objects. For more information, see [Section 2.4, "Implementing a Policy Use Case."](#)

- A *Role Mapping Policy* defines the criteria that control how external users, groups or roles are granted or denied membership to roles created using Oracle Entitlements Server. See [Section 2.1.2, "Understanding Role Assignments and the Role Mapping Policy."](#)

2.1.1 Understanding the Authorization Policy

An *Authorization Policy* is created to grant or deny access to a particular resource based on the profile of the requesting user. From a high level, the Authorization Policy defines an association between an effect (GRANT or DENY), a principal (requesting user), the target resource, the resource's allowed actions and an optional condition. An Authorization Policy is applicable to a request for access if the parameters in the request match those specified in the policy. Consider this Authorization Policy definition:

```
GRANT the SupportManagerEast role MODIFY access to the Incidents servlet
```

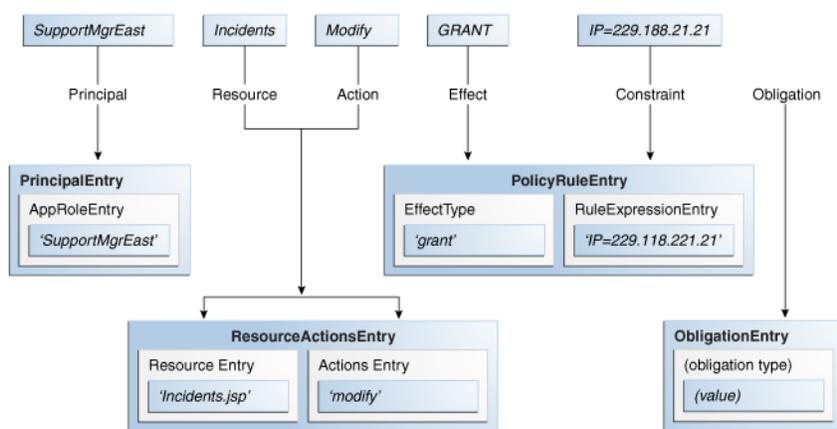
if the request is made from an IP address of 229.188.21.21

This Authorization Policy will GRANT any user that is a member of the SupportManagerEast role access to the Incidents servlet for the purpose of modifying it. The policy is also constrained by an optional condition - the request must be made from IP address 229.188.21.21. Thus, if the parameters in the request match the parameters in the policy (a member of the SupportManagerEast role wants to modify the Incidents servlet), and the request is made from IP address 229.188.21.21, the request is granted. If the parameters in the request match the parameters in the policy (a member of the SupportManagerEast role wants to modify the Incidents servlet) but the request is NOT made from IP address 229.188.21.21, the policy is ignored. The following list of terms and values are extracted from this policy definition and comprise the components of the Authorization Policy.

- Effect: GRANT
- Action: MODIFY
- Resource: Incidents servlet
- Principal: member of SupportManagerEast role
- Condition/Constraint: IP address 229.188.21.21

Figure 2–1 illustrates how the components of this policy map to the Oracle Entitlements Server Authorization Policy objects.

Figure 2–1 Policy Components Mapped to Authorization Policy Objects



For information on how to create, update and delete Authorization Policies, see Section 4.5.5, "Managing Authorization Policies."

2.1.2 Understanding Role Assignments and the Role Mapping Policy

An *Application Role* is a collection of users, groups, or other Application Roles; it is defined using Oracle Entitlements Server and stored in the policy store. It can be mapped to a user, group, or external role in an identity store, or another Application Role in the Oracle Entitlements Server policy store.

Note: Assigning one Application Role to another Application Role allows you to build an Application Role hierarchy.

Application Roles can be assigned to a user in either of the following ways:

- By statically granting a specific user membership in the role.
- By referencing the Application Role in a *Role Mapping Policy* that will be used to dynamically assign role membership at runtime.

A Role Mapping Policy allows you to dynamically assign (GRANT) role membership to a user or dynamically revoke (DENY) role membership from a user. Consider the following Role Mapping Policy definition:

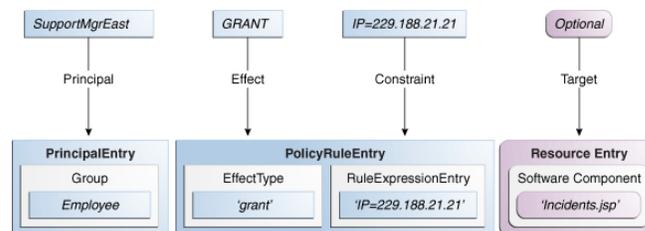
```
GRANT the Employee group application role SupportManagerEast
    if the request is made from an IP address of 229.188.21.21
```

This policy grants the `SupportManagerEast` Application Role to any user that is a member of the group `Employee`. It is also constrained by an optional condition - the request must be made from IP address `229.188.21.21`. Thus, if the parameters in the request match the parameters in the Role Mapping Policy (the requesting user is a member of the `Employee` group), and the request is made from IP address `229.188.21.21`, the Application Role is granted. If the request is not made from the defined IP address, the Role Mapping Policy is ignored. The target is also an optional addition to a Role Mapping Policy. The following terms and values are applicable to this Role Mapping Policy definition.

- Effect: GRANT
- Application Role: SupportManagerEast
- Principal: member of Employee group
- Condition/Constraint: IP address 229.188.21.21

If a Resource or Resource Name Expression is defined as a Target for a Role Mapping Policy, the Role Mapping Policy will only be applied if it matches the resource defined in the request. [Figure 2–2](#) illustrates how the components of this example policy might map to Oracle Entitlements Server Role Mapping Policy objects.

Figure 2–2 Policy Components Mapped to Role Mapping Policy Objects



A Role Mapping Policy can also be used to prevent specific users from being assigned an Application Role. Consider the following Role Mapping Policy definition:

```
DENY the Customers group the application role GoldCircle
    if the account balance is less then $10,000
```

This policy denies the `GoldCircle` Application Role to any members of the group `Customers` IF their account balance is less than \$10,000. For information on how to create, update and delete Role Mapping Policies, see [Section 4.5.7, "Managing Role Mapping Policies."](#)

2.2 How Oracle Entitlements Server Evaluates Policies

During Oracle Entitlements Server runtime evaluation, the following occurs:

1. Based on the subject, a list of Application Roles is determined by:
 - a. Retrieving the user's static role membership.
 - b. Evaluating all applicable Role Mapping Policies with a GRANT effect and adding them to the list of roles previously determined.
 - c. Evaluating all applicable Role Mapping Policies with a DENY effect and removing them from the list of roles previously determined.
2. Based on the subject and list of retrieved Application Roles, a list of Authorization Policies is evaluated to find any that might be applicable based on the grantee, target matching and conditions. (The actions allowed on the resource are defined by the Authorization Policy.)
3. A final authorization decision is based on the "DENY overrides" combining algorithm and returned to the calling application.

[Section 1.4, "How Oracle Entitlements Server Processes Authorization Policies"](#) contains additional details on this process.

2.3 The Policy Object Glossary

The policy objects defined in this section can be created, provisioned or managed using the Authorization Policy Manager Administration Console.

■ Application

An Application is a high-level container for managing roles, policies, resource definitions, and other policy objects; in effect, all items needed to define secure access to a particular resource. An Application may correspond to a single deployed software application, a set of deployed software applications, or components of a software application (such as an Enterprise Java Bean). You can manage more than one Application with Oracle Entitlements Server. For more information, see [Section 4.5.1, "Managing Applications."](#)

■ Application Role

An Application Role defines criteria for mapping users, groups, External Roles or other Application Roles to a particular Oracle Entitlements Server Application object. The Application Role can be granted to an external user, group, or role in an identity store, or another Application Role in the policy store. When creating an Application Role (in a Role Catalog) you might grant it all privileges necessary to access a given target Resource. Then, the Application Role can be assigned statically by explicitly granting membership to it, or the Application Role can be assigned dynamically by referencing it as the subject in a Role Mapping Policy. One target Application may have several different Application Roles, with each one assigned a different set of privileges offering more fine-grained access.

One External Role can be mapped to many Application Roles. For example, the External Role `employee` (stored in LDAP-based identity store) can be mapped to the Application Role `customersupport member` (defined in one Application) and to the Application Role `IT member` (defined in another Application). A Role Catalog is the container in which Application Roles are kept. For more information, see [Section 4.5.6, "Managing Application Roles in the Role Catalog."](#)

Note: An Application's Role Catalog provides the means to organize Application Roles. Search for Application Roles in the Role Catalog node of the Oracle Entitlements Server Administration Console. See [Chapter 5, "Querying Security Objects"](#) for more information.

- **Attribute**

An Attribute represents data that can be used in a policy condition, or returned with the policy determination as an obligation. It can be a built-in attribute (where its value is always defined - as in current time or current user), a Resource attribute (which is associated with, and managed within, a configured Oracle Entitlements Server Resource) or a Dynamic attribute. An attribute is defined by its name, the type of data it takes as a value, and whether the value is single or multiple. An attribute value can either be passed by the protected application as part of an authorization request, or retrieved by Oracle Entitlements Server using an attribute retriever. For more information, see [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#)

- **Authorization Policy**

An Authorization Policy specifies a set of rights that an entity (the grantee, a principal or code source) is allowed on a protected resource. This might include viewing a web page or modifying a report. In short, it specifies who can do what to a resource protected by Oracle Entitlements Server. For more information, see [Section 4.5.5, "Managing Authorization Policies."](#)

Note: Search for Authorization Policies in the Default Policy Domain node (or a custom Policy Domain node, if applicable) of a configured Application. See [Chapter 5, "Querying Security Objects"](#) for more information.

- **Condition**

A Condition is one or more boolean expressions that must evaluate to true in order for the policy to be included in the authorization decision. Adding a Condition to a policy is optional and when used, further restricts access to the protected resource. In general, a condition's boolean expression tests the value of some user, resource, or system attribute. Individual conditions can be combined with the following logical operators: AND, OR, and NOT. Conditions can define constraints based on date, time, a time range, a day of week, and so forth. For more information, see [Section 4.6, "Using the Condition Builder."](#)

- **Entitlement**

An Entitlement (also known as a *permission set*) represents a small set of Resources and the associated actions needed to perform a task. It groups related Resources, possibly of different types, needed to perform a business function. An Entitlement is a reusable collection of access rights that can be granted to multiple principals. For more information, see [Section 4.5.4, "Managing Entitlements."](#)

- **External Role**

An External Role is defined in an external identity store such as an LDAP server or a database. The term *external role* is often synonymous with the terms *enterprise role* or *enterprise group*; they are typically implemented as LDAP groups in the identity store. For information on adding an External Role to a policy, see [Section 4.5.5.1,](#)

"Creating an Authorization Policy" or Section 4.5.7.1, "Creating a Role Mapping Policy."

Note: Within Oracle Entitlements Server, external roles and users are read-only. They are managed with a different tool, such as Oracle Identity Manager. For more information, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

- **Function**

A Function represents code that can be invoked as part of the evaluation of a policy condition; the returned value will affect the evaluation of the condition. You can extend the functions supplied with Oracle Entitlements Server by creating additional, custom ones. For more information, see [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#)

- **Obligation**

An Obligation specifies optional information that is to be returned with a GRANT or DENY authorization decision. When used in a policy, an Obligation may impose an additional requirement for the policy enforcing component, or simply request useful information. For example, the reason a request for access has been denied might be returned as an Obligation. For information on adding an Obligation to a policy, see [Section 4.5.5.1, "Creating an Authorization Policy."](#)

- **Policy Domain**

A Policy Domain is a container under an Application object that can serve as a partition to facilitate management of Resources, Entitlements and Authorization Policies. The Policy Domain is an optional management construct that can restrict an administrator's right to a particular subset of Resource, Entitlements, and Authorization Policies. The Policy Domain has no effect upon runtime policy evaluation. Multiple Policy Domains can be created and can be hierarchical. A *default policy domain* is added to each Application upon its creation. For more information, see [Section 11.4, "Using Policy Domains to Delegate."](#)

- **Policy Store**

The Policy Store is where all Oracle Entitlements Server policy objects (including, but not limited to, Applications, Resources and various role types) are stored. A Policy Store can be a relational database (preferred) or an LDAP-based directory. For more information, see [Section 3.2.3, "Accessing the Policy Store."](#)

- **Principal**

A Principal is the identity to which the access rights defined in a policy are granted. A principal can be a user, a group, an External Role, or an Application Role. Most frequently, it is an Application Role. For information on adding a principal to an Oracle Entitlements Server policy, see [Section 4.5.5.1, "Creating an Authorization Policy"](#) or [Section 4.5.7.1, "Creating a Role Mapping Policy."](#)

- **Resource**

A Resource is a protected component or object to which access is granted or denied. A Resource represents the application component or business object that is secured by an Authorization Policy. At runtime, the application passes the Resource name to check for access definitions that will determine whether a Principal is authorized access. A Resource requires an associated Resource Type. For more information, see [Section 4.5.3, "Managing Resources."](#)

- **Resource Type**

A Resource Type represents the type of a secured object. Protected software application components that share common characteristics can be represented by particular Resource Type. For example, a set of pages can be represented by one Resource Type and bank accounts by another Resource Type. A Resource Type defines eligible *resource attributes* and possible valid actions that are applicable to the protected component. For more information, see [Section 4.5.2, "Managing Resource Types."](#)

- **Role Category**

A Role Category is an optional tag that can be associated with an Application Role; it can be used for searching. Role Categories allow administrators to organize roles in arbitrary flat collections. They have no effect upon runtime policy evaluation. For more information, see [Section 4.5.8, "Managing a Role Category."](#)

- **Role Mapping Policy**

A Role Mapping Policy is used to determine what external subjects (users, groups or External Roles) are assigned to the applicable Application Role. The Application Role, when referenced in an Authorization Policy, defines the principals affected by the Authorization Policy. Role Mapping Policies may also include conditions. For more information, see [Section 4.5.7, "Managing Role Mapping Policies."](#)

Note: Search for Role Mapping Policies under the Role Catalog node of the Oracle Entitlements Server Administration Console. See [Chapter 5, "Querying Security Objects"](#) for more information.

2.4 Implementing a Policy Use Case

Oracle Entitlements Server provides the ability to externalize policy management and policy decision making logic from an organization's resources. It secures access to the organization's resources by implementing policies that specify the users, groups, and roles that can access them. Resources can be application software components (URLs, Enterprise JavaBeans, JavaServer Pages) or enterprise business objects (customer accounts, patient records). This use case considers how the policy model can be used to secure the financial services offered by Acme Investment Bank. It is based on the concept of *hierarchical resources*; namely, that resources are organized as a tree and inherit from their parent elements.

Note: Oracle Entitlements Server also supports the concept of non-hierarchical (flat) resources. See [Section 4.5.2, "Managing Resource Types"](#) for more information.

In this use case, the following conditions apply:

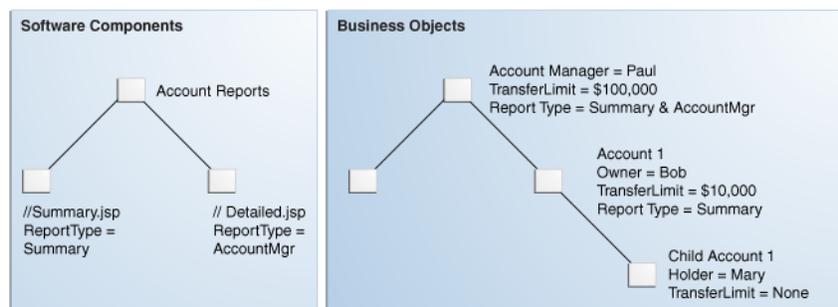
- A customer may open a family account and is considered an owner of the account.
- The customer may open a child account for family members and set transfer limits for each member. Transfer limits must be lower than the customer's own transfer limit.
- Each account has a bank employee that acts as an account manager and sets the transfer limits for the account.

- Both a Summary report and an Account Manager report are associated with each family account.

Figure 2–3 illustrates the financial services scenario by organizing the protected resources into business objects and software components. Paul is a bank employee who is an account manager and can set transfer limits up to \$100,000 on the accounts that he manages. Paul manages account owner Bob's family account which has a transfer limit of \$10,000. Bob manages his family account and a child account he created for Mary who may not transfer money. These accounts are considered business objects and are protected as such.

Account owner Bob has access to a Summary report generated for his family account. Account manager Paul has access to Bob's Summary report and his own Account Manager report. Child account holder Mary has access to no reports. These reports, generated as JavaServer Pages, are considered software components and are protected as such.

Figure 2–3 Use Case for Software Components and Business Objects



For any given user, a request for access to a financial services account (business object) or account report (software component) generates a decision based on the following questions:

1. Is this user an account holder, account owner or an account manager?
2. Can this user transfer funds from this account (subject to the role, transfer limit, and time of transaction)?
3. What reports can this user access?

The first two questions can be decided using policies created to protect business objects, while the last can be decided using policies created to protect software components. The following sections illustrate how to conceptualize the policies.

- Section 2.4.1, "Protecting Software Components"
- Section 2.4.2, "Protecting Business Objects"

2.4.1 Protecting Software Components

The Account Reports node in Figure 2–3, "Use Case for Software Components and Business Objects" represents the reporting application. `Summary.jsp` and `Detailed.jsp` are the software components. There are several options from which to choose when deciding how to model policies for securing these software components. One option is to set an Authorization Policy for the top node reporting application by using group membership. The following example illustrates how access is explicitly granted by naming the resource and the group of users that can access it.

```
GRANT the BankManagers group access to the AccountReports node
```

This top down Authorization Policy grants access to the Account Reports node for anyone in the BankManagers group. Because these resources are hierarchical, anyone in the allowed group has access to both the Summary and Detailed reports. But this access may be restricted using system-based or attribute-based conditions. For example, adding a condition based on time or based on the value of a specific user, group, or resource attribute would further limit access. The following example illustrates how a time-based condition restricts access of the reports to typical office hours.

```
GRANT the BankManagers group access to the AccountReports node
  IF the request is made between 09:00 and 17:00
```

Another option can set the top down Authorization Policy by defining the principal as a role rather than a group. A role is comprised of users or groups. (An LDAP role would be granted enterprise wide whereas an Application Role is specific to the Application for which it was configured.)

Note: A user can be assigned to a role through membership or a Role Mapping Policy as discussed in [Section 2.1, "Understanding Oracle Entitlements Server Policies."](#)

In the following example, the resource is explicitly named and access is implicitly granted to a user if the user is assigned the defined role.

```
GRANT access to AccountReports node if user has BankManagers role
```

You can also dynamically assign the BankManagers role to users accessing the reporting application if they are a member of the BankManagers group (as illustrated below).

```
GRANT BankManagers role to members of BankManagers group
  FOR access to AccountReports node
```

Another way to define the previous Authorization Policy is to assign the role based on a user attribute value rather than group membership. (In a large enterprise, it is typically more efficient to assign users based on attributes than on group membership.) The following example assigns the BankManagers role to the requesting user if the value of the UserType attribute in the user's profile is BankManager.

```
GRANT BankManagers role to anyone defined by UserType 'BankManager'
  FOR access to the AccountReports node
```

The previous examples represent Authorization Policies that scope from the top node reporting application down to the reports but Authorization Policies can also be defined for the specific report nodes. The following example grants access to the Summary.jsp report to all assignees of the BankManagers and AccountOwners roles. The additional condition is that the principal requesting access must be listed on the account to which the report pertains.

```
GRANT Summary.jsp access to all members of BankManagers and AccountOwners role
  IF the requesting assignee is listed as OWNER or MANAGER on specified account
```

Another example illustrates how access to the Detailed.jsp report can be granted to anyone who is assigned the BankManager role.

```
GRANT Detailed.jsp access to all assignees of BankManagers role
```

The previous examples show how an Authorization Policy can be modeled for specific application software components. In a real enterprise scenario, each application may have tens or hundreds of resources so it might not be practical to write an Authorization Policy for each one. The concept of *resource attributes* has been implemented by Oracle Entitlements Server to address this proliferation of application software component resources and associated Authorization Policies.

By associating a resource with an attribute, you can grant access based on the value of the attribute. For example, *filetype* could be a resource attribute that is used to define an HTML page, an image, or a PDF. By defining a condition as `if filetype=pdf`, you can grant access to all PDF files that are associated with the resource. The following example uses a resource attribute; it allows users assigned the BankManagers and AccountOwners role access to all reports although access is granted only if the report type being requested matches the value of the UserReportType attribute in the specific user's profile.

```
GRANT users assigned BankManagers or AccountOwners roles
    access to AccountReports
    IF requested ReportType matches UserReportType attribute value
        in user profile
```

This policy grants BankManagers and AccountOwners access to all reports although access is constrained based on matching resource attribute values with user attribute values. An advantage of this approach is that the policy governing access need not change as resources are added to, or removed from, an application. As resources change, the ReportType resource attribute attached to the application continues to govern access.

2.4.2 Protecting Business Objects

There are several options from which to choose when deciding how to model Authorization Policies for securing business objects. In this banking scenario, business objects are bank accounts. [Figure 2–3, "Use Case for Software Components and Business Objects"](#) illustrates the Acme bank account structure.

Each bank account can have a manager, an owner, and a holder with each *scope* assigned a certain set of privileges (or *entitlements*). The policy evaluating what a user can do on the bank account is then based on the user's attributes rather than the resource. The following example allows anyone to transfer money but that privilege is only granted if the user is defined as owner of the account requested and the amount of money being transferred is less than or equal to the limit defined for the user.

```
GRANT anyone transfer privileges only
    IF the user is listed as OWNER on specified account
    AND transfer amount is equal to or less than the transfer limit
```

There is another option to acquire a user's entitlements. Rather than comparing a transfer request to a transfer limit, Oracle Entitlements Server can return the transfer limit amount as the output of evaluation. In this scenario, the user's ability to access the account is verified but the transfer amount is returned to the caller (in a Java object) as an *obligation*. This leaves verification that the transfer amount is within the transfer limit up to the application. The following example illustrates this model.

```
GRANT anyone transfer privileges only
    IF the user is listed as OWNER on specified account
    THEN RETURN transfer limit to calling application
```

A model where the bank account corresponds to an individual resource instance can also be used; however, this would yield a proliferation of policies (one for each account) and become unmanageable. For example, if Acme Investment Bank had 100,000 accounts, it would need at least 100,000 policies just to manage transfers. For more information on adding obligations, see [Section 4.5.5, "Managing Authorization Policies."](#)

Getting Started

This chapter describes how to get started using Oracle Entitlements Server, including information about how to use and navigate the graphical interface. It contains the following sections.

- Section 3.1, "Before You Begin"
- Section 3.2, "Understanding The Graphical Interface"
- Section 3.3, "Accessing the Administration Console"
- Section 3.4, "Navigating the Administration Console"
- Section 3.5, "Upgrading from Oracle Entitlements Server Basic"
- Section 3.6, "Accessing Oracle Entitlements Server Examples"

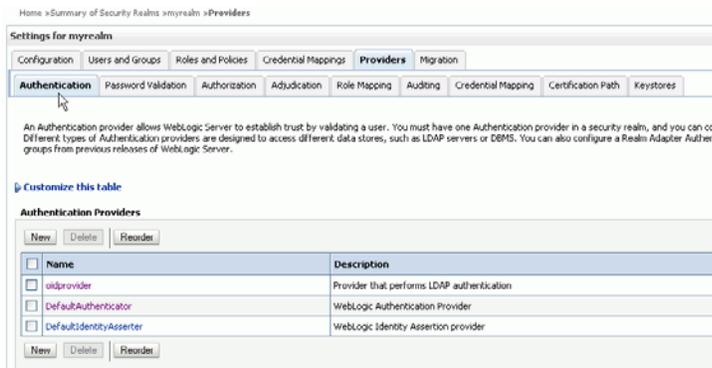
3.1 Before You Begin

Before getting started using Oracle Entitlements Server, the following tasks must be done. They include installing the product and its components (for example, remote Security Modules), and configuring features like high availability and Secure Sockets Layer (SSL), if applicable. After finishing with these tasks, you can begin with [Section 3.2, "Understanding The Graphical Interface."](#)

- Install and configure Oracle Entitlements Server according to the instructions in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
 - The policy store managed by Oracle Entitlements Server must be a relational database.
 - The identity store associated with Oracle Entitlements Server must be an LDAP-based directory.
- After installation, the Oracle Entitlements Server identity store is associated with the WebLogic Server embedded LDAP directory. While this embedded LDAP directory is fine for development purposes, a supported LDAP directory must be used in production. The following procedure reconfigures the default identity store settings. More specific information on configuring LDAP authentication providers can be found in the *Oracle Fusion Middleware Securing Oracle WebLogic Server*.
 1. Launch the WebLogic Server console.
 2. Click Security Realms.
 3. Click the settings for *myrealm*.

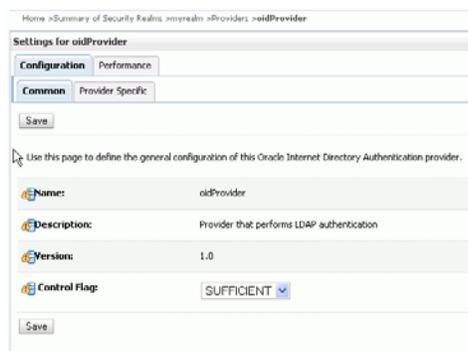
4. Click the Provider tab.
5. Click the Authentication tab as displayed in Figure 3–1.

Figure 3–1 The Authentication Provider Tab



6. Click the New button to create a new provider.
7. Enter a name and select the type of LDAP-based directory.
For example, *OracleInternetDirectoryAuthenticator*.
8. Configure the provider-specific attributes of the LDAP-based directory.
This might include the host name and port, credentials, group search base, user search base and the like.
9. Save the provider information.
10. Change the order of the providers so that the LDAP-based directory is first.
11. Click the new provider name to configure it.
 - a. Click the Configuration tab.
 - b. Click the Common tab.
 - c. Set the Control Flag to SUFFICIENT and click Save as displayed in Figure 3–2.

Figure 3–2 SUFFICIENT Control Flag



- d. Click the Provider Specific tab.

- e. Enter the LDAP configuration information for your identity store and click Save.
12. Return to the Providers tab.
13. Click **DefaultAuthenticator** to change its configuration.
14. Set the Control Flag to SUFFICIENT and click Save as displayed in Figure 3–3.

Figure 3–3 DefaultAuthenticator Tab in WebLogic Server Console



15. Restart WebLogic Server.
 - For information about configuring high availability for Oracle Entitlements Server, see *Oracle Fusion Middleware High Availability Guide*
 - For information regarding the authentication of users, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

Note: Oracle Entitlements Server is not involved in the authentication of users. This is normally done as part of the WebLogic Server security realm configuration.

- For information about configuring one-way SSL for connections that Oracle Entitlements Server establishes with the policy store, the identity store, and the database, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*. Access to Oracle Entitlements Server using 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.
- Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information.
 - The system requirements document covers information such as hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches:
<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html>
 - The certification document covers supported installation types, platforms, operating systems, databases, JDKs, and third-party products:
<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html>

These documents are available on Oracle Technology Network (OTN).

3.2 Understanding The Graphical Interface

Oracle Authorization Policy Manager is a sub-component of Oracle Entitlements Server that is the graphical management tool for administrators. It is a browser-based interface for managing policies and related policy objects. The following sections contain information to help understand the Authorization Policy Manager Administration Console.

- [Section 3.2.1, "Assigning Oracle Entitlements Server Administrators"](#)
- [Section 3.2.2, "Using the Identity Store"](#)
- [Section 3.2.3, "Accessing the Policy Store"](#)
- [Section 3.2.4, "Displaying Oracle Platform Security Services Application Grants"](#)

3.2.1 Assigning Oracle Entitlements Server Administrators

Only users with sufficient privileges can log in to the Oracle Entitlements Server Administration Console or use administrative command-line tools such as the WebLogic Scripting Tool (WLST). An Oracle Entitlements Server system-level Administrator Role named `SystemAdmin` is created during installation and is mapped to the WebLogic Server administrator user (`weblogic`). The password is set during installation. `SystemAdmin` has extensive privileges that includes the rights to create additional Administrative Roles and delegating administrative rights to others.

Note: At first log in to the Oracle Entitlements Server Administration Console, `SystemAdmin` must use the credentials set during installation. The identifier and password can be changed by using your identity store's management tool.

You can create separate administrative users with different access rights for administering Oracle Entitlements Server and your environment. For more information, see [Section 11.6, "Managing System Administrators Using Administrator Roles."](#)

3.2.2 Using the Identity Store

Oracle Entitlements Server administrator and user identities are stored in an identity store, typically an LDAP directory server. Users and external roles defined in the identity store are read-only; Oracle Entitlements Server reads and displays the data but cannot perform management operations on it. Management of the identity data is accomplished using the identity store's tools or an identity management product such as Oracle Identity Manager.

Note: After installation, the Oracle Entitlements Server identity store is associated with the WebLogic Server embedded LDAP directory. See [Section 3.1, "Before You Begin"](#) for the procedure to reconfigure Oracle Entitlements Server to use a supported LDAP directory.

Oracle Entitlements Server will use the Oracle Platform Security Services (OPSS) Identity Store Service to allow for the configuration and support of multiple identity

stores. The Identity Store Service allows access to, and management of, multiple identity types (users, groups, roles) and is extensible to support new identity types. For information on the Identity Store Service, see the *Oracle Fusion Middleware Application Security Guide*. See [Section 10.3, "Configuring Identity Directory Service Profiles"](#) for details specific to Oracle Entitlements Server.

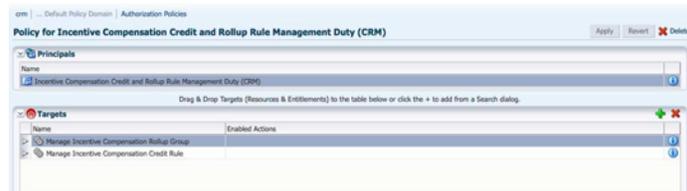
3.2.3 Accessing the Policy Store

The Policy Store used to maintain security objects and defined policies must be a relational database. For links regarding hardware requirements, see [Section 3.1, "Before You Begin."](#) Basic information about the Policy Store can be found in the *Oracle Fusion Middleware Application Security Guide*.

3.2.4 Displaying Oracle Platform Security Services Application Grants

The Administration Console displays advanced Authorization Policies created using Oracle Entitlements Server as well as the simpler Application Grants (application policies) created using Oracle Platform Security Services (OPSS). The OPSS Application Grants can be displayed for viewing, modification and deletion only. When created using OPSS, Application Grants are defined with a principal and target only. [Figure 3–4](#) is a screenshot of the Oracle Entitlements Server screen when an OPSS Application Grant is displayed using one of the search functions.

Figure 3–4 OPSS Application Grants Display Screen



Note the Name, Display Name and Description fields are not displayed as they would be if the Authorization Policy was created using Oracle Entitlements Server. OPSS Application Grants can only be removed or modified using Oracle Entitlements Server; they cannot be created using Oracle Entitlements Server. For more information on Application Grants, see the *Oracle Fusion Middleware Application Security Guide*.

3.3 Accessing the Administration Console

The following sections contain information on the Authorization Policy Manager graphical interface (also referred to as the Administration Console).

- [Section 3.3.1, "Signing In to the Administration Console"](#)
- [Section 3.3.2, "Signing Out of the Administration Console"](#)

3.3.1 Signing In to the Administration Console

Follow this procedure to sign in to the Authorization Policy Manager Administration Console.

1. Enter the Authorization Policy Manager Administration Console URL in the address bar of your browser. For example:

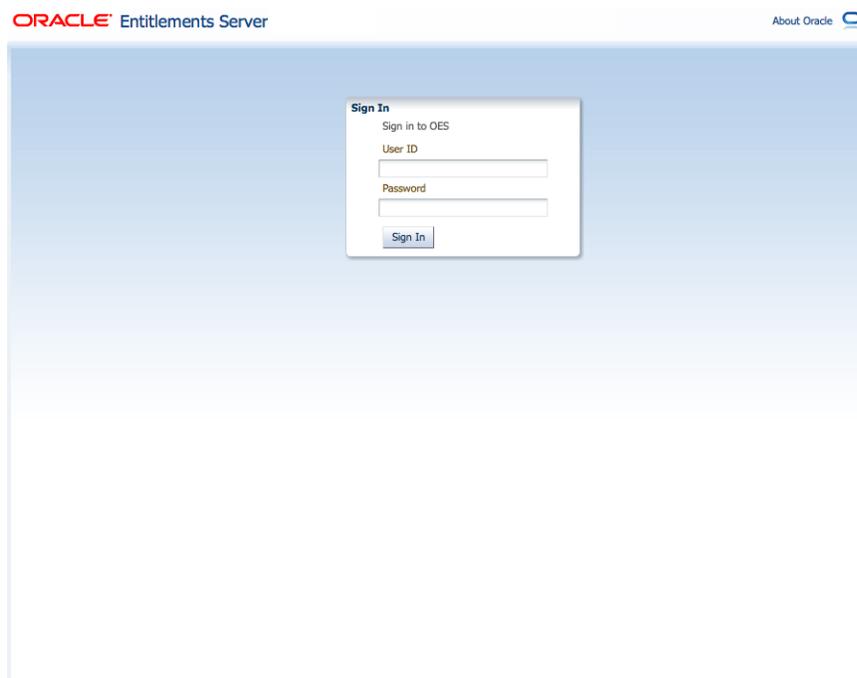
```
https://hostname:port/apm/
```

where:

- `https` represents the Hypertext Transfer Protocol (HTTP) with Secure Socket Layer (SSL) enabled to encrypt and decrypt user page requests and the pages returned by the Web server.
 - `hostname` refers to the fully qualified domain name of the computer hosting the Oracle Authorization Policy Manager Administration Console.
 - `port` refers to the designated bind port for the Authorization Policy Manager Administration Console. (This is the same as the bind port for the WebLogic Server Administration Console.)
 - `/apm/` refers to the context-root of the Authorization Policy Manager application which redirects to the login page.
2. Enter the System Administrator credentials.

The default system administrator identifier is `weblogic`. The password is the same one supplied during installation. [Figure 3–5](#) is a screenshot of the Sign In page.

Figure 3–5 Administration Console Sign In Page



3. Click **Sign In**.

3.3.2 Signing Out of the Administration Console

Follow this procedure to sign out of the Authorization Policy Manager Administration Console.

1. Click the **Sign Out** link located in the upper right corner of the Administration Console.

[Figure 3–6](#) is a screenshot of the Sign Out link.

Figure 3–6 Administration Console Sign Out Link

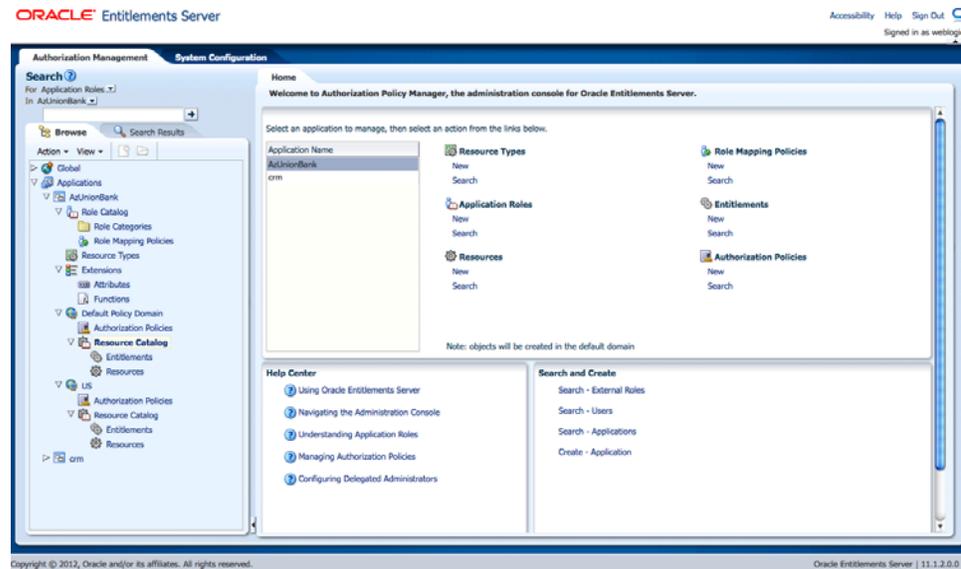


2. Close the browser window.

3.4 Navigating the Administration Console

After a successful log in, the Authorization Policy Manager Administration Console is displayed with the Authorization Management Tab active. The Navigation Panel is on the left side and the Home tab is displayed on the right side. Objects selected in the Navigation Panel are opened and displayed in new tabs next to the Home tab on the right. Figure 3–7 is a screenshot of the Administration Console after an administrative user has successfully signed in.

Figure 3–7 Oracle Entitlements Server Administration Console



The following list contains descriptions of the top-level items displayed in Figure 3–7. See the appropriate links for more information.

- Section 3.4.1, "Understanding the Main Tabs"
- Section 3.4.2, "Using The Navigation Panel"
- Section 3.4.3, "Using the Home Tab"
- Section 3.4.4, "Accessing Help"

3.4.1 Understanding the Main Tabs

See the following sections for information on the organizational tabs used in the Administration Console. Each tab is comprised of a Navigation Panel and Home area.

- Section 3.4.1.1, "Authorization Management Tab"

- Section 3.4.1.2, "System Configuration Tab"

3.4.1.1 Authorization Management Tab

The Authorization Management tab is used to search and manage policy objects. This tab is active upon successful log in to the Administration Console. Figure 3–8 is a screenshot of the Authorization Management tab.

Figure 3–8 Authorization Management Tab

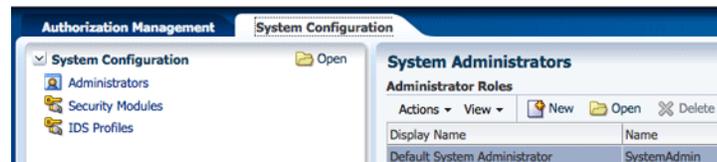


Under Authorization Management, the left side is the Navigation Panel and the right side is Home. The Home display changes based on what is selected from the Navigation Panel. For more information, see Section 3.4.2, "Using The Navigation Panel" and Section 3.4.3, "Using the Home Tab."

3.4.1.2 System Configuration Tab

The System Configuration tab is used to manage administrative and system type objects for the Oracle Entitlements Server deployment. Figure 3–9 is a screenshot of an active System Configuration tab. The object selected in the Navigation Panel is displayed using tabs in the Home area.

Figure 3–9 System Configuration Tab



The following tasks are performed under System Configuration:

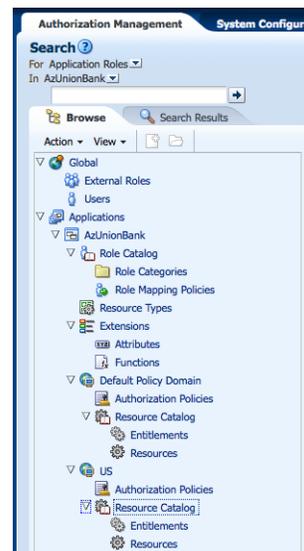
- Creating Security Module definitions and binding them to Applications
- Managing system administrators (for example, creating additional system administrator roles, assigning users to system administrator roles, and assigning rights to system administrator roles)
- Managing Identity Store profiles

For more information, see Chapter 10, "Managing System Configurations".

3.4.2 Using The Navigation Panel

The Navigation Panel is used to find security objects by browsing the Global or Applications information trees, or by conducting a simple search. It lists all Global and Application policy objects in a navigatable tree. You can browse the tree or display objects as Search Results based on defined search criteria. Figure 3–7 is a screenshot that displays the Navigation Panel with its nodes collapsed. Figure 3–10 displays the Navigation Panel with its nodes expanded and many policy objects in view.

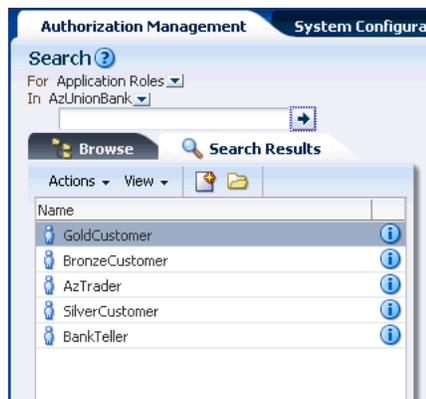
Figure 3–10 Navigation Panel Browse Tab With Nodes Expanded



The Navigation Panel contains, from top to bottom, the following elements:

- A pull-down list to select the policy object for a simple search. For more information, see [Section 5.2, "Finding Objects with a Simple Search."](#)
- A pull-down list to select the scope of a simple search. For more information, see [Section 5.2, "Finding Objects with a Simple Search."](#)
- A text box to enter the simple search string. The string is compared against both the Name and Display Name of policy objects; those that match are displayed in the Search Results tab.
- The **Browse** tab displays the following expandable and collapsible nodes:
 - The **Global** node collects global objects such as external roles and users.
 - The **Applications** node contains one or more Applications being managed by the administrator that is logged in. (Only Applications which the logged in user is authorized to access are displayed.) From any of those displayed, the administrator can access application-specific policy objects such as resource types, entitlements, resources, policies, and roles. For more information, see [Chapter 10, "Managing System Configurations"](#).
- The **Search Results** tab displays the results of the last simple search as seen in [Figure 3–11](#).
- Action and View drop downs to select operations on the chosen policy object.

Figure 3–11 Navigation Panel Search Tab



From the Navigation Panel, there are two methods for displaying the **New** and **Open** options comprised in the Actions drop-down list.

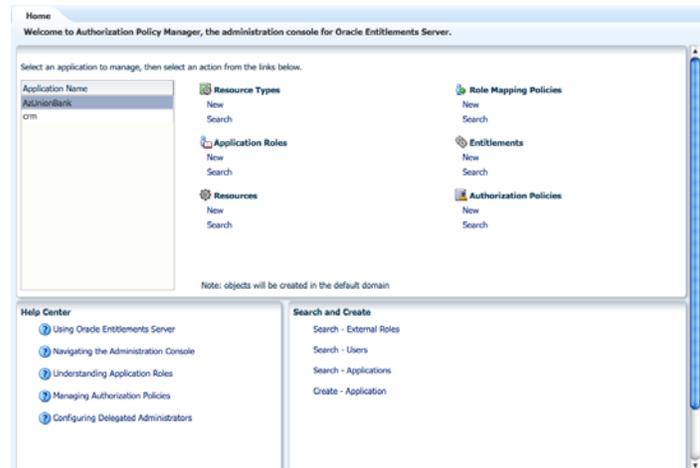
- Locate the desired Application, expand the node, and select the desired object. Click the Actions drop-down menu and select New or Open.
- Locate the desired Application, expand the node, right-click the desired object and select New or Open.

Select **New** to create a new object of the same type and select **Open** to display a search tab in the Home area. Double-clicking an object from the node also opens a Search tab in the Home area.

3.4.3 Using the Home Tab

The Home tab displays on the right side of the Navigation Panel and contains quick access links to New and Search screens for the most commonly used policy objects. As displayed in Figure 3–12, the Home tab of the Administration Console is divided into the following sections.

- The **Application** area is the upper region of the Home tab. The Application Name pane displays all applications available to the logged in user. To the right of this pane are links to screens for performing common operations such as creating new policy objects (entitlements, resources, resource types, application roles, and authorization policies) or searching defined policy objects.
- The **Global** section is the lower right region of the Home tab. This section is for objects shared across all applications and includes external role search.
- The **Entitlements Resource Center** section is the lower left region of the Home tab. It contains links to information regarding the most commonly used procedures.

Figure 3–12 The Home Tab

3.4.4 Accessing Help

To get more information while using the Administration Console, click the Help link located in the upper right corner (as seen in [Figure 3–6](#)). A separate window opens. From this window you can access both the online help and an embedded version of this book in HTML. After the window displays, select either *Oracle Entitlements Server Administration Console Online Help* or *Administrator's Guide for Oracle Entitlements Server* from the drop-down Book list. The help topics link to the corresponding section of the embedded book as do the links in the book's Table of Contents.

3.5 Upgrading from Oracle Entitlements Server Basic

Oracle Entitlements Server can be licensed separately from other Oracle products with an agreement that defines usage restrictions. Oracle Entitlements Server Basic replaces the embedded authorization engine within Oracle Platform Security Services (OPSS) and is used to define, enforce and audit basic Role Based Access Control and Java/JAAS permission based authorization policies. A Basic license allows the use of a limited set of features provided by Oracle Entitlements Server and the Oracle Entitlements Server Security Modules, and is included and available for use only with Oracle products that list this component in their respective licensing documentation. More information is in the *Oracle Fusion Middleware Licensing Information*.

In the simplest scenario, nothing other than licensed Oracle Fusion Middleware or Fusion Applications technologies that include Oracle Entitlements Server Basic need be installed. Oracle Fusion Middleware products that include Oracle Entitlements Server Basic contain:

- The Oracle Entitlements Server authorization engine (Policy Decision Point)
- A default policy store (not supported for production environments) is configured based on the `system-jazn.xml` file. You must configure either the Oracle Relational Database Management System or Oracle Internet Directory based policy store for production environments.

The Oracle Entitlements Server Administration Console (Authorization Policy Manager) can optionally be installed to provide centralized policy management.

3.5.1 Changing From Basic to Advanced Policy Authorization

When Authorization Policy Manager is installed for Oracle Fusion Applications, it is configured to allow for Oracle Entitlements Server Basic authorization. Basic authorization is based on the permissions policy model in which permissions are granted to users, groups, and code sources. For users and groups, the permissions determine what a user or a group member is allowed to access. For code sources, they determine what actions the code is allowed to perform. Advanced authorization allows for the use of more fine-grained policy objects including Role Mapping Policies and hierarchical resources.

Use the following procedure to reconfigure Authorization Policy Manager for advanced authorization. It assumes WebLogic Server is installed and the Fusion Middleware home directory is available.

1. Change to the Fusion Middleware home directory at `$FMW_HOME/oracle_common/common/bin`.

2. Connect to the WebLogic Server using the `wlst.sh` command.

```
connect ('weblogic','weblogic1','t3://localhost:7101')
```

The command takes the following arguments: user name (weblogic), password associated with the user (weblogic1) and the T3 connection URL for the Administration Server. In this example, it is running locally on port 7101.

3. Export the Authorization Policy Manager configuration file using the `exportMetadata` command.

```
exportMetadata(application='oracle.security.apm', server='AdminServer',
toLocation='/tmp/repository/',
docs='/oracle/security/apm/config/apm-config.xml')
```

This command will export the `apm-config.xml` configuration file to the `/tmp/repository` sub-directory on the machine that hosts the Administration Server. The command takes the following arguments:

- The application owner of the document being exported; in this case, the default value is `oracle.security.apm`.
 - The name of the WebLogic Server Administration Server.
 - The directory to which `apm-config.xml` will be exported. Be sure you have access rights to this directory.
 - The document being exported; in this example, `oracle/security/apm/config/apm-config.xml` will be exported, so please make sure you have access right to that file path in the AdminServer machine once you downloaded the documents
4. Open the `apm-config.xml` configuration file in a text editor.
The file is in the `/tmp/repository` directory as previously specified.
 5. Change the value of the `oracle.security.apm.oes.mode` attribute in this file from *basic* to *advanced*.
 6. Save the changes and close the file.
 7. Upload the modified file back to the repository.

```
importMetadata(application='oracle.security.apm', server='AdminServer',
fromLocation='/tmp/repository/',
docs='/oracle/security/apm/config/apm-config.xml')
```

This command will import the `apm-config.xml` configuration file back to the machine that hosts the Administration Server. The command takes the following arguments:

- The application owner of the document being imported; in this case, the default value is `oracle.security.apm`.
 - The name of the WebLogic Server Administration Server.
 - The directory from which `apm-config.xml` will be imported.
 - The document being imported; in this example, `apm-config.xml` will be imported to the `oracle/security/apm/config/` directory.
8. Issue the exit command.

```
exit()
```

3.6 Accessing Oracle Entitlements Server Examples

<http://www.oracle.com/technetwork/indexes/samplecode/index.html> is the repository on Oracle Technology Network from which developer and administration examples for Oracle Entitlements Server can be accessed.

Managing Policies and Policy Objects

The Oracle Entitlements Server Administration Console is used to manage Authorization and Role Mapping Policies, and the security objects from which they are created. This chapter contains the following sections.

- Section 4.1, "Introducing Policy and Policy Object Management"
- Section 4.2, "Defining an Authorization Policy And Its Components"
- Section 4.3, "Adding Fine-Grained Elements to an Authorization Policy"
- Section 4.4, "Implementing An Authorization Policy Step by Step"
- Section 4.5, "Managing Policy Objects in An Application"
- Section 4.6, "Using the Condition Builder"

4.1 Introducing Policy and Policy Object Management

Oracle Entitlements Server allows administrators to perform create, read, update, and delete operations on all policy objects. This can be done in any of the following ways:

- Using the Administration Console (as described in this book)
- Using the Management API (as described in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*)
- Using the WebLogic Scripting Tool on the command line (as described in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*)

Authorization Management tasks performed in the Administration Console typically require that an administrator identify an object (by browsing or searching), select it, and choose one of the operations available for it. Objects are organized in the main groupings displayed in the Navigation Panel.

- **Application** objects include the objects used to create Role Mapping and Authorization Policies (Resources, Application Roles and the like). They apply to, and can only be used for Authorization Policies within, the Application under which they are defined. The Applications node in the Navigation Panel is the branch under which all configured Applications (and their respective objects) are organized. This chapter contains information on managing Applications and their child objects.
- **Global** objects include users and External Roles. These objects may apply to all configured Applications throughout the system. The Global node in the Navigation Panel is the branch under which all system-wide objects are organized.

Note: Within Oracle Entitlements Server, External Roles (and users) are read only and managed with a tool such as Oracle Identity Manager. For more information, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager*.

System Configuration tasks performed in the Administration Console typically include Security Module profile definitions and bindings, system administrator configurations, and identity store profile definitions and bindings. These objects are discussed in [Chapter 10, "Managing System Configurations."](#)

Note: Oracle Entitlements Server supports the mapping of policies to Users, External Roles, and Application Roles. However, mapping policies to Application Roles is recommended because managing authorization based on grants to individual Users and External Roles can become unmanageable as the number increases. Additionally, if the identity store changes (for example, when a move between development, test and production environments results in a new LDAP server), no changes to policy definitions are needed. All that is required is a re-mapping of the Application Roles to the Users and External Roles available in the target environment.

By default, all access to a resource is denied until an Authorization Policy is written and deployed that explicitly grants access action. If the Authorization Policy only grants an entitlement on a Resource to a role, the user must be statically assigned to it or a Role Mapping Policy must be written and deployed that assigns a user or a group to the defined role. If an Authorization Policy denies a previously granted entitlement, it takes precedence over the grant. Explicit DENY authorization policies cannot be overruled. A practical use of a DENY policy is to explicitly deny an entitlement to ensure that a user or group can never gain access to a specific resource.

4.2 Defining an Authorization Policy And Its Components

Defining a policy requires that the objects be created in a particular order. For example, a Resource can only be created after defining a Resource Type. A policy can be composed by following the sequence described below.

1. Create an Application.

In the Navigation Panel, an Application should be created as the overall container for policies and related information that secure the components of a particular resource. You may create as many Applications as needed although it is recommended that only one is created for each application to be secured. For more information, see [Section 4.5.1, "Managing Applications."](#)

2. Create a Resource Type.

A Resource Type specifies one or more Resource attributes, and definitions of all possible valid actions that can be performed on a particular kind of resource.

Note: Before an attribute can be added to a Resource Type it must be defined as documented in [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#)

The actions can be standard actions (GET and POST to a URL) or custom actions on a business object (transfer money to or from a bank account). Consider the following Resource Types and their valid actions:

- A file may support Read, Write, Copy, Edit, and Delete actions, depending on its type. A `clearance` Resource attribute may be associated with the file to define who can see it. It might do this by defining a security level that must be held by the subject for access; values might include `unclassified`, `restricted`, `confidential`, or `topSecret`. For example, if the clearance attribute has a value of `topSecret`, an Authorization Policy can be created to grant access by adding the condition: `if securityLevel = topSecret`.
- A checking account application may support deposit, withdrawal, view account balance, view account history, transfer to savings, and transfer from savings.

Resource instances are created from Resource Types. Actions defined by the Resource Type are granted or denied when accessing a protected Resource instance created from the Resource Type.

Note: A Resource instance is defined in a Policy Domain and references the Resource Type. For more information, see [Section 4.5.3, "Managing Resources."](#)

For more information, see [Section 4.5.2, "Managing Resource Types."](#)

3. Instantiate a Resource from the Resource Type.

A specific protected target (Resource) is instantiated from a Resource Type. A Resource represents a secured target (for example, an application) and is created under a Policy Domain in the Resource Catalog.

Note: A Policy Domain is an optional object that is created for purposes of delegated administration and organization. If no Policy Domain is specified, the Resource instance is created under the Default Policy Domain. See [Chapter 11, "Delegating With Administrator Roles."](#)

It is not necessary to create a Resource instance for each protected resource. A Resource Name Expression can also be used in an Authorization Policy. A Resource instance is required, though, if a Resource attribute is being created. For more information, see [Section 4.5.3, "Managing Resources."](#)

4. Build the Authorization Policy.

This entails specifying the effect (GRANT or DENY), adding a user, group or role as the policy principal and the Resource and actions as the policy target. Optionally, you can add an Obligation or build a Condition. For more information, see [Section 4.5.5, "Managing Authorization Policies."](#)

4.3 Adding Fine-Grained Elements to an Authorization Policy

[Section 4.2, "Defining an Authorization Policy And Its Components"](#) documented the minimum components needed to create an authorization policy. The following fine-grained elements can be added to a simple policy.

- Entitlements

An Entitlement associates an instantiated Resource with the applicable actions that can be performed on it. The set of actions for a Resource are a subset of the set of legal actions already defined in its corresponding Resource Type. For more information, see [Section 4.5.4, "Managing Entitlements."](#)

- Application Roles

An Application Role can be assigned statically or dynamically to a user, group, or external role in an identity store, or another Application Role in the policy store. One target application may have several different Application Roles, with each role assigned a different set of privileges for more fine-grained access. For more information, see [Section 4.5.6, "Managing Application Roles in the Role Catalog."](#)

- Role Mapping Policy

Membership in an Application Role can be granted dynamically with a Role Mapping Policy. An Application Role, referenced as a Principal in a Role Mapping Policy, could grant a user access to the defined resources but the Role Mapping Policy must be resolved before an authorization decision is reached. The resolution of the Role Mapping Policy answers the question *Can the user requesting access be assigned this Application Role?* The Role Mapping Policy returns a list of roles. The results garnered from a Role Mapping Policy (the roles granted the Principal) may be used in an Authorization Policy; the Role Mapping Policy itself cannot. During runtime evaluation of a request for access, the following occurs:

1. Based on the subject requesting access, a list of Application Roles is determined by retrieving static role membership and evaluating any applicable Role Mapping Policies.
2. Based on the subject and determined list of Application Roles, a list of Authorization Policies is evaluated to find any that might be applicable based on the grantee, target matching and constraints evaluation. The actions allowed on the Resource are defined by the Authorization Policy.
3. Final authorization decision is based on the "DENY overrides" combining algorithm.

For more information, see [Section 4.5.7, "Managing Role Mapping Policies."](#)

- A Condition can be added to a policy as a way of setting an additional contingency on the policy. It is applicable to either an Authorization Policy or a Role Mapping Policy. A Condition is written in the form of an expression that resolves to true or false and has one of the following outcomes:
 - If the expression resolves to true, the policy condition is satisfied and the effect defined in the PolicyRuleEntry is applicable.
 - If the expression does not resolve to true, the policy is not applicable.

A Condition must be true for the policy to evaluate to true. Conditions can be complex combinations of boolean expressions that test the value of some user, resource, dynamic or system attributes or, custom Java evaluation functions that evaluate complex business logic. For more information, see [Section 4.6, "Using the Condition Builder."](#)

- An Obligation specifies optional information to be evaluated during the policy enforcement phase of authorization. The obligation is returned with the corresponding policy effect (GRANT or DENY). This information may or may not be taken into account during policy enforcement based on settings defined by the application. For example, the reason a request for access has been denied might be

returned as an obligation. A different type of obligation might involve sending a message; for example, if a certain amount of money is withdrawn from a checking account, send a text message to the account holder's registered mobile phone. For more information, see [Section 4.5.5, "Managing Authorization Policies."](#)

4.4 Implementing An Authorization Policy Step by Step

In [Section 2.4, "Implementing a Policy Use Case,"](#) several use cases for creating a policy are discussed. This section documents the step by step procedure to create an Authorization Policy (and the policy objects from which it is comprised) using the Administration Console. This procedure assumes you have installed Oracle Entitlements Server and a Java Security Module to protect an application.

1. Create an Application.

The Application Name must match what is used in the application code. For example, create a `HelloOESworld` Application object to map to a `HelloOESworld` Application. See [Section 4.5.1.1, "Creating an Application."](#)

2. Create a Resource Type.

The Resource Type Name must match what is used in the application code. For example, create a `Files` Resource Type object for use in collecting files that will be protected. (You might also create Resource attribute for the Resource Type; for example, a `filetype` attribute that may contain a value of `html`, `image`, `jsp` or `pdf` defines the file type.) Associate the `write` and `read` actions with the Resource Type. See [Section 4.5.2.1, "Creating a Resource Type."](#)

3. Create a Resource.

A Resource Name must match what is used in the application code. Additionally, the Resource is created from the Resource Type. For example, create a `FinanceFile` Resource from the `Files` Resource Type. See [Section 4.5.3.1, "Creating a Resource."](#)

4. Create the Authorization Policy.

In the `HelloOESworld` Application, create an Authorization Policy. Add one or more Principals (Roles or Users), one or more targets (Resources or Entitlements) and confirm the actions for the target. Optional conditions or obligations can also be added before saving. See [Section 4.5.5.1, "Creating an Authorization Policy."](#)

5. Create a Security Module definition and bind it to the Application.

This step defines the Security Module to which this Authorization Policy is distributed once bound. See [Section 10.2, "Configuring Security Module Definitions."](#)

6. Distribute the Authorization Policy to the Security Module.

See [Chapter 6, "Managing Policy Distribution."](#)

4.5 Managing Policy Objects in An Application

The following sections describe how to manage policy objects specific to the Applications.

- [Section 4.5.1, "Managing Applications"](#)
- [Section 4.5.2, "Managing Resource Types"](#)
- [Section 4.5.3, "Managing Resources"](#)
- [Section 4.5.4, "Managing Entitlements"](#)

- [Section 4.5.5, "Managing Authorization Policies"](#)
- [Section 4.5.6, "Managing Application Roles in the Role Catalog"](#)
- [Section 4.5.7, "Managing Role Mapping Policies"](#)
- [Section 4.5.8, "Managing a Role Category"](#)
- [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#)

4.5.1 Managing Applications

An Application is created as the overall container for policies and related artifacts that secure the components of a particular application. These artifacts include (but are not limited to) roles, resources, attributes and functions. You may create as many Application instances as needed although it is recommended that only one is created for each application to be secured. The following sections describe management operations on Application instances.

- [Section 4.5.1.1, "Creating an Application"](#)
- [Section 4.5.1.2, "Modifying an Application"](#)
- [Section 4.5.1.3, "Deleting an Application"](#)

4.5.1.1 Creating an Application

To create an Application, proceed as follows:

1. Right-click Applications in the Navigation Panel and select New from the menu.

Note: Alternately, click Create Application under Search and Create in the Home area.

An Untitled page with several tabs displays in the Home area. The General tab is active. You can only configure the Delegated Administrators and Policy Distribution details after the Application has been created. See [Section 4.5.1.2, "Modifying an Application"](#) for information.

2. Provide the following information for the application being created under the General tab.
 - **Display Name:** The Display Name is optional and case insensitive. Specifying a meaningful value, though, is recommended as it is displayed in the Administration Console and can be used as a search parameter.
 - **Name:** The name is required and case insensitive. It must match what is used in the application code.
 - **Description:** Although optional, it is recommended to provide useful information about the Application.
3. Select one of the following from the Save menu.
 - **Save** saves the configuration, renames the tab with the value provided for the Application's Display Name and activates the Delegated Administrators and Policy Distribution tabs.
 - **Save and Close** saves the configuration and closes the tab.

- **Save and Create Another** saves the configuration to the policy store, refreshes the information tree in the Navigation Panel and leaves an Untitled area open for you to create another Application.

4.5.1.2 Modifying an Application

To modify an Application, proceed as follows:

1. Expand the **Applications** node in the Navigation Panel.
2. Select the name of the Application to modify.
3. Right-click the Application name and select **Open** from the menu.
Alternately, double-click the Application name. The Application page is displayed and the General tab, the Delegated Administrators tab and the Policy Distribution tab are all active.
4. Select the tab you want to modify or configure and see the appropriate section for parameter details.
 - **General:** [Section 4.5.1.1, "Creating an Application"](#)
 - **Delegated Administrators:** [Chapter 11, "Delegating With Administrator Roles"](#)
 - **Policy Distribution:** [Chapter 6, "Managing Policy Distribution"](#)
5. Apply or save as necessary.

4.5.1.3 Deleting an Application

To delete an Application instance, proceed as follows:

1. Find the Application to delete using an advanced search (as documented in [Section 5.3.2, "Searching Applications"](#)).
The Search Applications page is displayed.
2. Enter query parameters and click Search.
The results are displayed.
3. Select the Application name from the results and click Delete.
4. Choose one of the following methods to search for the Application:
A Delete Warning is displayed.
5. Click Delete.
The Application is deleted. Alternately, you can expand the Applications information tree in the Navigation Panel and double click the name of the Application to delete. When the Application's tab is displayed, click Delete in the upper right corner.

4.5.2 Managing Resource Types

Resource Types specify the full scope of traits for a particular kind of protected resource. It contains one or more resource attributes, and definitions of all possible valid actions that can be performed on the particular kind of resource. An *action* represents an activity or task in your business process that can be executed on a resource. Actions can be standard (GET and POST to a URL) or custom on a specific business object (transfer to or from a bank account). A Resource instance for a specific

target is created from a Resource Type. The following sections describe management operations on Resource Types.

- [Section 4.5.2.1, "Creating a Resource Type"](#)
- [Section 4.5.2.2, "Modifying a Resource Type"](#)
- [Section 4.5.2.3, "Deleting a Resource Type"](#)

4.5.2.1 Creating a Resource Type

To create a Resource Type, proceed as follows:

1. Display the page for creating a Resource Type by choosing from the following methods:
 - Expand the information tree in the Navigation Panel, right-click Resource Types under the particular Application in which the Resource Type will be created and select from the menu.
 - In the Home area, select the Application Name under which the Resource Type will be created and click New under Resource Types.

An Untitled page is displayed in the Home area. Alternately, you can click New from the Simple or Advanced Search results pages. See [Chapter 5, "Querying Security Objects"](#) for information.

2. Provide the following information for the Resource Type.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful value, though, is recommended as it is displayed in the Administration Console and can be used as a search parameter.
 - **Name:** The name is required and case insensitive.
 - **Resource Finder:** An (optional) class that implements the `oracle.security.jps.service.policystore.entitymanager.ResourceFinder` interface. It allows resources managed outside of the Policy Store to be consumed. (*Reserved for future use.*)
 - **Description:** Although optional, it is recommended to provide useful information. The description string is case insensitive.
3. Add actions allowed by the Resource Type in the Actions section.
 - a. Click **New** to display the New Action dialog
 - b. Enter the name of the action.

The string entered must match the actions for which your application is asking for authorization. If a Permission class is added, the action must be meaningful to it.
 - c. Click **Save**.The Action list is updated with the new action.
4. Use the Find Existing Attribute dialog to add attributes to the Resource Type being created.
 - a. In the Attributes section, click **Add** to display the Find Existing Attribute dialog.

Before an attribute can be displayed, it must be defined. See [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#)
 - b. Select the attribute **Type** from the list.

- c. Enter an (optional) string to match in the **Search** text box.
- d. Click the arrow icon next to the Search text box to begin the search.
- e. Select the attributes to add and click **Add**.

Use **Ctrl+click** to select multiple items from the list.

These attributes are used when instantiating a Resource. See [Section 4.5.3.1, "Creating a Resource."](#)

5. Configure the remaining fields.

The selection changes according to the Resource Type being created.

- Supports Resource Hierarchy - Select Yes or No to set the Resource Type as hierarchical. This means the following when the Resource Type is used to instantiate a Resource:
 - A policy applicable to a Resource created from a hierarchical Resource Type is also applicable to Resources that are its children.
 - Any attribute defined for a Resource created from a hierarchical Resource Type is inherited by Resources that are its children.
- Resource Name Delimiter - Only valid when Supports Resource Hierarchy is enabled. The default delimiter is Slash (/).
- Evaluation Logic - Evaluation logic for a Resource Type can be either a default matching algorithm or a permission class. Select Default or Permission Class from the drop down menu.
- Permission Class - If the evaluation logic for a Resource Type is defined as Permission Class, specify a case-sensitive Permission class name. An authorization decision for permission based policies is requested using the `checkPermission` call.
- Action Name Delimiter - The specified character is used to separate actions in a list when the Resource Type represents a permission.
- All Action Keyword - If the policy's target contains the defined keyword as an action, the policy will match any action passed in with the authorization request. For example, assume that this parameter is set to ANY and you create the following policy:

```
GRANT user "Michael" action:"ANY" on resource:"Resource1
```

The decision for authorization requests like *Can Michael do 'write' on Resource1?* or *Can Michael do 'transfer' on Resource1?* will return ALLOW. The use of this parameter allows you to create a single Authorization Policy that would be applicable to any valid action for that Resource Type.

6. Select one of the following from the Save menu.

- **Save** saves the configuration and renames the tab with the value provided for the Resource Type's Display Name.
- **Save and Close** saves the configuration and closes the tab.
- **Save and Create Another** saves the configuration to the policy store, refreshes the information tree in the Navigation Panel and leaves an Untitled area open for you to create another Resource Type.

4.5.2.2 Modifying a Resource Type

To modify a Resource Type, proceed as follows:

1. Choose from the following methods to display the desired Resource Type.
 - Expand the information tree in the Navigation Panel to find the Resource Types node under the appropriate Application and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.3, "Searching Resource Types."](#)
 - Search for Resource Types using the Navigation Panel's search function and double-click the Resource Type name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Resource Type was created and click **Search** under **Resource Types**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.3, "Searching Resource Types."](#)

When the correct Resource Type name is displayed, select it and click Open to display the details.

2. Modify as necessary.
3. Click **Apply**.

4.5.2.3 Deleting a Resource Type

To delete a Resource Type, proceed as follows:

1. Choose from the following methods to delete the desired Resource Type.
 - Expand the information tree in the Navigation Panel to find the Resource Types node under the appropriate Application and double click it. A search dialog opens in the Home area. Enter criteria for the lookup and click Search. Select the appropriate Resource Type from the search results and click Delete. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Resource Types using the Navigation Panel's search function. Find the appropriate Resource Type from the search results and double-click it. After the Resource Type profile opens in the Home area, click Delete. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)

A Delete Warning is displayed.

2. Click Delete.

The Resource Type is deleted.

4.5.3 Managing Resources

A Resource represents a specific, secured target in a protected application. Each Resource belongs to a defined Resource Type and can represent software components managed by a container (URLs, EJBs, JSPs) or business objects in an application (reports, transactions, revenue charts).

Note: Resources can be hierarchical (in that the child resource inherits attributes from parent resources) or non-hierarchical. When organized in a hierarchy (root down), you can add new attributes to the parent resources or overwrite any existing attributes that are inherited.

The following sections describe management operations on Resources.

- [Section 4.5.3.1, "Creating a Resource"](#)
- [Section 4.5.3.2, "Modifying a Resource"](#)
- [Section 4.5.3.3, "Deleting a Resource"](#)

4.5.3.1 Creating a Resource

To create a Resource, proceed as follows

1. Display the page for creating a Resource by choosing from the following methods:
 - Navigate to the Resource Catalog by expanding the applicable Policy Domain node in the appropriate Application node using the Navigation Panel. Right-click **Resources** from the Resource Catalog node and select **New** from the menu.
 - Select the Application under which you will create the Resource instance from the Home area and click **New** under **Resources**.

Note: This option creates the Resource in the Application's Default Policy Domain.

An Untitled page is displayed in the Home area. Alternately, you can click New from the Simple or Advanced Search results pages. See [Chapter 5, "Querying Security Objects"](#) for information.

2. Provide the following information.
 - **Resource Type:** Select from the list. This defines what is displayed in the Instance Attributes and Overwrites table.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Name:** The name is required and case sensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
3. Add or remove the attributes for this Resource from those displayed in the Instance Attributes and Overwrites dialog.

The Overwrites dialog is displayed only in the case of hierarchical Resources.

4. Select the attributes from the list (use **Ctrl+click** to select multiple items from the list) and click **Add**.

5. Select one of the following from the Save menu.
 - **Save** saves the configuration and renames the tab with the value provided for the Resource's Display Name.
 - **Save and Close** saves the configuration and closes the tab.
 - **Save and Create Another** saves the configuration to the policy store, refreshes the information tree in the Navigation Panel and leaves an Untitled area open for you to create another Resource.

4.5.3.2 Modifying a Resource

To modify a resource, proceed as follows:

1. Choose from the following methods to display the desired Resource.
 - Navigate to the Resource Catalog by expanding the applicable Policy Domain node in the appropriate Application node using the Navigation Panel and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.6, "Searching Resources."](#)
 - Search for Resources using the Navigation Panel's search function and double-click the Resource name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Resource Type was created and click **Search** under **Resources**. A search dialog opens in the Home area. This search dialog will only query the Default Policy Domain. For information about searching in the Home area, see [Section 5.3.6, "Searching Resources."](#)

When the correct Resource name is displayed, select it and click Open to display the details.

2. Modify the Resource as necessary.
3. Click **Apply**.

4.5.3.3 Deleting a Resource

To delete a Resource, proceed as follows:

1. Choose from the following methods to delete the desired Resource.
 - Navigate to the Resource Catalog by expanding the applicable Policy Domain node in the appropriate Application node using the Navigation Panel and double click it. A search dialog opens in the Home area. Enter criteria for the lookup and click Search. Select the appropriate Resource from the search results and click Delete. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Resources using the Navigation Panel's search function. Find the appropriate Resource name from the search results and double-click it. After the Resource Type profile opens in the Home area, click Delete. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Resource was created and click **Search** under **Resources**. A search dialog opens in the Home area. Enter criteria for the lookup and click Search. (This search queries only in the Default Policy Domain.) Select the appropriate Resource from the search

results and click Delete. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

A Delete Warning is displayed.

2. Click Delete.

The Resource is deleted. If the Resource Type is hierarchical, child resources of the Resource are also deleted.

4.5.4 Managing Entitlements

After instantiating a Resource, define the actions that can be performed on it in an Entitlement. The actions are defined using the set of legal actions defined in the Resource's parent Resource Type. The following sections describe management operations on Entitlements.

- [Section 4.5.4.1, "Creating an Entitlement"](#)
- [Section 4.5.4.2, "Modifying an Entitlement"](#)
- [Section 4.5.4.3, "Deleting an Entitlement"](#)

Note: An Entitlement may be created if there are plans to use the same list of Resource and Action pairs in multiple policies. Otherwise, the Resource and Action pair itself can be directly specified as a target when you create an Authorization Policy. See [Section 4.5.5, "Managing Authorization Policies"](#) for more information.

4.5.4.1 Creating an Entitlement

To create an Entitlement, proceed as follows.

1. Display the page for creating an Entitlement by choosing from the following methods:
 - Navigate to the Resource Catalog by expanding the applicable Policy Domain node in the appropriate Application node using the Navigation Panel. Right-click **Entitlements** from the Resource Catalog node and select **New** from the menu.
 - In the Home area, select the Application Name under which the Entitlement will be created and click **New** from **Entitlements**.

An Untitled page is displayed in the Home area.

2. Provide the following information.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Entitlement Name:** The name is required and case insensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
3. Choose one of the following methods to add Resources to the Entitlement.
 - Drag and drop

- a. Use the Navigation Panel to list the Application's available Resources by performing a search on Resource instances. The Resources must be searched from the same Policy Domain in which the Entitlement is being created. For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
- b. Drag and drop Resources from the **Search Results** tab into the area labeled **Resources**.
- Add Targets pop up search
 - a. Click **Add** in the **Targets** section.
The **Add Targets** dialog displays. This will search in the current Policy Domain.
 - b. Search for available targets by entering a string.
The resources matching the query are displayed in **Search Results**. If no search string was entered, a list of all objects of the specified type is returned.
 - c. Select your choice(s) and click Add Selected.
The Target(s) are added to the Selected Targets. Use **Ctrl+click** to select multiple items from the list.

Note: Alternately, you can click the Resource Expression link under the Resources tab, select a Resource Type, enter a string expression and click Add to Targets. This will search for targets, using the defined criteria, dynamically at runtime. All Resources that belong to the selected Resource Type that contain the string expression are returned, within the context of the administrator privileges.

- d. Click **Add Targets**.
4. Add actions to the Resources as follows:
 - a. Select an added resource from the Resources list to display the resource details in the **Resource Details** section.
 - b. Expand the selected row to see the range of actions.
Only the actions allowed for the type of the selected resource are available in this area.
 - c. Check the desired actions for the Resource in the **Actions** section.
 - d. Repeat this procedure for each Resource you have added to the Entitlement being created.
 5. Select one of the following from the Save menu.
 - **Save** saves the configuration and renames the tab with the value provided for the Entitlement's Display Name.
 - **Save and Close** saves the configuration and closes the tab.
 - **Save and Create Another** saves the configuration to the policy store, refreshes the information tree in the Navigation Panel and leaves an Untitled area open for you to create another Entitlement.

4.5.4.2 Modifying an Entitlement

To modify an entitlement, proceed as follows:

1. Choose from the following methods to display the desired Entitlement.
 - Navigate to the Resource Catalog by expanding the applicable Policy Domain node in the appropriate Application node using the Navigation Panel and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.7, "Searching Entitlements."](#)
 - Search for Entitlements using the Navigation Panel's search function and double-click the Entitlement name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Entitlement was created and click **Search** under **Entitlements**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.7, "Searching Entitlements."](#)

When the correct Entitlement name is displayed, select it and click Open to display the details.

2. Modify the entitlement as necessary.
3. Click **Apply**.

4.5.4.3 Deleting an Entitlement

To delete an Entitlement, proceed as follows:

1. Choose from the following methods to delete the desired Entitlement.
 - Expand the information tree in the Navigation Panel to find the Entitlement node under the appropriate Application's Resource Catalog and double click it. A search dialog opens in the Home area. Enter criteria for the lookup and click Search. Select the appropriate Entitlement from the search results and click Delete. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Entitlements using the Navigation Panel's search function and double-click the Entitlement name in the Search Results tab. Select the appropriate Entitlement from the search results and click Delete. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Entitlement was created and click **Search** under **Entitlements**. A search dialog opens in the Home area. Enter criteria for the lookup and click Search. Select the appropriate Entitlement from the search results and click Delete. ((In this case, the search is done only within the Application's Default Policy Domain.) For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

A Delete Warning is displayed.

2. Click Delete.
The Entitlement is deleted.

4.5.5 Managing Authorization Policies

The Authorization Policy is the mechanism that defines the access rights of a protected resource. A user, an Application Role or an External Role is *granted* the rights of the policy. An Authorization Policy must have:

- At least one principal which can be a user, External Role or Application Role. Code sources are not allowed as a principal.
- At least one target that can be a Resource and Action association (created within the policy) or an Entitlement (created outside the policy and added to it) but not both.
- A defined effect of PERMIT or DENY.

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.

The following sections describe management operations on Authorization Policies.

- [Section 4.5.5.1, "Creating an Authorization Policy"](#)
- [Section 4.5.5.2, "Modifying an Authorization Policy"](#)
- [Section 4.5.5.3, "Deleting an Authorization Policy"](#)

4.5.5.1 Creating an Authorization Policy

To create a policy, proceed as follows:

1. Display the page for creating a policy by choosing one of the following methods:
 - Navigate to the Policy Domain under the appropriate Application node in the Navigation Panel and expand it. Right-click **Authorization Policies** from the Resource Catalog node and select **New** from the menu.
 - In the Home area, select the Application Name under which the Authorization Policy will be created and click **New** from **Authorization Policies**. (When using this option, the policy will be created in the Default Policy Domain.)

An Untitled page is displayed in the Home area.

2. Provide the following information.
 - **Effect:** Select **Permit** if the policy will grant rights or **Deny** if the policy will deny rights.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Name:** The name is required and case insensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
3. Choose one of the following methods to add Principals to the Authorization Policy.

- Drag and drop
 - a. Use the Navigation Panel to list the Application's available Principals by performing a search on Users, External Roles or Application Roles. For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
 - b. Drag and drop Principals from the **Search Results** tab into the area labeled **Principals**.
 - c. Select Any or All.

If Any, the user must match at least one of the specified principals. For example, if the principals are roles, the user must be a member of at least one of the roles for the Authorization Policy to apply. If All, the user must match all of the specified principals. For example, if the principals are roles, the user must be a member of all of them for the Authorization Policy to apply.

- Add Principals pop-up search

For details on how to use the pop-up search box, see [Section 5.1, "Searching with the Administration Console."](#)

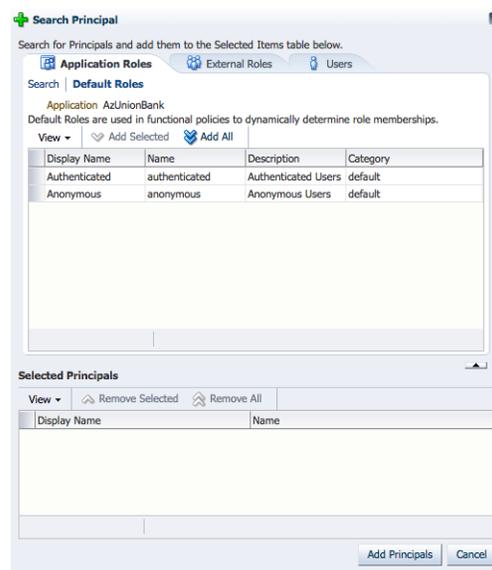
- a. Click **Add** in the **Principals** section.

The **Add Principals** dialog displays.

- b. Select the appropriate tab to search for available Principals.

Options are Application Roles, External Roles and Users. You can navigate between tabs and add as many selected Principal types as desired. The Application Roles tab contains two links: Search and Default Roles. The dialog opens on Search which allows a pop-up Application Role search as explained in [Chapter 5, "Querying Security Objects."](#) By clicking Default Roles, you can add an Anonymous Role or an Authenticated Role to the Principal. (See *Oracle Fusion Middleware Application Security Guide* for detailed descriptions of these roles.) [Figure 4–1](#) is a screenshot of the Default Roles pop up box.

Figure 4–1 Add Default Roles Pop Up



- c. Search for the available Principals by entering a string.
The Principals matching the query are displayed in **Search Results**.
 - d. Select your choice(s) and click Add Selected.
The Principal(s) are added to the Selected Principals. Use **Ctrl+click** to select multiple items from the list.
 - e. Click **Add Principals**.
 - f. Select Any or All.
If Any, the user must match at least one of the specified principals. For example, if the principals are roles, the user must be a member of at least one of the roles for the Authorization Policy to apply. If All, the user must match all of the specified principals. For example, if the principals are roles, the user must be a member of all of them for the Authorization Policy to apply.
4. Choose one of the following methods to add Targets to the Authorization Policy. This step adds either Resource and action associations or Entitlements or both to the Authorization Policy.
- Drag and drop
 - a. Use the Navigation Panel to list the Application's available Resources or Entitlements by performing a search. (Be sure to look for these objects in the same Policy Domain to which you are adding the Authorization Policy.) For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
 - b. Drag and drop one or more Resources or Entitlements from the **Search Results** tab into the area labeled **Targets**. Expanding the added object in **Targets** allows you to associate an action with it.
 - Add Targets pop up search
For details on how to use the pop-up search box, see [Section 5.1, "Searching with the Administration Console."](#)
 - a. Click **Add** in the **Targets** section.
The **Add Targets** dialog displays.
 - b. Select the appropriate tab to search for available Targets.
Options are Entitlements and Resources. You can navigate between tabs and add as many selected Targets as desired.
 - c. Search for available targets under the Entitlements tab by entering a string.
The resources matching the query are displayed in **Search Results**. If no search string was entered, a list of all objects of the specified type is returned.
 - d. Select your choice(s) and click Add Selected.
The Target(s) are added to the Selected Targets. Use **Ctrl+click** to select multiple items from the list.
 - e. Search for available targets under the Resources tab by entering a string.
The resources matching the query are displayed in **Search Results**. If no search string is entered, a list of all objects of the specified type is returned.

Alternately, you can click the Resource Expression link under the Resources tab, select a Resource Type, enter a string expression and click Add to Targets. This will search for targets, using the defined criteria, dynamically at runtime. All Resources that belong to the selected Resource Type that contain the string expression are returned, within the context of the administrator privileges.

f. Click Add Targets.

You will have to select the action for any non-entitlement targets (Resource or Resource Name Expression) added.

5. Select the **Conditions tab to add a condition.**

For more information, see [Section 4.6, "Using the Condition Builder."](#)

6. Select the **Obligations tab.**

An Authorization Policy may have zero, one or more Obligations.

a. Click **New to display the New Obligation dialog.**

b. Provide a Name and an (optional) Display Name and Description for the New Obligation and click Add.

c. Click **New in the Attributes section to add an obligation attribute.**

An Obligation has a set of attributes. Each attribute is a name-value pair. The value can be either static or the value of a previously defined attribute. Each obligation should have at least one attribute. See [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#) for information.

d. Provide a Name for the attribute in the New Obligation Attribute dialog.

If the obligation attribute is static, select one of the Data Types and provide a Value. If the obligation is an attribute, select **Attribute** for Data Type and choose from the list of predefined attributes.

e. Click **Add.**

7. Click **Save to save the Authorization Policy.**

4.5.5.2 Modifying an Authorization Policy

To modify a policy, proceed as follows:

1. Choose from the following methods to display the desired Authorization Policy.

- Expand the information tree in the Navigation Panel to find the Authorization Policies node under the appropriate Application's Policy Domain and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.8, "Searching Authorization Policies."](#)
- In the Home area, select the Application Name under which the Authorization Policy was created and click **Search** under **Authorization Policies**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3.8, "Searching Authorization Policies."](#)

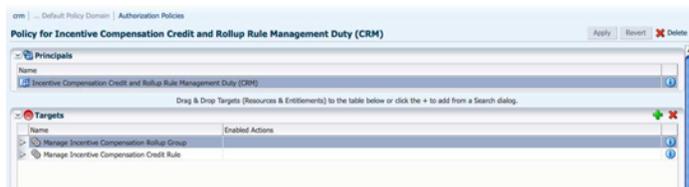
The search results are displayed.

2. Select the correct policy from the displayed search results and click Open to display its details.

In addition to displaying advanced Authorization Policies created using Oracle Entitlements Server, the Administration Console also displays the simpler

Application Grants (system policies) created using Oracle Platform Security Services (OPSS). The OPSS Application Grants can be viewed, modified or deleted only with the Administration Console. When created using OPSS, Application Grants are defined with a principal and target only. [Figure 4–2](#) is a screenshot of the Oracle Entitlements Server screen when an OPSS Application Grant is displayed.

Figure 4–2 OPSS Application Grants Display Screen



Note the Name, Display Name and Description fields are not displayed as they would be if the Authorization Policy was created using Oracle Entitlements Server. OPSS Application Grants cannot be created using Oracle Entitlements Server. For more information on Application Grants, see the *Oracle Fusion Middleware Application Security Guide*.

3. Modify the policy as necessary.
 - Select the Principal to modify.
 - For more information, see [Section 4.5.5.1, "Creating an Authorization Policy."](#)
 - Select (or expand) the Target to modify.
 - For more information, see [Section 4.5.5.1, "Creating an Authorization Policy."](#)
 - Click the Conditions tab to edit conditions.
 - For more information, see [Section 4.6, "Using the Condition Builder."](#)
 - Click the Obligations tab to modify the Obligation or its attributes.
 - To modify the obligation, click **Edit** from the Obligations table, make changes in the displayed dialog and click **Update**.
 - To modify an attribute, select the attribute from the Attributes table and click Edit. Make changes in the displayed dialog and click Update.
 - To delete the Obligation, select it in the Obligations table and click Remove.
4. Click **Apply**.

4.5.5.3 Deleting an Authorization Policy

To delete an Authorization Policy, proceed as follows:

1. Choose from the following methods to display the Authorization Policy search screen.
 - Expand the information tree in the Navigation Panel to find the Authorization Policies node under the appropriate Application's Policy Domain, right-click it and select Open. A search dialog opens in the Home area.

- In the Home area, select the Application Name under which the Authorization Policy was created and click **Search** under **Authorization Policies**. A search dialog opens in the Home area.

For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

2. Enter criteria for the lookup and click Search.
3. Select the appropriate Authorization Policy from the search results and click Remove.

The Administration Console can display advanced Authorization Policies created using Oracle Entitlements Server as well as the simpler Application Grants (system policies) created using Oracle Platform Security Services (OPSS). Either Authorization Policies or Application Grants can be deleted by clicking Remove.

4.5.6 Managing Application Roles in the Role Catalog

Application Roles are defined at the Application level (thus, its name) and created using Oracle Entitlements Server. An Application Role can be assigned to an External Role, user, or group in an identity store, or another Application Role in the policy store. One target application may have several different roles, with each assigned a different set of privileges for more fine-grained authorization. Membership can be granted statically to External Roles or individual users, or dynamically using a Role Mapping Policy that is processed at runtime.

Note: A Role Mapping Policy assigns the role to subjects and an Authorization Policy defines the role's access rights.

You can use Application Roles to control access by establishing relationships with the following procedure:

1. Define Application Roles to represent the functional roles users have in the application.
2. Map each Application Role to External Roles or Users.
3. Create Authorization Policies to provide the level of access rights (Permit/Deny) required to meet the goals of the Application Roles.
4. Add the Application Role as a Principal to one or more Authorization Policies.

Application Roles use role inheritance and hierarchy. The inheritance pattern is such that a subject assigned to a role (using a Role Mapping Policy or static role assignments) also inherits any child roles if it is not prohibited by Role Mapping Policies. When an Application Role is referenced as a Principal in a policy, access to the resource for all users assigned to the role is governed by the policy. The following sections describe management operations on Application Roles.

- [Section 4.5.6.1, "Creating an Application Role"](#)
- [Section 4.5.6.2, "Modifying an Application Role"](#)
- [Section 4.5.6.3, "Mapping External Roles to an Application Role"](#)
- [Section 4.5.6.4, "Mapping an External User to an Application Role"](#)
- [Section 4.5.6.5, "Deleting an Application Role or Removing External Role Mappings"](#)

- [Section 4.5.6.6, "Removing External User Mappings"](#)

4.5.6.1 Creating an Application Role

The following procedure describes the steps to create a new Application Role. You are not required to add members to the role at the same time and can return to the saved role later. To create an Application Role, proceed as follows:

1. Display the page for creating an Application Role by choosing one of the following methods:

- Navigate to the Role Catalog under the appropriate Application node in the Navigation Panel. Right-click the **Role Catalog** node and select **New** from the menu.
- In the Home area, select the Application Name under which the Application Role will be created and click **New** from **Application Roles**.

An Untitled page with four tabs is displayed in the Home area: General (active), Application Role Hierarchy, External Role Mapping and External User Mapping.

2. Provide the following information under the **General** tab.

- **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
- **Role Name:** The name is required and case insensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
- **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
- **Role Category:** A Role Category is a tag you can assign to a role for ease of management. See [Section 4.5.8, "Managing a Role Category."](#)

3. Click **Save**.

The page is renamed to match the entry provided for Role Name and the Application Role Hierarchy, External Role Mapping and External User Mapping tabs become active. At this point, you can create a policy with this Application Role as the Principal or find a policy with this Application Role as the Principal by clicking Create Policies or Find Policies, respectively. To define the Application Role Hierarchy continue to the next step.

4. Optionally, select the **Application Role Hierarchy** tab to define from which roles this Application Role will inherit permissions (Inherits) and to see a list of roles which are inherited by this role (Is Inherited By). Hierarchy is not required but if you choose to define it, the following example sub procedure is specific to the former option.

- a. Click **Inherits**.
- b. Click **Add**.
- c. Select the radio button that corresponds to the role to which you are adding the hierarchy.

When you add roles to the hierarchy, you can either add the roles to the role under which you are working or to a role that you can select in the Application Role Hierarchy table.

- d. Complete the criteria fields in the **Add a Role** dialog and click **Search**.
The results display in the **Search Results** table. Empty strings fetch all roles.
- e. Select the role from which this role will inherit permissions in the **Search Results** table.
Use **Ctrl+click** to select multiple roles.
- f. Click **Add**.
The selected roles display in the **Application Role Hierarchy** tab, and the Application Role inherits permissions from them.

For information about external role mapping, see [Section 4.5.6.3, "Mapping External Roles to an Application Role."](#) For information about external user mapping, see [Section 4.5.6.4, "Mapping an External User to an Application Role."](#)

4.5.6.2 Modifying an Application Role

To modify or view an Application Role, proceed as follows:

1. Choose from the following methods to display the desired Application Role.
 - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application, right-click it and select Open. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Application Roles**. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.

When the correct Application Role is displayed, select it and click Open to display the details in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

2. Select the tab that contains the parameters you want to modify and click Add.

For information on the available tabs, see:

- Application Role Hierarchy: [Section 4.5.6.1, "Creating an Application Role"](#)
- External Role Mapping: [Section 4.5.6.3, "Mapping External Roles to an Application Role"](#)
- External User Mapping: [Section 4.5.6.4, "Mapping an External User to an Application Role"](#)

4.5.6.3 Mapping External Roles to an Application Role

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

1. Choose from the following methods to display the desired Application Role.
 - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Application Roles using the Navigation Panel's search function and double-click the Application Role name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)

- In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Application Roles**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

When the correct Application Role is displayed, select it and click Open to display the details in the Home area.

2. Select the **External Role Mapping** tab.
3. Click **Add** to display the **Add a Role** dialog.
4. Complete the query fields in the **Add a Role** dialog and click **Search**.
Empty strings fetch all roles. The results display in the **External Role Search** table.
5. Select the external role to map to by clicking its name in the table.
Use **Ctrl+click** to select multiple roles.
6. Click **Map Roles**.
The selected roles display in the **External Role Mapping** tab.

4.5.6.4 Mapping an External User to an Application Role

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

1. Choose from the following methods to display the desired Application Role.
 - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application and double click it. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Application Roles using the Navigation Panel's search function and double-click the Application Role name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Application Roles**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

When the correct Application Role is displayed, select it and click Open to display the details in the Home area.

2. Select the **External Users Mapping** tab.
3. Click **Add** to display the **Add a User** dialog.
4. Complete the query fields in the **Add a User** dialog and click **Search**.
Empty strings fetch all roles. The results display in the **External User Search** table.
5. Select the user to map by selecting its name in the table.
Use **Ctrl+click** to select multiple roles.
6. Click **Map Users**.
The selected roles display in the **External User Mapping** tab.

4.5.6.5 Deleting an Application Role or Removing External Role Mappings

To delete an Application Role or remove External Role Mappings from an Application Role, proceed as follows:

1. Choose from the following methods to display the desired Application Role.
 - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application, right-click it and select Open. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Application Roles**. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.

For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

2. Select the Application Role in the Search Results table and:
 - Click Delete to remove the role.
 - Select the appropriate mapping in the External Role Mapping table and click Remove.
 - To remove External User Mappings, see [Section 4.5.6.6, "Removing External User Mappings."](#)

4.5.6.6 Removing External User Mappings

To remove External User Mappings from an Application Role, proceed as follows:

1. Choose from the following methods to display the desired Application Role.
 - Expand the information tree in the Navigation Panel to find the Role Catalog node under the appropriate Application, right-click it and select Open. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Application Roles**. A search dialog opens in the Home area. Enter criteria for the lookup and click Search.

For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

2. Select the Application Role in the Search Results table and click Open.
The Application Role details open in a new tab.
3. Click the External User Mappings tab.
4. Select the appropriate User and click Remove.
A dialog box is displayed asking for confirmation.
5. Click Delete to remove the External User Mapping.

You can also remove External Role Mappings by clicking the External Role Mappings tab.

4.5.7 Managing Role Mapping Policies

Membership to an Application Role can be granted statically or dynamically with a Role Mapping Policy. An Application Role, referenced in a Role Mapping Policy, could

grant a user access to the defined resources. The following sections describe management operations on Role Mapping Policies.

- [Section 4.5.7.1, "Creating a Role Mapping Policy"](#)
- [Section 4.5.7.2, "Modifying a Role Mapping Policy"](#)
- [Section 4.5.7.3, "Deleting a Role Mapping Policy"](#)

4.5.7.1 Creating a Role Mapping Policy

To create a Role Mapping Policy, proceed as follows:

1. Display the page for creating a Role Mapping Policy by choosing one of the following methods:
 - Navigate to the appropriate Application node in the Navigation Panel and expand the Role Catalog branch. Right-click **Role Mapping Policies** and select **New** from the menu.
 - In the Home area, select the Application Name under which the Role Mapping Policy will be created and click **New** from **Role Mapping Policies**.

An Untitled page is displayed in the Home area.

2. Provide the following information.
 - **Effect:** Select **Permit** if the policy will grant membership in the Application Role or **Deny** if the policy will deny membership in the Application Role.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Name:** The name is required and case insensitive.
 - **Description:** Although optional, it is recommended to provide useful information about the policy. The description string is case insensitive.
3. Choose one of the following methods to add Application Roles.
 - Drag and drop
 - a. Use the Navigation Panel to list the Application's available Application Roles by performing a search. For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
 - b. Drag and drop Application Roles from the **Search Results** tab into the area labeled **App Role**.
 - Add Application Roles dialog
 - a. Click **Add** in the **App Role** section.
The **Search Application Roles** dialog displays.
 - b. Search for the available Application Roles by entering a string.
The resources matching the query are displayed in **Search Results**.
 - c. Select the principals to add and click **Add Application Roles**.
Use **Ctrl+click** to select multiple items from the list.

Note: For this release, this dialog displays the Search Principals title and Add Principals button.

4. Choose one of the following methods to add Principals.
 - Drag and drop
 - a. Use the Navigation Panel to list the Application's available Users and External Roles by performing a search. For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
 - b. Drag and drop Users and External Roles from the **Search Results** tab into the area labeled **Principals**.
 - Add Principals dialog
 - a. Click **Add** in the **Principals** section.
The **Search Principals** dialog displays.
 - b. Search for the available Principals (in this case, Users or External Roles) by entering a string.
The resources matching the query are displayed in **Search Results**.
 - c. Select the principals to add and click **Add Principals**.
Use **Ctrl+click** to select multiple items from the list.
5. Optionally, choose one of the following methods to add Resources (also referred to as Targets).
 - Drag and drop
 - a. Use the Navigation Panel to list the Application's available Resources by performing a search. For more information, see [Section 5.2, "Finding Objects with a Simple Search"](#).
 - b. Drag and drop one or more Resources from the **Search Results** tab into the area labeled **Resources**.
 - Add Targets pop up search
 - a. Click **Add** in the **Resources** section.
The **Add Targets** dialog displays.
 - b. Choose the Policy Domain that contains the Resource (if applicable).
 - c. Enter a string and click Search.
The resources matching the query are displayed in **Search Results**. If no search string was entered, a list of all objects of the specified type is returned.
 - d. Select the appropriate Targets to add and click **Add Selected**.
The Target(s) are added to the Selected Targets. Use **Ctrl+click** to select multiple items from the list.
 - e. Click the Resource Expression link to add an expression as a Target.
Select a Resource Type, enter a string expression and click Add to Targets. This will search for targets, using the defined criteria, dynamically at runtime. All Resources that belong to the selected Resource Type that contain

the string expression are returned, within the context of the administrator privileges.

f. Click **Add Targets**.

6. See [Section 4.6, "Using the Condition Builder"](#) for information on using the Condition Builder.
7. Click Save.

4.5.7.2 Modifying a Role Mapping Policy

To modify a Role Mapping Policy, proceed as follows:

1. Choose from the following methods to display the desired Role Mapping Policy.
 - Expand the information tree in the Navigation Panel to find Role Mapping Policies under the Role Catalog node of the appropriate Application and double click Role Mapping Policies. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Role Mapping Policies**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

When the correct Role Mapping Policy is displayed, select it and click Open to display the details in the Home area.

2. Modify the policy as necessary.
3. Click Apply.

4.5.7.3 Deleting a Role Mapping Policy

To delete a Role Mapping Policy, proceed as follows:

1. Choose from the following methods to display the desired Role Mapping Policy.
 - Expand the information tree in the Navigation Panel to find Role Mapping Policies under the Role Catalog node of the appropriate Application and double click Role Mapping Policies. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - In the Home area, select the Application Name under which the Application Role was created and click **Search** under **Role Mapping Policies**. A search dialog opens in the Home area. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

When the correct Role Mapping Policy is displayed, select it and click Open to display the details in the Home area.

2. Double-click the Role Mapping Policy to delete.
The Role Mapping Policy displays in the Home area.
3. Click Delete in the upper right corner of the Home area.

4.5.8 Managing a Role Category

A Role Category is a tag you can assign to a role for ease of management. You can create or delete a Role Category but you cannot modify them. To create a Role

Category, proceed as follows. Instructions to delete a Role Category are detailed after the final step.

1. Expand the appropriate Application node in the Navigation Panel and double-click the **Roles Categories** node.



The Role Categories page opens in the Home area.

2. Click **New** to display the **New Category** dialog.
3. Provide the following information.
 - **Name**
 - **Display Name**
 - **Description**

 A dialog box titled 'New Category' with a close button in the top right. It contains three text input fields:

- * Name: New Role Category
- Display Name: Manager Roles
- Description: All manager roles

 At the bottom of the dialog are two buttons: 'Create' and 'Cancel'.

4. Click **Create**.

The new category displays in the Role Categories list.



To delete a Role Category, expand the appropriate Application node in the Navigation Panel and double-click the **Roles Categories** node. Select the Role Category to delete and click Delete.

4.5.9 Managing Attributes and Functions as Extensions

Attributes and Functions are definitions organized under the Extensions node of the Application for which they were created. Attribute and function definitions can be used in a Condition or an Obligation. In regards to a Condition, attribute and function definitions can be used to make an optional expression that can be added to a policy to further restrict access to the protected resource. In regards to an Obligation, this optional set of name-value pairs returns additional information, with a policy decision, to the calling application. There are two ways to define an Obligation:

- Statically where an attribute with an absolute value is returned.
- Dynamically where an attribute value, or a custom function, is evaluated at runtime and the output is returned.

An Attribute can be a value dynamically defined at runtime (for example, the locality of the user) or a value based on the type of protected resource (for example, creation date of a text file). During policy evaluation, attribute values can be passed in by the application or Oracle Entitlements Server can retrieve it using a custom attribute retriever. Attributes must have a defined type. Boolean, integer, date, time and string are Oracle Entitlements Server predefined types. An attribute may be singular or a multi-valued list. A Function is a definition of externally implemented logic. It can be added to a policy as a condition on the policy's outcome. The following sections describe management operations on Attributes and Functions.

- [Section 4.5.9.1, "Creating an Attribute"](#)
- [Section 4.5.9.2, "Modifying an Attribute"](#)
- [Section 4.5.9.3, "Deleting an Attribute"](#)
- [Section 4.5.9.4, "Creating a Function"](#)
- [Section 4.5.9.5, "Modifying a Function"](#)
- [Section 4.5.9.6, "Deleting a Function"](#)

4.5.9.1 Creating an Attribute

To create an attribute, proceed as follows:

1. Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel.
2. Right-click the **Attributes** node and select **New** from the menu.
An Untitled page is displayed in the Home area.
3. Provide the following information for the attribute.
 - **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Name:** The name is required and case insensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
 - **Category:** Select from Resource and Dynamic as a value for this required parameter. A Resource attribute is defined and maintained using Oracle Entitlements Server. All other attributes would be Dynamic.
 - **Type:** Select from Boolean, Date, Date Time, Integer, String, Time, Base64 Binary, Day Time Duration, DNS Name, Double, Email, Hex Binary, IP Address, URI, X500 Name or Year Month Duration.
 - **Input Values:** Select from Single and Multiple.
4. Select one of the following from the Save menu.
 - **Save** saves the configuration and renames the tab with the value provided for the Display Name.

- **Save and Close** saves the configuration and closes the tab.
- **Save and Create Another** saves the configuration to the policy store, refreshes the information tree in the Navigation Panel and leaves an Untitled area open for you to create another Attribute.

4.5.9.2 Modifying an Attribute

To modify an attribute, proceed as follows:

1. Choose from the following methods to display the desired Attribute.
 - Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel. Double-click Attributes to open a search dialog in the Home area. For information about searching in the Home area, see [Section 5.3.9, "Searching Attributes."](#)
 - Search for Attributes using the Navigation Panel's search function and double-click the Attribute name in the Search Results tab. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)

When the correct Attribute is displayed, select it and click Open to display the details in the Home area.

2. Modify the attribute as necessary.
3. Click **Apply**.

4.5.9.3 Deleting an Attribute

To delete an attribute, proceed as follows:

1. Choose from the following methods to display the Attribute.
 - Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel. Right-click Attributes and select Open to display a search dialog in the Home area. Enter criteria for the lookup and click Search. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
 - Search for Attributes using the Navigation Panel's search function, right-click the Attribute name in the Search Results tab and select Open to display the Attribute in the Home area. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
2. Select the Attribute and click **Delete**.

A Delete Warning is displayed.
3. Click Yes.

If the Attribute is being used, it cannot be deleted.

4.5.9.4 Creating a Function

To create a function, proceed as follows:

1. Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel.
2. Right-click the **Functions** node and select **New** from the menu.

An Untitled page is displayed in the Home area.
3. Provide the following information for the function.

- **Display Name:** The display name is optional and case insensitive. Specifying a meaningful display name is recommended since it is displayed in the Administration Console, and provides extra information to help administrators identify objects.
 - **Name:** The name is required and case insensitive. At runtime, this is the string the application passes to determine whether a user is authorized to access this Resource.
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement. The description string is case insensitive.
 - **Function Class Name:** The name of the class that provides the functionality.
If creating a custom function implemented from the `InspectableOesFunction` interface, Oracle Entitlements Server will load the metadata based on the interface and dynamically evaluate the class to ensure its viability. See the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* for details.
 - **Input Parameter:** A list of the types of parameters passed to the function.
 - **Return Type:** Select the data type returned by the function.
 - **Syntax Preview** displays a preview of the function's syntax.
4. Select one of the following from the Save menu.
 - **Save and Close** saves the configuration and renames the page with the value provided for the Display Name.
 - **Save and Create Another** saves the configuration to the information tree in the Navigation Panel but leaves the Untitled area open for you to create another.

4.5.9.5 Modifying a Function

To modify a function, proceed as follows:

1. Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel.
2. Double-click Functions to open a search dialog in the Home area.
3. Enter search criteria to display the Function.

For information about searching in the Home area, see [Section 5.3.10, "Searching Functions."](#)

4. Select the Function from the Search Results and click Open.
The Function's details are displayed in the Home area.
5. Modify the Function as necessary.
6. Click **Apply**.

4.5.9.6 Deleting a Function

To delete a Function, proceed as follows:

1. Choose from the following methods to display the Function.
 - Navigate to, and expand, Extensions under the appropriate Application node in the Navigation Panel. Right-click Functions and select Open to display a search dialog in the Home area. Enter criteria for the lookup and click Search.

Select the appropriate Function from the Search Results. For information about searching in the Home area, see [Section 5.3, "Finding Objects with an Advanced Search."](#)

- Search for Functions using the Navigation Panel's search function, right-click the Function name in the Search Results tab and select Open to display the Function in the Home area. For information about searching in the Navigation Panel, see [Section 5.2, "Finding Objects with a Simple Search."](#)
2. Click Delete.
A Delete Warning is displayed.
 3. Click Yes.
If the Function is being used, it cannot be deleted.

4.6 Using the Condition Builder

An optional Condition in a policy rule can be used to further evaluate the applicability of an authorization decision returned in response to a request for access. For example, a Condition can be used to grant access to a resource only on the condition that the request was issued from a specific location or at a specific time.

Note: Conditions in Role Mapping Policies provide the same functionality, and take the same format, as conditions in Authorization Policies.

A Condition is written in the form of an expression that resolves to either true or false. If the expression resolves to true, the condition is satisfied and the policy is applicable. If the expression does not resolve to true, the policy is not applicable. The expression can operate on attributes, functions or literals. Oracle Entitlements Server contains predefined attributes and functions that can be inserted or you can create custom ones. The literals belong to the supported data types and are constants.

Note: All Attributes and Functions (both custom and predefined) are created, collected and further managed under the Extensions node of the Application. For more information, see [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#)

The Condition Builder allows an administrator to quickly create Condition expressions that can then be added to an Authorization Policy or a Role Mapping Policy. The following procedure illustrates how to use the Condition Builder to create a Condition for your policy. To create a Condition, you either create or modify an Authorization Policy or a Role Mapping Policy. Following one of these procedures will bring you to a step in which you can build a Condition.

- [Section 4.5.5.1, "Creating an Authorization Policy"](#)
- [Section 4.5.5.2, "Modifying an Authorization Policy"](#)
- [Section 4.5.7.1, "Creating a Role Mapping Policy"](#)
- [Section 4.5.7.2, "Modifying a Role Mapping Policy"](#)

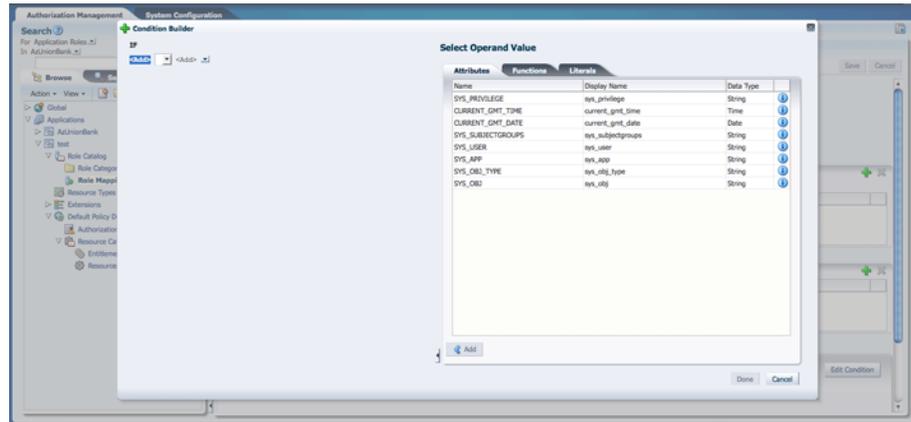
When you get to the appropriate screen, follow this procedure.

1. Click the Condition tab.

- Click Edit Condition.

The Condition Builder (as displayed in Figure 4–3) displays. Note the Condition expression on the left contains two **Add** replaceables and an operator drop down (which is empty until an operand has been added). Build the expression by adding components from the Attributes, Functions and Literals tabs on the right.

Figure 4–3 The Condition Builder



- Click the appropriate Operand Value tab that contains the component type you want to add to the Condition.

Figure 4–4 is a screen shot of the Attributes, Functions and Literals tabs. The Attributes and Functions listed in these tabs are filtered based on the Application in which the policy is being created. For example, a custom Function created within Application 1 will not be visible when the Condition Builder is activated to create a policy within Application 2.

Figure 4–4 Operand Value Tabs



Note: If accessing the Functions tab to add a custom function implemented from the `InspectableOesFunction` interface, Oracle Entitlements Server will dynamically evaluate the values entered based on how the interface is implemented. See the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* for details.

4. Select the line that contains the component you want to add to the Condition and click Add.

Click the blue **i** to display a Details box with more information regarding the component. Figure 4–5 is a screenshot after having added a SYS_APP attribute which takes a string value.

Figure 4–5 Adding a Literal to the Condition



5. Populate the value on the right of the expression by selecting the appropriate Operand Value and click Add.
6. Specify the operator on the right of the Condition Builder by clicking the drop down and selecting your choice.
The operator options are dependent on the Operand Value.
7. Add additional expressions by clicking the last arrow in the expression and selecting AND, OR or NOT from the drop down menu, if applicable.
REMOVE will clear the expression of all components so you may begin again.
8. Select components for the additional expression from the appropriate Operand Value tabs, if applicable.
You may add as many expressions (and components) as necessary by clicking the last arrow in the current expression and selecting from the Operand Value tabs.
9. Click Done to complete the Condition.

The following points should be taken into account as you navigate the Condition Builder to create your expression.

- The Condition Builder contains Tool Tips on most fields for additional details.
- Click the appropriate blue **i** for information on the Operand Value.
- At the minimum, an expression must contain two operands and an operator.
- You can compare an Attribute and an Attribute, an Attribute and a Function, an Attribute and a Literal, a Function and a Function, and a Function and a Literal.
- The input parameters for Functions can be Attributes, Literals or Functions.
- The choice of operators displayed is directly related to the first operand chosen. For example, you cannot do less than or equal to on a string.
- The choice of a second Operand Values displayed within an expression is also directly related to the first operand chosen.
- REMOVE clears the expression to which it is tied of all components so you may begin again. It does not clear the entire Condition.
- The completed Condition (expression) is evaluated by Oracle Entitlements Server at runtime. The interpretation is governed by the rules of precedence.
- The outcome of this Condition must be a boolean.

The following sections contain procedures for more complex conditions.

- [Section 4.6.1, "Building a Complex Expression"](#)
- [Section 4.6.2, "Passing Parameters to Functions"](#)

4.6.1 Building a Complex Expression

This procedure explains how you might build a complex expression using parenthesis.

1. Follow one of these procedures to bring you to the Condition Builder.
 - [Section 4.5.5.1, "Creating an Authorization Policy"](#)
 - [Section 4.5.5.2, "Modifying an Authorization Policy"](#)
 - [Section 4.5.7.1, "Creating a Role Mapping Policy"](#)
 - [Section 4.5.7.2, "Modifying a Role Mapping Policy"](#)

2. Click the Condition tab.
3. Click Edit Condition.

The Condition Builder displays as in [Figure 4-3](#).

4. Click the Attributes tab.
5. Select the `DateAttr` custom attribute and click Add.

`DateAttr` is not a predefined Oracle Entitlements Server attribute so this step assumes a custom attribute has been defined as documented in [Section 4.5.9, "Managing Attributes and Functions as Extensions."](#) `DateAttr` is added to the left of the operator.

6. Select the equal sign (=) as the operator.
7. Select the `CURRENT_GMT_DATE` predefined attribute and click Add.

`CURRENT_GMT_DATE` is a predefined Oracle Entitlements Server attribute and can be viewed under the Attributes tab. It is added to the right of the operator.

8. Add more complexity to the Condition by selecting the appropriate AND, OR or NOT operation at the end of the line of code.

Parentheses must match; there must be an equal number of open and closing parentheses. If you select an operation at the end of a line of code, the operation will involve the code itself. If you select an operation at the end of the entire Condition, it will allow you to add on to the Condition as a whole.

9. Add additional conditions by choosing values from Attributes, Functions or Literals as necessary.
10. Click Done when finished.

4.6.2 Passing Parameters to Functions

This procedure describes how to pass parameters into a Function.

Note: If adding a custom function implemented from the `InspectableOesFunction` interface, Oracle Entitlements Server will evaluate the class on the fly to ensure its viability. See the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server* for details.

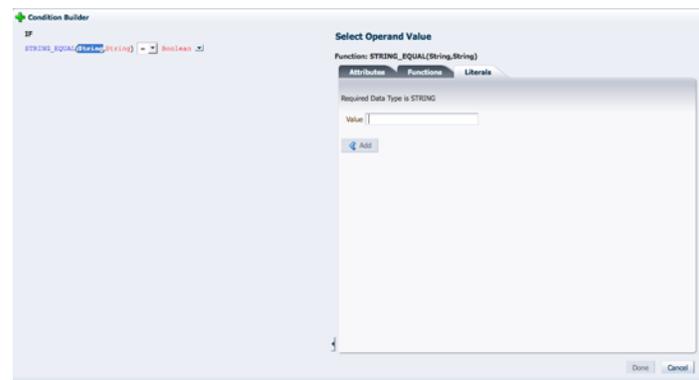
1. Follow one of these procedures to bring you to the Condition Builder.
 - Section 4.5.5.1, "Creating an Authorization Policy"
 - Section 4.5.5.2, "Modifying an Authorization Policy"
 - Section 4.5.7.1, "Creating a Role Mapping Policy"
 - Section 4.5.7.2, "Modifying a Role Mapping Policy"
2. Click the Condition tab.
3. Click Edit Condition.

The Condition Builder displays as in Figure 4–3.

4. Click the Functions tab.
5. Select STRING_EQUAL and click Add.

Figure 4–6 illustrates an added Function and contains placeholders for the two parameters that must be passed to it. This Function will compare the two strings (one the value of a predefined attribute).

Figure 4–6 Adding a Function



6. Select the first parameter if not already.
7. Click the Attributes tab.
8. Select SYS_USER and click Add.

The second parameter is highlighted and the Literal tab is activated.
9. Enter a value for the second parameter and click Add.

For this example, joe. The boolean to the right of the operator is highlighted and the Literal tab is activated.
10. Choose the appropriate operator.
11. Click the Boolean replaceable and select whether this function output should be true or false.
12. Add Additional operands as you see fit.
13. Click Done when finished.

Querying Security Objects

Oracle Entitlements Server enables querying for policies and policy objects from within the Oracle Entitlements Server Administration Console. This chapter explains the types of search functionality and for what purposes they can be used. It contains the following topics.

- Section 5.1, "Searching with the Administration Console"
- Section 5.2, "Finding Objects with a Simple Search"
- Section 5.3, "Finding Objects with an Advanced Search"
- Section 5.4, "Understanding Case Sensitivity in Object Names"

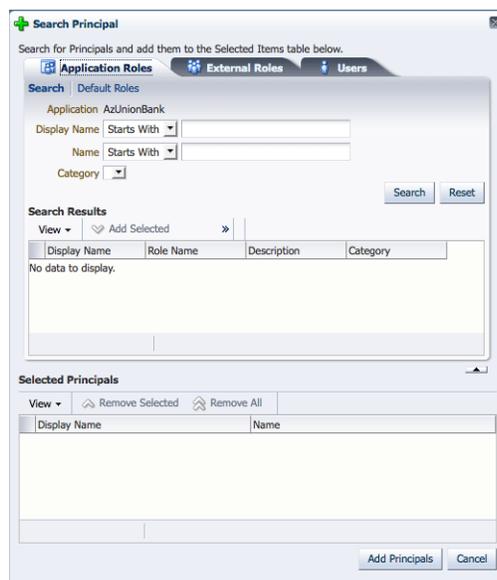
5.1 Searching with the Administration Console

Oracle Entitlements Server enables different kinds of search queries using the Administration Console.

- A *simple search* matches names and display names only. The search is generated from the top of the Navigation Panel and results are displayed in the Navigation Panel. For more information, see [Section 5.2, "Finding Objects with a Simple Search."](#)
- An *advanced search* uses operators that enable more sophisticated matching. The advanced search screen is launched by double-clicking an object in the Navigation Panel, or from the Home area. The search box opens in the Home area and results are also displayed there. For more information, see [Section 5.3, "Finding Objects with an Advanced Search."](#)
- A *blind search* will search objects without specifying search criteria. This can be done as a simple search or an advanced search. A blind search will display no more than 300 objects in the system. Oracle Entitlements Server will not display more than 300 rows in the search results.
- A *pop-up search* opens from within the Authorization Policy or Role Mapping Policy screens, when the policy is being created or modified, by clicking the green Add button (plus sign). The pop-up search box uses a shopping cart paradigm. You add choices selected from the multiple, displayed tabs on the top of the search box to the Selected box on the bottom of the search box. All choices in the Selected box are added when you click Add.

[Figure 5-1](#) is a screen shot of the pop-up search box for adding a Principal. You can click between the three tabs (Application Roles, External Roles, and Users), selecting one or more policy subjects and adding them to the Selected Principals box. When you click Add Principals, all choices added from all tabs will then be added to the policy.

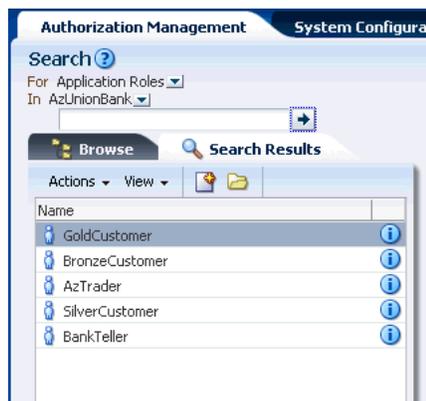
Figure 5–1 Pop-up Search Box



5.2 Finding Objects with a Simple Search

A simple query matches names and display names only. The fields in the top portion of the Authorization Management tab in the Navigation Panel, as shown in [Figure 5–2](#), are used to specify simple queries.

Figure 5–2 Simple Search Fields and Results Tab in Navigation Panel



To specify a simple search, proceed as follows:

1. Select the policy object for which you are searching from the **For** list.

The following object types are available:

- Application Roles
- External Roles
- Users
- Resources
- Resource Types

- Entitlements
 - Attributes
2. Select the search scope from the **In** list.

The *search scope* defines the level at which the search will take place. When searching for Application Roles, Resources, Resource Types, Entitlements and Attributes, the search scope is an Application. For External Roles and Users, the search scope can be Global (the default option) or the name of an Application bound to a particular Identity Directory Service profile.

Note: In the latter case, the search will be in the identity data store that corresponds to the Identity Directory Service profile to which the Application is bound. See [Section 10.3, "Configuring Identity Directory Service Profiles"](#) for more information.

For Entitlements and Resources, the search scope is the Policy Domain within an Application. If performing a Resource search, you also select the Resource Type from the **Type** list.

3. Optionally, enter a string to match in the text box.
Wildcard characters percent (%) and asterisk (*) are supported for a simple search.
4. Click the arrow icon next to the text box to begin the search.
Names and display names matching the specified criteria are returned and displayed in the **Search Results** tab. If no search string was entered, a list of all objects of the specified type is returned.
5. Double-click the object to edit, right click the object and select New to create, or click the object's information icon for details.

For more information on managing policy objects, see [Chapter 4, "Managing Policies and Policy Objects."](#)

5.3 Finding Objects with an Advanced Search

An advanced search is generally initiated by double-clicking the object name in the Navigation Panel, or from the Search link for the object in the Home area. An advanced search can use the following operators:

- Starts with
- Ends with
- Contains
- Equal to

There is no support for wildcard characters in an advanced search. In particular, the asterisk (*) or percent (%) characters are treated as plain text in any advanced search parameter. The following sections have information on searching for policy objects with an advanced search.

- [Section 5.3.1, "Searching External Roles"](#)
- [Section 5.3.2, "Searching Applications"](#)
- [Section 5.3.3, "Searching Resource Types"](#)
- [Section 5.3.4, "Searching Application Roles"](#)

- Section 5.3.5, "Searching Role Mapping Policies"
- Section 5.3.6, "Searching Resources"
- Section 5.3.7, "Searching Entitlements"
- Section 5.3.8, "Searching Authorization Policies"
- Section 5.3.9, "Searching Attributes"
- Section 5.3.10, "Searching Functions"
- Section 5.3.11, "Searching for Users"

5.3.1 Searching External Roles

To search External Roles, proceed as follows:

1. Select from the following methods to display the Search External Roles page:
 - In the Navigation Panel, expand Global and double-click External Roles. Alternately, right-click External Roles and select Open.
 - In the Home area, click **Search - External Roles** from the Search and Create section.
2. Enter the following query parameters:
 - **Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.Optionally, select from the **Saved Search** drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select **Personalize...** to set options for previously saved searches.
3. Optionally, click **Save...** to name the current query parameters. The named search is added to the **Saved Search** list.
4. Click **Search**. The results are displayed in Search Results.

5.3.2 Searching Applications

To search applications, proceed as follows:

1. Select from the following methods to display the Search Applications page:
 - In the Navigation Panel, double-click Applications to display the Search Applications page. Alternately, right-click Applications and select Open.
 - In the Home area, click **Search - Applications** from the Search and Create section.
2. Enter the following query parameters:
 - **Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.Optionally, select from the **Saved Search** drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select **Personalize...** to set options for previously saved searches.

3. Optionally, click Save... to save the current query parameters as a Saved Search. The search is added to the Saved Search list.
4. Click Search. The results are displayed in Search Results.

5.3.3 Searching Resource Types

To search Resource Types, proceed as follows:

1. Select from the following methods to display the Search Resource Types page as in Figure 5-3.
 - In the Navigation Panel, expand the Application node and double-click Resource Types. Alternately, right-click Resource Types and select Open.
 - In the Home area, select the appropriate Application Name and click Search under Resource Types.

Figure 5-3 Searching for Resource Types



2. Enter the following query parameters:
 - **Display Name:** Select an operator from the list and enter a string to match.
 - **Name:** Select an operator from the list and enter a string to match.
 - **Actions:** Select an operator from the list and enter a string to match.

Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.

3. Optionally, click Save... to save the current query parameters as a Saved Search. The search is added to the Saved Search list.
4. Click Search.

All results matching the query specifications are displayed in the **Search Results** table as illustrated in Figure 5-4.

Figure 5-4 Resource Type Search Results

| Search Results | | | |
|--|---------------------------|---------------------------|-------------|
| A limit of 300 resource types are shown below. | | | |
| Display Name | Name | Description | Actions |
| DataSecResourceType | DataSecResourceType | DataSecResourceType | view |
| UINavigationResource | UINavigationResource | UINavigationResource | view |
| UIWidgetResource | UIWidgetResource | UIWidgetResource | view |
| AccountUpdateResourceType | AccountUpdateResourceType | AccountUpdateResourceType | update |
| TradeWidgetType | TradeWidgetType | TradeWidgetType | trade, view |
| MutualFundsAssetClsType | MutualFundsAssetClsType | MutualFundsAssetClsType | view |

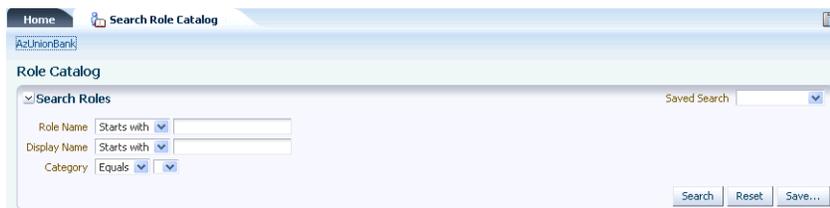
5.3.4 Searching Application Roles

To search Application Roles, proceed as follows:

1. Select from the following methods to display the Search Role Catalog page.
 - In the Navigation Panel, expand Applications and the named Application node applicable to the search, and double-click Role Catalog.
Alternately, right-click Role Catalog and select Open.
 - In the Home area, select the Application Name and click Search from Application Roles.

The Search Role Catalog tab is displayed as in [Figure 5-5](#).

Figure 5-5 Searching for Application Roles in a Role Catalog



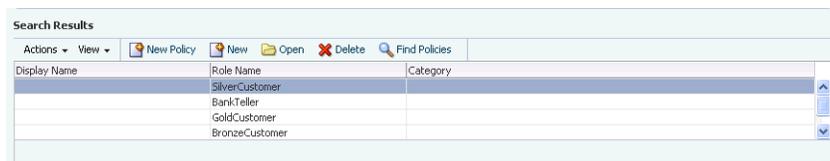
2. Enter the following query parameters:
 - **Role Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.
 - **Category:** Select a Role Category from the list. (Oracle Entitlements Server only supports an *equals* search for Role Category.)

Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.

3. Optionally, click Save... to save the current query parameters as a Saved Search. The search is added to the Saved Search list.
4. Click Search.

All results matching the query specifications are displayed in the **Search Results** table as in [Figure 5-6](#).

Figure 5-6 Application Role Search Results



5.3.5 Searching Role Mapping Policies

1. Select from the following methods to display the Search Role Mapping Policies page:

- In the Navigation Panel, expand Applications and the named Application node applicable to the search, and double-click Role Mapping Policies.
Alternately, right-click Role Mapping Policies and select Open.
- In the Home area, select the Application Name and click Search from Role Mapping Policies.

The Search Role Policies page is displayed as in [Figure 5-7](#).

Figure 5-7 Searching for Role Mapping Policies



2. In the Search section, enter the query parameters as follows:
 - **Effect:** Select the policy effect (Grant/Deny) from the list.
 - **Display Name:** Select an operator from the list and enter a string to match.
 - **Name:** Select an operator from the list and enter a string to match.
 - **Role:** Select an operator from the list and enter a string to match.
 - **Principal:** Select an operator from the list and enter a string to match.
 - **Target:** Select an operator from the list and enter a string to match.
3. Click Search.

All results matching the query specifications are displayed in the **Search Results** table as in [Figure 5-8](#).

Figure 5-8 Role Mapping Policy Search Results

| Search Results | | | | | | |
|------------------------------|-----------------------|-----------------------|----------------|---------------|-----------|------------|
| Actions View New Open Remove | | | | | | |
| Effect | Name | Description | Roles | To Principals | Resources | Constraint |
| 1 | GoldCustomerMapRule | GoldCustomerMapRule | GoldCustomer | Siva | | |
| 2 | SilverCustomerMapRule | SilverCustomerMapRule | SilverCustomer | Siva | | |
| 3 | BronzeCustomerMapRule | BronzeCustomerMapRule | BronzeCustomer | Siva | | |

5.3.6 Searching Resources

A Resource can be hierarchical (a scenario in which the sub resource inherits attributes from the parent resource) or non-hierarchical. If a Resource is hierarchical, its tiered-organization is shown in the Search results. To search Resources, proceed as follows:

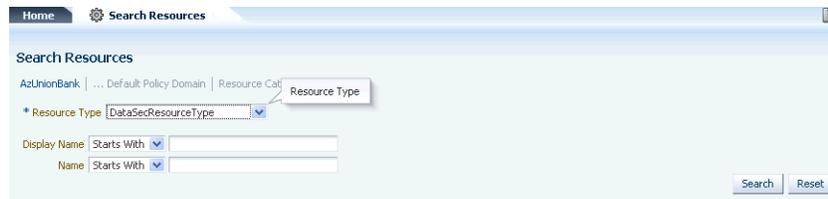
1. Select from the following methods to display the Search Resources page:
 - In the Navigation Panel, expand Applications and the named Application node applicable to the search. Expand the appropriate Policy Domain and Resource Catalog and double-click Resources.

Alternately, right-click Resources and select Open.

- In the Home area, select the Application Name and click Search from Resources.

The Search Resources page is displayed as in [Figure 5–9](#).

Figure 5–9 Searching for Resources



2. Enter the following query parameters:
 - **Resource Type:** Select a resource type from the list. This parameter is required.
 - **Display Name:** Select an operator from the list and enter a string to match.
 - **Name:** Select an operator from the list and enter a string to match.
3. Click Search.

All results matching the query specifications are displayed in the **Search Results** table.

5.3.7 Searching Entitlements

To search Entitlements, proceed as follows:

1. Select from the following methods to display the Search Entitlements page:
 - In the Navigation Panel, expand Applications and the named Application node applicable to the search. Expand the appropriate Policy Domain and Resource Catalog and double-click Entitlements.
Alternately, right-click Entitlements and select Open.
 - In the Home area, select the Application Name and click Search from Entitlements. (In this case, the search is done only within the Default Policy Domain.)

The Search Entitlements tab is displayed in the Home area as in [Figure 5–10](#).

Figure 5–10 Searching for Entitlements



2. Enter the following query parameters:
 - **Entitlement Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.

- **Resource name:** Select an operator from the list and enter a string to match. Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.
3. Optionally, click Save... to save the current query parameters as a Saved Search. The search is added to the Saved Search list.
 4. Click Search.

All results matching the query specifications are displayed in the Search Results table.

5.3.8 Searching Authorization Policies

Authorization Policies can be searched by specifying a policy name, a principal, or a target. To search Authorization Policies, proceed as follows:

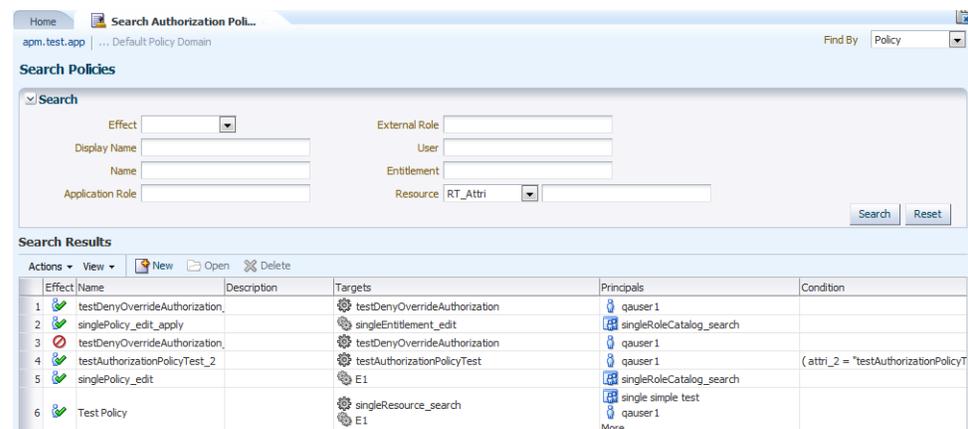
1. Select from the following methods to display the Search Policies page:
 - In the Navigation Panel, expand Applications and the named Application node applicable to the search. Expand the appropriate Policy Domain and Resource Catalog and double-click Authorization Policies.

Alternately, right-click Authorization Policies and select Open.
 - In the Home area, select the Application Name, and click Search under Authorization Policies. (In this case, the search is done within the Default Policy Domain.)

The Search Policies tab is displayed.

The Search Policies tab is displayed in [Figure 5–11](#).

Figure 5–11 Searching Policies



2. Select the search type from the Find By list.

The query parameters change according to the selection. Options include Policy, Principal or Target.

[Figure 5–11](#) is a screenshot in which Policy is selected. [Figure 5–12](#) is a screenshot in which Target is selected.

Figure 5–12 Searching Polices by Target

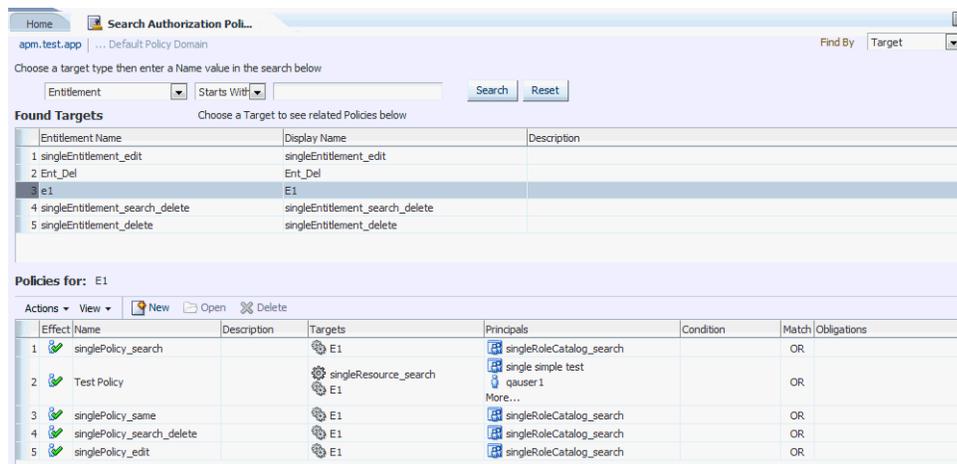
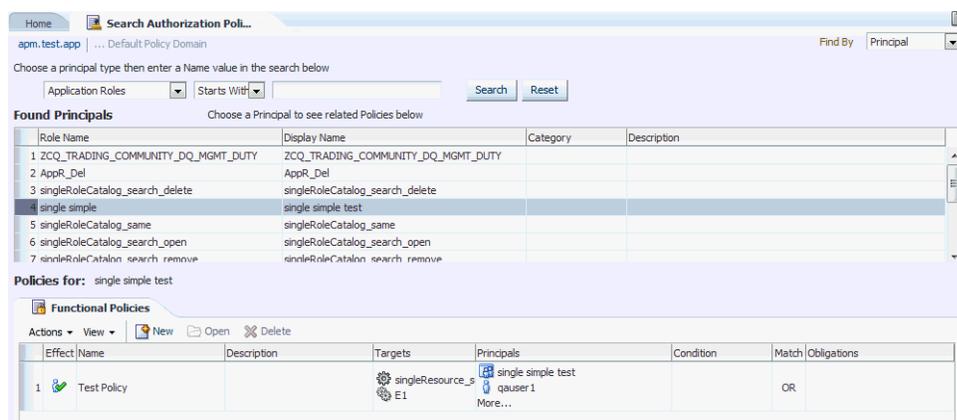


Figure 5–13 is a screenshot in which Principal is selected.

Figure 5–13 Searching Polices by Principal



3. Search using the option based on your previous selection.
 - To Find By: Policy, enter the following query parameters:
 - **Effect:** Select the policy effect (Grant/Deny) from the list.
 - **Display Name:** Enter a string to match. The search allows wildcard operators such as begins with, ends with, and contains.
 - **Name:** Enter a string to match. The search allows wildcard operators such as begins with, ends with, and contains.
 - **Application Role:** Enter a string to match. A drop-down list of suggested application roles is displayed if the beginning characters match. The string entered must exactly match an application role.
 - **External Role:** Enter a string to match. A drop-down list of suggested external roles is displayed if the beginning characters match. The string entered must exactly match an external role.
 - **User:** Enter the string to match. A drop-down list of suggested users is displayed if the beginning characters match. The string entered must exactly match a user.

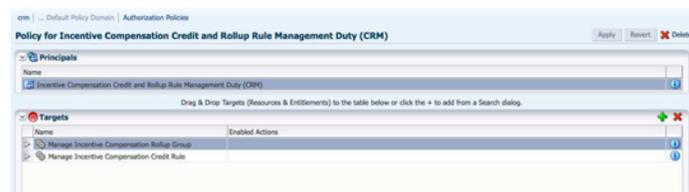
- **Entitlement:** Enter the string to match. A drop-down list of suggested entitlements is displayed if the beginning characters match. The string entered must exactly match an entitlement.
- **Resource:** Select an operator from the list and enter the string to match. A drop-down list of suggested resources is displayed if the beginning characters match. The string entered must exactly match a resource.
- To Find By: Principal or Find By: Target, select an operator from the list, and enter a string to match.

A Resource Type must be provided if the Resource or Resource Type operator is selected.

4. Click Search.

The Administration Console can display Authorization Policies created using Oracle Entitlements Server as well as the simpler Application Grants (system policies) created using Oracle Platform Security Services (OPSS). The OPSS Application Grants can be displayed for viewing, modification and deletion only. When created using OPSS, Application Grants are not given a policy name or description; they are defined with a principal and target only. Figure 5–14 is a screenshot of the Oracle Entitlements Server screen when an OPSS Application Grant is displayed.

Figure 5–14 OPSS Application Grants Display Screen



Note the Name, Display Name and Description fields are not displayed as they would be if the Authorization Policy was created using Oracle Entitlements Server. OPSS Application Grants can only be removed or modified with Oracle Entitlements Server; they cannot be created using Oracle Entitlements Server. For more information on Application Grants, see the *Oracle Fusion Middleware Application Security Guide*.

5.3.9 Searching Attributes

To search Attributes, proceed as follows:

1. In the Navigation Panel, expand Applications and the named Application node applicable to the search.
2. Expand Extensions and double-click Attributes to display the Search Attributes page.

Alternately, right-click Attributes and select Open.

3. Enter the following query parameters.
 - **Display Name:** Select an operator from the list and enter a string to match.
 - **Name:** Select an operator from the list and enter a string to match.

- **Type:** Select an operator from the list and enter a string to match.
Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.
- 4. Optionally, click Save... to save the current query parameters as a Saved Search.
The search is added to the Saved Search list.
- 5. Click Search.

5.3.10 Searching Functions

To search application functions, proceed as follows

1. In the Navigation Panel, expand Applications and the named Application node applicable to the search.
2. Expand Extensions and double-click Functions to display the Search Functions page.
Alternately, right-click Functions and select Open.
3. Enter the following query parameters.
 - **Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.
Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.
4. Optionally, click Save... to save the current query parameters as a Saved Search.
The search is added to the Saved Search list.
5. Click Search.

5.3.11 Searching for Users

To search for Users, proceed as follows:

1. Select from the following methods to display the Search External Roles page:
 - In the Navigation Panel, expand Global and double-click Users. (Alternately, right-click Users and select Open.)
 - In the Home area, click Search - Users from the Search and Create section.
2. Enter the following query parameters:
 - **User Name:** Select an operator from the list and enter a string to match.
 - **Display Name:** Select an operator from the list and enter a string to match.
Optionally, select from the Saved Search drop-down list of previously saved searches. Its query parameters automatically populate the search fields. Select Personalize... to set options for previously saved searches.
3. Optionally, click Save... to save the current query parameters as a Saved Search.
The search is added to the Saved Search list.
4. Click Search.
The results are displayed in Search Results.

5.4 Understanding Case Sensitivity in Object Names

This section provides information regarding the case sensitivity of names that define policy objects. The objects below are case sensitive. Those not listed are case insensitive.

- Principal (defined for an Administration Role or an Application Role)
- Grant Action
- Permission Class Name
- Resource Name
- Resource Type
- Resource Action
- Resource Name Expression
- Resource Type Resource Matcher
- Policy Action
- Policy Grantee

See [Chapter 2, "Understanding the Policy Model"](#) for information on the policy objects.

Managing Policy Distribution

Policy distribution is the process of distributing configured policies and policy objects from the Oracle Entitlements Server Administration Server to specified Security Modules. After a successful policy distribution, each Security Module to which the data was distributed can evaluate requests for access without the Administration Server being online. Evaluation of the policies will produce a *grant* or *deny* authorization decision in answer to a request for access. This chapter contains the following sections.

- Section 6.1, "Defining Distribution Modes"
- Section 6.2, "Understanding Policy Distribution"
- Section 6.3, "Distributing Policies"
- Section 6.4, "Using Default or Third Party Digital Certificates"
- Section 6.5, "Debugging Policy Distribution"

6.1 Defining Distribution Modes

The Oracle Entitlements Server Policy Distribution Component handles the task of distributing policies to individual Security Modules that protect applications and services. Policy data is distributed in either a *controlled* manner or a *non-controlled* manner. The distribution mode is defined in the `jps-config.xml` configuration file for each Security Module. The specified distribution mode is applicable for all Application objects bound to that Security Module. The following sections have more information.

- Section 6.1.1, "Controlled Distribution"
- Section 6.1.2, "Non-controlled Distribution"

For information on the Security Modules and their supported policy distribution modes, see [Table 8-1, "Security Modules with Supported Policy Distribution Modes"](#).

6.1.1 Controlled Distribution

Controlled distribution is initiated by the Policy Distribution Component, ensuring that the PDP client (Security Module) receives policy data that has been created or modified since the last distribution. In this respect, distribution is controlled by the policy administrator who takes explicit action to distribute the new or updated policy data. (The Policy Distribution Component maintains a versioning mechanism to keep track of policy changes and distribution.) When controlled distribution is enabled, the Security Module cannot request distribution of the Policy Distribution Component directly.

Note: The exception is when a Security Module starts and registers itself with the Policy Distribution Component with a Configuration ID. As long as the appropriate Application bound to the Security Module is marked as (policies are) Ready For Distribution, the policies are distributed to the Security Module based on this registration.

With controlled distribution, the Policy Distribution Component distributes new and updated policy data to the Security Module where the data is stored in a local persistent cache, a file-based cache maintained by the PDP to store policy objects and provide independence from the policy store. The Policy Distribution Component does not maintain constant live connections to its Security Module clients; it will establish a connection before distributing policy to it. Thus, the Security Module is not dependent on the policy store for making policy decisions; it can use its own local cache if the policy store is offline. When the Security Module starts, it will check if the policy store is available. If it is not available, the Security Module will use policy data from the local persistent cache. With controlled distribution, if any policy distribution operation fails, the entire policy distribution fails.

Caution: Controlled distribution is supported only on database type policy stores - not on LDAP-based policy stores. If the distribution API is invoked for an LDAP policy store, it will be non-operable.

6.1.2 Non-controlled Distribution

When the PDP client (Security Module) periodically retrieves (or pulls) policies and policy modifications from a policy store, it is referred to as non-controlled distribution. Non-controlled distribution makes policy changes available as soon as they are saved to the policy store. Non-controlled distribution is initiated by the Security Module and may retrieve policies that are not yet complete. The policy store must be online and constantly available for non-controlled distribution. Non-controlled distribution is supported on any policy store type including a relational database, an LDAP directory or XML.

6.2 Understanding Policy Distribution

Managing policies and distributing them are distinct operations. Policy management operations are used to define, modify and delete policies in the policy store. The Policy Distribution Component then makes the policies available to a Security Module where the data is used to grant or deny access to a protected resource. Policies cannot be enforced until they are distributed. Conceptually, policy distribution may include any or all of the following actions:

- Reading policies from the policy store.
- Caching policy objects in the in-memory policy cache maintained by the Security Module for use during authorization request processing.
- Preserving policy objects in a file-based persistent cache, local to the Policy Distribution Component, that provides independence from the policy store.

Both the central Oracle Entitlements Server Administration Console and the locally-installed (to the protected application) Security Module contain the Policy Distribution Component. This architecture allows two deployment scenarios: the first involves a centralized Policy Distribution Component that can communicate with

many Security Modules while the second involves a Policy Distribution Component that is local to, and communicates with, only one Security Module.

Note: For details on configuring the Security Module parameters for policy distribution, see [Section A.1, "Policy Distribution Configuration."](#) For details on creating definitions and binding Security Modules, see [Section 10.2, "Configuring Security Module Definitions."](#)

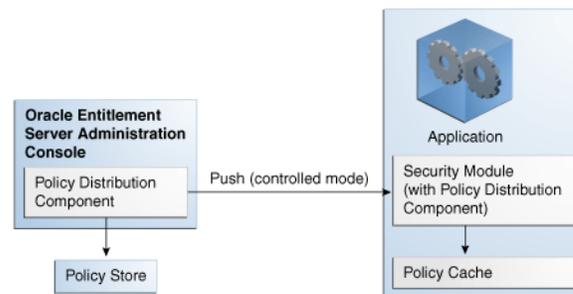
The following sections contain more information.

- [Section 6.2.1, "Using a Central Policy Distribution Component"](#)
- [Section 6.2.2, "Using a Local Policy Distribution Component"](#)

6.2.1 Using a Central Policy Distribution Component

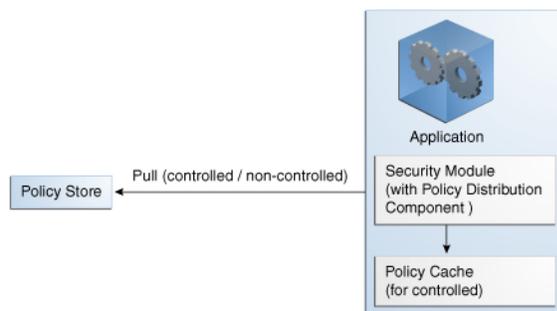
The centralized Policy Distribution Component scenario involves the use of the Policy Distribution Component (within the Administration Console) to act as a server communicating with the Security Module's Policy Distribution Component client. [Figure 6–1](#) illustrates how, in this scenario, the Security Module's Policy Distribution Component client does not communicate with the policy store. The distribution of policies is initiated by the Oracle Entitlements Server administrator and *pushed* to the Policy Distribution Component client. Currently, data can only be pushed in a *controlled* manner as described in [Section 6.1.1, "Controlled Distribution."](#) This scenario allows for a central Policy Distribution Component that can communicate with many Security Modules.

Figure 6–1 Using Oracle Entitlements Server Policy Distribution Component



6.2.2 Using a Local Policy Distribution Component

The local (to the Security Module) scenario involves the Security Module's Policy Distribution Component communicating directly with the policy store. This scenario allows for a local Policy Distribution Component to communicate with one Security Module only. The application administers management operations and decides when the Security Module instance of the Policy Distribution Component will distribute policies or policy deltas. In this deployment, as illustrated in [Figure 6–2](#), the Policy Distribution Component *pulls* data from the policy store (by periodically checking the policy store for data to be distributed) and sends policy data from the policy store, making it available to the PDP after administrator-initiated policy distribution.

Figure 6–2 Using Security Module Policy Distribution Component

Currently, data can be pulled in either a controlled manner as described in [Section 6.1.1, "Controlled Distribution"](#) or a non-controlled manner as described in [Section 6.1.2, "Non-controlled Distribution."](#)

Note: It is recommended that you use controlled-pull mode in a production environment for better performance and scalability when large policy sets are distributed to the Security Modules.

6.3 Distributing Policies

From a high level, the following steps are needed to get to the point where you can distribute policies. Distributing policies using these steps (from the Administration Console or with the API) will work for Controlled-push Distribution only.

Security Modules configured for Controlled-pull and Non-controlled Distribution retrieve policy data from the policy store directly and don't require explicit distribution. For Security Modules configured for Controlled-pull Distribution, the Security Module will directly obtain the policy from the policy store in intervals.

1. Create a Security Module definition.
See [Section 10.2.1, "Creating a Security Module Definition."](#)
2. Bind the definition to the appropriate Application.
See [Section 10.2.2, "Binding an Application to a Security Module."](#) To unbind the Security Module, see [Section 10.2.3, "Unbinding an Application From a Security Module."](#)
3. Open the Application in the Home area.
See [Section 6.3.1, "Distributing Policies Using the Administration Console."](#)
4. Distribute the policies.
See [Section 6.3.1, "Distributing Policies Using the Administration Console."](#)

6.3.1 Distributing Policies Using the Administration Console

Policies are distributed from within an Application. The following procedure documents how to distribute policies using the Administration Console.

1. Expand the Applications node in the Navigation Panel.
2. Select the Application which contains the policies for distribution.

3. Right-click the Application name and select Open from the menu.
The General tab, the Delegated Administrators tab and the Policy Distribution tab are all active.
4. Click the Policy Distribution tab.
5. Click Distribute.
Policies are distributed to all Security Modules bound to the Application.
6. Click Refresh to update the distribution progress.

6.4 Using Default or Third Party Digital Certificates

Secure Sockets Layer (SSL) uses public key encryption technology to establish and verify server identity and trust. With public key encryption, a public key and a private key are generated for the server. Data encrypted with the public key can only be decrypted with the corresponding private key and data encrypted with the private key can only be decrypted with the corresponding public key. The private key is protected so that only the owner can decrypt messages encrypted using the public key. The public key is embedded in a digital certificate with additional information describing the owner of the public key (such as name, street address and e-mail address).

Note: The data embedded in the digital certificate is verified by a certificate authority (CA) and digitally signed with the CA's trusted digital certificate. The CA's trusted digital certificate establishes trust for the application's digital certificate itself.

An application participating in an SSL connection is authenticated when the other party evaluates and accepts its digital certificate. Web browsers, servers, and other SSL-enabled applications generally accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid.

During the creation of a Security Module instance (for more information, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*), the default Oracle Entitlements Server Security Module (client) digital certificate is stored in `your_oes_sm_folder/oes_sm_instances/your_oes_sm/security/identity.jks` and the trusted Certificate Authority (CA) digital certificates are stored in `your_oes_sm_folder/oes_sm_instances/your_oes_sm/security/trust.jks`. Both are Java Key Stores (JKS) with the passwords defined during the creation of the Security Module instance. The password will be encrypted and stored in the standard Oracle Wallet (with auto logon). The default Oracle Entitlements Server client keys are generated by itself and signed during the enrollment process. The following sections document how to use third party certificates with the applicable security module.

- [Section 6.4.1, "Configuring Oracle Entitlements Server Security Module \(Client\) When Third Party Certificate is Used in Administration Server"](#)
- [Section 6.4.2, "Adding Signer if Third Party Certificate Is Used in a Security Module with an IBM Websphere Administration Side"](#)
- [Section 6.4.4, "Using a Third Party Certificate with a WebLogic Server Security Module"](#)
- [Section 6.4.5, "Using a Third Party Certificate with a Web Services or Java Security Module"](#)

- Section 6.4.6, "Using a Third Party Certificate with a WebSphere Application Server Security Module"
- Section 6.4.7, "Using a Third Party Certificate with a Tomcat or JBoss Security Module"

Note: By default, an installation of WebLogic Server creates and uses `DemoIdentity.jks` and `DemoTrust.jks` as the identity and trust stores respectively. The full paths to the locations of these stores can be found using the WebLogic Server console. The default password for the trust store is `DemoTrustKeyStorePassPhrase`.

6.4.1 Configuring Oracle Entitlements Server Security Module (Client) When Third Party Certificate is Used in Administration Server

This section contains information on configuring the security modules if third-party certificates are used on the Administration side.

6.4.1.1 Configuring the WebLogic Security Module if a Third Party Digital Certificate Is Used On the Administration Side

To set up a WebLogic Security Module when a third party certificate is used on the Administration side, follow these steps:

1. Run the `./config.sh` command from `OES_CLIENT_HOME/oessm/bin` as follows:

```
config.sh -smType wls -smConfigId mySM_WLS -skipEnroll
```

Table 6–1 describes the parameters you specify on the command line.

Table 6–1 Web Services or Java Security Module Parameters

| Parameter | Description |
|-------------------------|--|
| <code>smType</code> | Type of security module instance you want to create. It should be <code>wls</code> . |
| <code>smConfigId</code> | Name of the security module instance. For example, <code>mySM_WLS</code> . |
| <code>skipEnroll</code> | Skips enrollment when creating a Security Module. After the Security Module is created with <code>skipEnroll</code> , you should prepare and put certificates for the Security Module to the Security Module's identity/trust store. |

2. Import the administration certificate to the WebLogic Server (SM) trust store.

The WebLogic trust store can be found using the WebLogic console. The default is `WLS_HOME/wlserver_10.3/server/lib/DemoTrust.jks`.

Issue the following command:

```
keytool -import -alias jksuser
-file /scratch/tools/certs/jksuser.crt
-keystore WLS_HOME/wlserver_10.3/server/lib/DemoTrust.jks
-storepass DemoTrustKeyStorePassPhrase
-storetype JKS
-trustcacerts
```

6.4.1.2 Configuring the Web Services or Java Security Module if a Third Party Digital Certificate Is Used On the Administration Side

To set up a Web Service or Java Security Module when a third party certificate is used on the Administration side, follow these steps:

1. Run the `./config.sh` command from `OES_CLIENT_HOME/oessm/bin` as follows:

```
config.sh -smType ws (or java) -smConfigId mySM_ws -skipEnroll
```

2. Copy identity/trust store file to `OES_SM_INSTANCE_HOME/security`.

The identity/trust store filename must be `identity.jks` and `trust.jks`.

Alternatively, you may edit the `jps-config.xml` file to include the location of the file.

For example:

```
<property name="oracle.security.jps.pd.client.ssl.identityKeyStoreFileName"
value="OES_SM_INSTANCE_HOME/security/identity.jks"/>
<property name="oracle.security.jps.pd.client.ssl.trustKeyStoreFileName"
value="OES_SM_INSTANCE_HOME/security/trust.jks"/>
```

The trust store must trust the signer of the administration certificate using the above `keytool` command.

3. Run `oesPassword.sh` in the `OES_SM_INSTANCE_HOME/bin` directory to save the identity/trust store password into the credential store:

```
./oesPassword.sh -initenroll
```

Note: Set the following classes to the CLASSPATH before running `oesPassword.sh`:

- `OES_ORACLE_HOME/modules/javax.security.jacc_1.0.0.0_1-1.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wseeclient.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wlthint3client.jar`
-

6.4.1.3 Configuring the IBM WebSphere Application Server Security Module if a Third Party Digital Certificate Is Used On the Administration Side

To set up an IBM WebSphere Security Module if a third party certificate is used on the Administration side, complete the following steps:

1. Run `./config.sh` command from `OES_CLIENT_HOME/oessm/bin` as follows:

```
./config.sh -smType was -smConfigId mySM_WAS
-serverLocation WAS_HOME/
-skipEnroll -profileName dmgr_profileName -serverName OesServer
```

`WAS_HOME` is the location of the IBM WebSphere Application Server.

Table 6–2 describes the parameters you specify on the command line.

Table 6–2 IBM WebSphere Security Module Parameter

| Parameter | Description |
|----------------|--|
| smType | Type of security module instance you want to create. For example, was. |
| smConfigId | Name of the security module instance. For example, mySM_WAS. |
| serverLocation | Location of the IBM WebSphere Server. |

2. Configure SSL for the IBM WebSphere application server as follows:

- a. Import the trust certificate into IBM WebSphere node default trust keystore and cell default trust keystore by using `keytool` to export customer trust certificate from customer trust keystore file into a `.der`, as shown in the following example:

```
keytool -exportcert -keystore <your_trust_store> -alias your_alias -file
~/was.der
```

You must provide your trust store location.

- b. Import the `was.der` file into the IBM WebSphere node default trust keystore and cell default trust keystore as follows:
- You may find the import in the IBM WebSphere Administration Server console:

security >SSL certificate and key management > Key stores and certificates > <NodeDefaultTrustStore> <CellDefaultTrustStore> (here you need to choose one name) **> Signer certificates.**
 - Click **Add**.
 - Enter an alias. For example, **WLS**.
 - Choose the `.der` file that you exported earlier, and select data type as **DER**.
- c. Import the your private key into the IBM WebSphere node default keystore as follows:
- You may find the import in the IBM WebSphere Administration Server console:

security >SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
 - Click **Import**.
 - Select **Keystore** and enter the path to the keystore file (your keystore file).
 - Select **JKS** as type and enter the password you used to create the keystore file.
 - The certificate alias name is the same name as the hostname.
- d. Enable Inbound SSL for the server running IBM WebSphere Security Module as follows:
- In the IBM WebSphere administration console, go to **Security >SSL certificate and key management > Manage endpoint security configurations.**

- Expand inbound tree to get: **Inbound**
>**DefaultCell(CellDefaultSSLSettings)** > **nodes** >
DefaultCellFederatedNode > **servers** > *Server_name_running_IBM_WebSphere_Security_Module* and select the server.
 - In the General Properties page, select **Override inherited values**.
 - From the **SSL configuration** list, select **NodeDefaultSSLSettings**.
 - Click **Update certificate alias list** button and then choose the new imported private key alias in the **Certificate alias in key store** list.
 - Click **Apply**.
- e. Enable Out bound SSL for the server running IBM WebSphere Security Module, follows:
- In the IBM WebSphere administration console, go to **Security** >**SSL certificate and key management** > **Manage endpoint security configurations**.
 - Expand inbound tree to get: **Outbound** >
DefaultCell(CellDefaultSSLSettings) > **nodes** >
DefaultCellFederatedNode > **servers** > *Server_name_running_IBM_WebSphere_Security_Module* and select the server.
 - In the General Properties page, select **Override inherited values**.
 - From the **SSL configuration** list, select **NodeDefaultSSLSettings**.
 - Click **Update certificate alias list** and choose the new imported private key alias in the **Certificate alias in key store** list.
 - Click **Apply**.

6.4.2 Adding Signer if Third Party Certificate Is Used in a Security Module with an IBM Websphere Administration Side

If third party certificate is used in the WebSphere Application Server Security Module side, you must add a signer of the third-party certificate into the IBM WebSphere administration trust store:

1. Import the trust certificate into IBM WebSphere node default trust keystore and cell default trust keystore by using `keytool` to export trust certificate file from trust keystore file. For example, `trust.jks` file into a `.der`, as shown in the following example:

```
keytool -exportcert -keystore trust.jks -alias wlsccertgencab -file ~/was.der
```

2. Import the `was.der` file into the IBM WebSphere node default trust keystore and cell default trust keystore. as follows:
 - You may find the import in the IBM WebSphere Administration Server console:


```
security > SSL certificate and key management > Key stores and certificates
> <NodeDefaultTrustStore> <CellDefaultTrustStore> (here you need to
choose one name) > Signer certificates.
```
 - Click **Add**.
 - Enter an alias. For example, **WS**.
 - Choose the `.der` file that you exported earlier, and select data type as **DER**.

6.4.3 Adding Signer if Third Party Certificate Is Used in a Security Module with a WebLogic Administration Side

If third party certificate is used in the WebLogic Server Security Module side, you must add a signer of the third-party certificate into the WebLogic Server administration trust store. To do this:

Import the third party generated certificate to the WebLogic Server trust store using this command:

```
keytool -import -alias keyAlias -file cert_file -keystore ./DemoTrust.jks
-storepass DemoTrustKeyStorePassPhrase -storetype JKS -keypass password
```

By default, the administration server uses `DemoIdentity.jks` and `DemoTrust.jks` as the default identity and trust stores, respectively.

6.4.4 Using a Third Party Certificate with a WebLogic Server Security Module

The following procedure illustrates how to use a third party certificate with a WebLogic Server Security Module.

1. Import the third party generated certificate to Administration Trust Store.

If you are using a WebSphere Administration Side, follow the instructions in [Section 6.4.2, "Adding Signer if Third Party Certificate Is Used in a Security Module with an IBM Websphere Administration Side."](#)

If you are using a WebLogic Administration Side, follow the instructions in [Section 6.4.3, "Adding Signer if Third Party Certificate Is Used in a Security Module with a WebLogic Administration Side."](#)

2. Import the administration CA certificate to the client trust store using the `keytool` command line interface.

The following command imports the CA certificate in the default trust store to a client trust store. The absolute path to the client trust store is defined in the WebLogic Administration Console. Modify the parameters in the command to reflect your deployment.

```
keytool -importkeystore -srckeystore ./DemoTrust.jks
-destkeystore yourTrustStore -srcstorepass DemoTrustKeyStorePassPhrase
-deststorepass passwordForYourTrustStore
-srccalias wlscertgencab -destalias wlscertgencab
```

This step is not needed if using the default trust store.

3. Configure a third party key store using the WebLogic Server Administration Console in the WebLogic Server domain for the appropriate Security Module.
 - a. In the left pane of the Administration Console, expand Environment and select Servers.
 - b. Click the name of the server for which you want to configure the identity and trust keystores.
 - c. Click Configuration -> Keystores.
 - d. Select the method for storing and managing private key/digital certificate pairs and trusted CA certificates in the Keystores field. The available options are described in [Table 6-3](#).

Table 6–3 Storing and Managing Certificate Options

| Option | Description |
|---|--|
| Demo Identity and Demo Trust | The demonstration identity and trust keystores (located in the <code>WLS_HOME\server\lib</code> directory) and the JDK cacerts keystore (located in the <code>JAVA_HOME\jre\lib</code> directory) are configured by default. Use for development only. |
| Custom Identity and Java Standard Trust | A keystore you create and the trusted CAs defined in the cacerts file (located in the <code>JAVA_HOME\jre\lib</code> directory) directory are configured. |
| Custom Identity and Custom Trust | Identity and trust keystores you create are configured. |
| Custom Identity and Command Line Trust | An identity keystore you create and command-line arguments that specify the location of the trust keystore are configured. |

- e. Define values for the identity keystore attributes in the Identity section. [Table 6–4](#) defines the attributes.

Table 6–4 Using the Identity Keystore Attributes

| Attribute | Description |
|-------------------------------------|--|
| Custom Identity Keystore | The fully qualified path to the identity keystore. |
| Custom Identity Keystore Type | The type of the keystore. Generally, this attribute defines a Java KeyStore (JKS); if left blank, it defaults to JKS. |
| Custom Identity Keystore Passphrase | The password to be entered when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore however, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore. Note: The passphrase for the Demo Identity keystore is <code>DemoIdentityKeyStorePassPhrase</code> . |

- f. Define values for the trust keystore attributes in the Trust section.

If you chose Java Standard Trust as your keystore (as documented in [Table 6–3](#)), specify the password defined when creating the keystore and confirm it. If you chose Custom Trust, define the attributes documented in [Table 6–5](#).

Table 6–5 Using Trust Keystore Attributes

| Attribute | Description |
|----------------------------------|--|
| Custom Trust Keystore | The fully qualified path to the trust keystore. |
| Custom Trust Keystore Type | The type of the keystore. Generally, this attribute is JKS; if left blank, it defaults to JKS. |
| Custom Trust Keystore Passphrase | The password you will enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore so whether or not you define this property depends on the requirements of the keystore. |

- g. Click Save.

- h. Click Activate Changes in the Change Center of the Administration Console.
Some changes require a server restart.

6.4.5 Using a Third Party Certificate with a Web Services or Java Security Module

The following procedure illustrates how to use a third party certificate with a Web Services or Java Security Module.

1. Import the third party generated certificate to the administration trust store using this command.

```
keytool -import -alias keyAlias -file cert_file -keystore ./DemoTrust.jks  
-storepass DemoTrustKeyStorePassPhrase -storetype JKS -keypass password
```

By default, the administration server uses `DemoIdentity.jks` and `DemoTrust.jks` as the default identity and trust stores, respectively.

2. Import the administration CA certificate to the client trust store using the `keytool` command line interface.

The following command imports the CA certificate in the default trust store to a client trust store. The absolute path to the client trust store is defined in the WebLogic Administration Console. Modify the parameters in the command to reflect your deployment.

```
keytool -importkeystore -srckeystore ./DemoTrust.jks  
-destkeystore yourTrustStore -srcstorepass DemoTrustKeyStorePassPhrase  
-deststorepass passwordForYourTrustStore  
-srcalias wlscertgencab -destalias wlscertgencab
```

This step is not needed if using the default trust store.

3. Configure the following properties in `jps-config.xml`.

- `oracle.security.jps.pd.client.ssl.identityKeyStoreFileName`
- `oracle.security.jps.pd.client.ssl.trustKeyStoreFileName`
- `oracle.security.jps.pd.client.ssl.identityKeyStoreKeyAlias`

See [Appendix A, "Installation and Configuration Parameters"](#) for details.

4. Run `oesPassword.sh` in the appropriate `SM-instance/bin` directory to save the trust store password, the key store password and the key password into the credential store.
 - If the trust store, key store and key all have the same password, run `./oesPassword.sh`.
 - If the trust store, key store and key all have different passwords, run `./oesPassword.sh -diffpass`. You will be asked to enter (and confirm) the passwords for the `identity.jks` key store, the `trust.jks` trust store and the key.

The password for the default key store (identity store), each of the key store's disparate key entries, and the default trust store is `welcome1`.

Note: Set the following classes to the CLASSPATH before running oesPassword.sh:

- `OES_ORACLE_HOME/modules/javax.security.jacc_1.0.0.0_1-1.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wseeclient.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wlthint3client.jar`
-

6.4.6 Using a Third Party Certificate with a WebSphere Application Server Security Module

The following procedure illustrates how to use a third party certificate with a WebSphere Application Server Security Module.

1. Import the third party generated certificate to the administration trust store using this command.

```
keytool -import -alias keyAlias -file cert_file -keystore ./DemoTrust.jks
-storepass DemoTrustKeyStorePassPhrase -storetype JKS -keypass password
```

By default, the administration server uses `DemoIdentity.jks` and `DemoTrust.jks` as the default identity and trust stores, respectively.

2. Import the administration CA certificate to the client trust store using the `keytool` command line interface.

The following command imports the CA certificate in the default trust store to a client trust store. The absolute path to the client trust store is defined in the WebLogic Administration Console. Modify the parameters in the command to reflect your deployment.

```
keytool -importkeystore -srckeystore ./DemoTrust.jks
-destkeystore yourTrustStore -srcstorepass DemoTrustKeyStorePassPhrase
-deststorepass passwordForYourTrustStore
-srccalias wlscertgencab -destalias wlscertgencab
```

This step is not needed if using the default trust store.

3. Configure a third party key store and trust store using the WebSphere Application Server console located at `servername:port/ibm/console`.

Information on configuring the IBM WebSphere Security Module itself is documented in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- a. Export the WebLogic Server `DemoTrust.jks` keystore or Oracle Entitlements Server `trust.jks` into a `.DER` file using the `keytool` command line interface.

```
keytool -exportcert -keystore yourtruststore -alias wlscertgencab
-file ~/was.der
```

- b. Import generated `was.der` file into the WebSphere default trust keystore and cell default trust keystore nodes.

- a. Access the WebSphere Administration Server console Signer certificates page by navigating through Security -> SSL certificate and key management -> Key stores and certificates -> *choose the appropriate*

- f. Click Apply.

6.4.7 Using a Third Party Certificate with a Tomcat or JBoss Security Module

The following procedure illustrates how to use a third party certificate with a Tomcat or JBoss Application Server Security Module.

1. Import the third party generated certificate to the administration trust store using this command.

```
keytool -import -alias keyAlias -file cert_file -keystore ./DemoTrust.jks
-storepass DemoTrustKeyStorePassPhrase -storetype JKS -keypass password
```

By default, the administration server uses `DemoIdentity.jks` and `DemoTrust.jks` as the default identity and trust stores, respectively.

2. Import the administration CA certificate to the client trust store using the `keytool` command line interface.

The following command imports the CA certificate in the default trust store to a client trust store. The absolute path to the client trust store is defined in the WebLogic Administration Console. Modify the parameters in the command to reflect your deployment.

```
keytool -importkeystore -srckeystore ./DemoTrust.jks
-destkeystore yourTrustStore -srcstorepass DemoTrustKeyStorePassPhrase
-deststorepass passwordForYourTrustStore
-srcalias wlscertgencab -destalias wlscertgencab
```

This step is not needed if using the default trust store.

3. Set the `keystoreFile` and `truststoreFile` properties for the SSL connector in the `server.xml` file. They include:
 - `keystoreFile`: location of your key store
 - `keystorePass`: password for your key store
 - `keyAlias`: certificate alias in the key store
 - `keyPass`: password for the certificate alias
 - `truststoreFile`: location of your trust store
 - `truststorePass`: password for the trust store

For the Tomcat Application Server Security Module, `server.xml` is located in the `TOMCAT_HOME/conf/` directory. For the JBoss Application Server Security Module, the location is dependent on which profile is used; for example, `JBOSS_HOME/server/jbossProfileName/deploy/jbossweb.sar/server.xml`.

6.5 Debugging Policy Distribution

Information on debugging the Policy Distribution Component is documented in [Section 13.8.3, "Debugging Policy Distribution."](#)

Deploying the Policy Decision Point

This chapter discusses why and how the Policy Decision Point (PDP) is deployed. It contains the following sections.

- Section 7.1, "Understanding the PDP Deployment Models"
- Section 7.2, "Using the Security Module Proxy Mode"
- Section 7.3, "Using the XACML Gateway"

7.1 Understanding the PDP Deployment Models

Oracle Entitlements Server supports deployment models that differ in the placement of the Policy Decision Point (PDP), depending on where the request for access will be evaluated. Java clients, for example, have the option of making a local call to the Security Module embedded with the application, or making remote calls to a Remote Method Invocation (RMI) or Web Services Security Module via a proxy. These models are not mutually exclusive; any combination of them is possible.

The PDP can be embedded locally with the application or it can be installed elsewhere (outside the application) for remote communication. Real time or near real time applications (stock trading or banking applications, respectively) would typically use the embedded model (where Security Modules are distributed) for a good response time. It should also be used if the application needs to work offline (no connectivity to the back end). A remote PDP (where one central Security Module commodities with multiple clients) can be used when there is a need to minimize the number of PDPs or if security concerns prevent deploying the PDP next to the application (like in a DMZ). Additionally, it can be used if overhead related to remote invocation is acceptable or if the PDP is invoked from an application written in a programming language other than Java (C, C++, C#).

Note: Proxy Mode is used to configure a Security Module to send authorization requests to a remote PDP. It provides the ability to issue a request for access and receive the decision of GRANT or DENY. See [Section 7.2, "Using the Security Module Proxy Mode."](#)

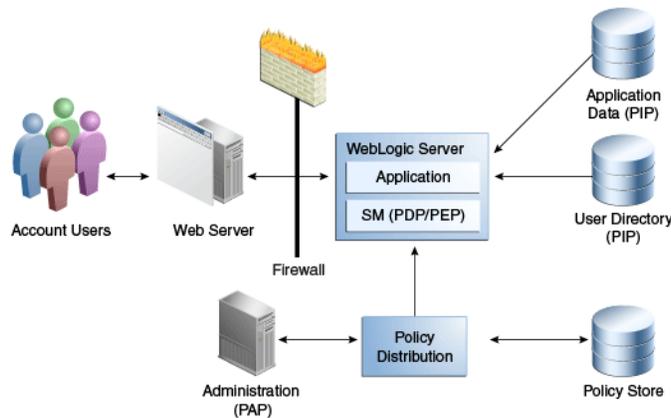
The following sections have additional information.

- Section 7.1.1, "Embedding the PDP Locally"
- Section 7.1.2, "Locating the PDP Remotely"

7.1.1 Embedding the PDP Locally

In the distributed deployment model, the Security Module/PDP is embedded in the protected application's container and runs in the same process. Policies are distributed to the Security Module and authorization decisions are made and cached locally so no network calls to a central server are needed. Additionally, no changes to the application itself are required. A typical embedded PDP deployment is illustrated in Figure 7-1.

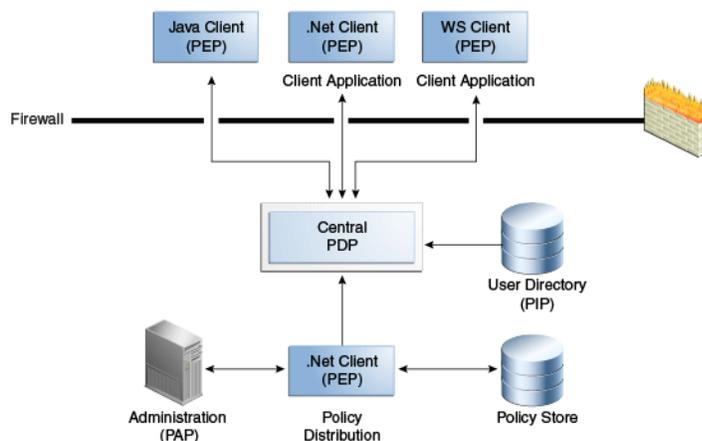
Figure 7-1 Embedded PDP Deployment



7.1.2 Locating the PDP Remotely

In the centralized deployment model, the PDP runs in a process that is separate from the protected application and is hosted in a location that is remote from the protected resources. The central PDP (Oracle Entitlements Server or a Security Module) receives authorization requests from multiple clients and then evaluates the applicable policies, returning the authorization decision (GRANT or DENY) to the PEP to enforce. Figure 7-2 illustrates this centralized deployment model.

Figure 7-2 Remote PDP Deployment

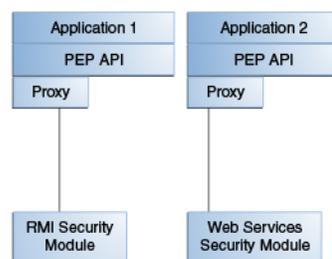


The centralized PDP is invoked using the XACML Gateway, RMI, or SOAP. It maintains local caches of roles, policies, policy decisions and attributes which can be updated on demand or at startup.

7.2 Using the Security Module Proxy Mode

Oracle Entitlements Server supports a Proxy Mode that allow clients to invoke authorization services remotely. When the Oracle Entitlements Server PEP API are used by an application to make authorization calls, a proxy can be set up on the application's host to communicate with the remote Security Module (on another machine) for access decisions. Web services or Remote Method Invocation (RMI) are the proxy's communication options. Figure 7-3 illustrates this topology.

Figure 7-3 Proxy Mode Deployment

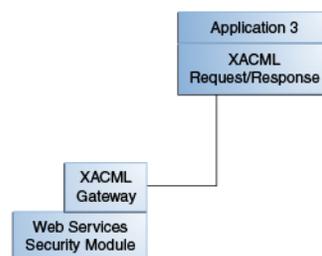


The Oracle Entitlements Server PEP API can be called from an application regardless of whether that application is calling an embedded PDP or a remote PDP. Proxy Mode can be configured to provide security services locally (including authorization caching, logging and failover) and can communicate with the PDP using RMI or SOAP.

7.3 Using the XACML Gateway

The XACML Gateway is a SOAP endpoint that uses web services functionality and provides for communication using the XACML request/response protocol. The XACML Gateway is with the PDP (not the client) and is available with the instantiation of the Web Services Security Module. No special configuration is required to use the XACML Gateway. The Web Services Security Module will use a web services call when instantiated locally with the client. If it sees a SOAP envelope at its endpoint, it uses the XACML Gateway. Figure 7-4 illustrates a XACML Gateway deployment.

Figure 7-4 XACML Gateway Deployment



Note: If the application is using the XACML request/response protocol, it is not using the PEP API.

Managing Security Module Configurations

The Security Module Configuration User Interface (SMConfig UI) is used to configure a Security Module after the OES Client has been successfully installed and a Security Module type has been instantiated. Basic configurations are accomplished during the installation and instantiation processes but the SMConfig UI allows for additional configurations or modifications to a Security Module profile. This chapter contains the following sections.

- Section 8.1, "Before You Begin"
- Section 8.2, "Starting the SMConfig UI"
- Section 8.3, "Modifying Security Module Configurations"
- Section 8.4, "Configuring Security Modules Post-Instantiation"
- Section 8.5, "Configuring the PDP Proxy Client for RMI or Web Services"

8.1 Before You Begin

The SMConfig UI assumes the following Oracle Entitlements Server installation procedures have already been completed.

- For information on installing Oracle Entitlements Server, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.
- For information on installing the OES Client and instantiating a Security Module, see *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

The OES Client installs the Security Module bits and the SMConfig Tool. The SMConfig Tool will define the Security Module type and create a directory structure for each Security Module instance. The instance's home directory is created at `$OES_CLIENT_HOME/oes_sm_instances/SM_Name/` and contains the configuration files used to run the applicable Security Module SMConfig UI script; `oessmconfig.sh` and `oessmconfig.bat` are located in the `/bin` directory of the Security Module instance's home directory.

Table 8–1 shows the Security Modules with their supported policy distribution modes or PDP Proxy Client.

Table 8–1 Security Modules with Supported Policy Distribution Modes

| SM Type | Non-controlled (non-JRF) | Controlled-pull ¹ | Controlled-push | PDP Proxy Client ² | JRF (Java Runtime Framework) ³ |
|----------------------------|--------------------------|------------------------------|-----------------|--|---|
| Java SM | Supported | Supported | Supported | Supported | NA |
| WebLogic SM | Supported | Supported | Supported | NA | Supported |
| Web service SM on WebLogic | Supported | Supported | Supported | NA | NA |
| Web service SM standalone | Supported | Supported | Supported | NA | NA |
| RMI SM | Supported | Supported | Supported | NA | NA |
| .NET SM ⁴ | NA | NA | NA | Supported to connect to Web service SM | NA |
| MOSS SM ⁵ | NA | NA | NA | Supported to connect to Web service SM | NA |
| WebSphere SM | Supported | Supported | Supported | NA | Supported |
| JBoss SM | Supported | Supported | Supported | NA | NA |
| Tomcat SM | Supported | Supported | Supported | NA | NA |

¹ Oracle recommended mode

² PDP proxy client is not a distribution mode. The proxy client does not need distribution mode configuration. The Security Module as a PDP proxy will delegates its authorization requests to one Web service Security Module or RMI Security Module.

³ JRF mode could be enabled for WebLogic domain, or IBM WebSphere. Non-controlled mode is the only supported distribution mode.

⁴ Connects to Web service Security Module as a proxy. It does not require distribution mode.

⁵ .NET Security Module based

Note: In Oracle Entitlements Server 11g Release 2 and Release 2 PS1, a Security Module can be installed in a Fusion Middleware domain, version 11gR1 PS5 (11.1.1.6). In Oracle Entitlements Server 11g Release 2 PS2, a Security Module can be installed in a Fusion Middleware domain, version 11g Release 1 PS6 (11.1.1.7). Also, when an Oracle Entitlements Server Security Module is installed into a JRF domain, only non-controlled mode is supported.

8.2 Starting the SMConfig UI

The SMConfig UI is a standalone Java-based tool distributed with the OES Client installation package. The tool configures the Policy Decision Point (PDP), the Policy Information Point (PIP), and the policy store, among other data. The SMConfig UI script is available in the directory created during the instantiation of a Security Module; for example, `$OES_CLIENT_HOME/oes_sm_instances/SM_Name/bin/`.

Note: The SMConfig UI script will run only after SMConfig Tool has exited. See [Section 8.1, "Before You Begin"](#) for details.

In a Linux environment the SMConfig UI script is named `oesmconfig.sh` and in a Windows environment it is called `oesmconfig.bat`. To start the SMConfig UI change to the `bin` directory in the appropriate Security Module instance directory and run the script on the command line.

```
cd $OES_CLIENT_HOME/oes_sm_instances/SM_Name/bin/
./oesmconfig.sh
```

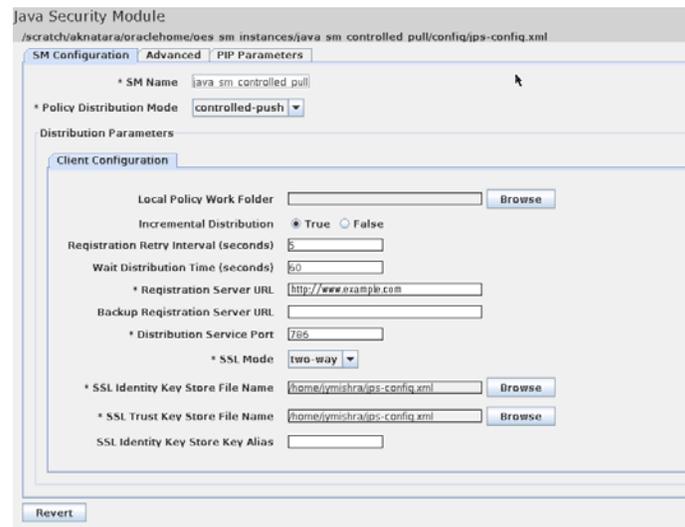
The SMConfig UI runs on the same host as the Security Module. The script will modify the Security Module's `jps-config.xml` file. The location of the `jps-config.xml` can be specified as an input parameter when first creating the Security Module. If this parameter is not specified, the default file (located in the Security Module's home directory at `$OES_CLIENT_HOME/oes_sm_instances/SM_Name/config`) is used.

Note: For the WebLogic Server Security Module, specify the `jps-config.xml` file located under `user_projects/domains/domain_name/config/oeswlssmconfig/AdminServer` when using `oesmconfig.sh`. Pass the file's location to the tool using the `-jpsconfig` parameter. For more information, enter the following:

```
./oesmconfig.sh -help
```

Figure 8–1 is a screenshot of the SMConfig UI for a Java Security Module.

Figure 8–1 SMConfig UI for Java Security Module



Depending on the type of Security Module, you can expect to configure some or all of the following:

- If installed in non-controlled mode, configure the Policy Store Type as either LDAP, Oracle DB, or XML.
 - If a database, define a location URL and database credentials, and verify database connectivity.
 - If an LDAP store, define a location URL and LDAP credentials, and verify LDAP connectivity.
- If installed in controlled push mode, configure the host, distribution port, listener port, username and password for Policy Distribution.

- If installed in Proxy Mode, configure the communication protocol, and host and distribution point of the Security Module.

8.3 Modifying Security Module Configurations

The SMConfig UI allows an administrator to fine-tune parameter values for a specific Security Module instantiation. This includes the following groups of parameters.

- PIP parameters refer to information that is used with Attribute Retrievers. PIP parameter modification includes managing values for predefined LDAP and RDBMS Attribute Retrievers as well as custom Attribute Retrievers and individual attributes that may be created and associated with a particular Attribute Retriever. See Table 8–6, "Java Security Module PIP Parameters (Attribute Retrievers)" and Table 8–7, "Java Security Module PIP Parameters (Attributes)" for details.

Note: If the Security Module is configured in Proxy Mode, PIP parameter modification is disabled.

- Many Security Module parameters are tailored to a specific Security Module type. These parameters are documented in [Section A.2, "Security Module Configuration."](#)
- Parameters associated with policy distribution are documented as follows:
 - If distributing policies in uncontrolled mode, see [Section A.4, "Policy Store Service Configuration."](#)
 - If distributing policies in a controlled push mode to a Java, RMI or Web Services Security Module, see [Section A.1.2.1, "Policy Distribution Component Client Java Standard Edition Configuration \(Controlled Push Mode\)."](#)
 - If distributing policies in a controlled push mode to a WebLogic Server, WebSphere Application Server, JBoss or Tomcat Security Module, see [Section A.1.2.2, "Policy Distribution Component Client Java Enterprise Edition Container Configuration \(Controlled Push Mode\)."](#)
 - If distributing policies in controlled-pull mode, see [Section A.4, "Policy Store Service Configuration."](#)
- Enabling Proxy Mode entails specifying the `oracle.security.jps.pdp.PDPTransport` parameter. For Proxy Mode parameters, see [Section A.3, "PDP Proxy Client Configuration."](#)

Note: The SMConfig UI cannot change the type of Security Module. To create another type of Security Module, execute the SMConfig Tool and create a new Security Module instance.

8.4 Configuring Security Modules Post-Instantiation

The following sections have information regarding the parameters, specific to the Security Module type, that can be modified post-instantiation. See [Appendix A, "Installation and Configuration Parameters"](#) for detailed descriptions.

- [Section 8.4.1, "Configuring the Java Security Module"](#)
- [Section 8.4.2, "Configuring the RMI Security Module"](#)
- [Section 8.4.3, "Configuring the Web Services Security Module"](#)

- Section 8.4.4, "Configuring the WebLogic Server Security Module"
- Section 8.4.5, "Configuring the SharePoint Server (MOSS) Security Module"
- Section 8.4.6, "Configuring the .NET Security Module"
- Section 8.4.7, "Configuring the WebSphere, Tomcat and JBoss Security Modules"
- Section 8.4.8, "Configuring the Oracle Service Bus Security Module"

Note: It is recommended that you use controlled-pull mode in a production environment for better performance and scalability when large policy sets are distributed to the Security Modules.

8.4.1 Configuring the Java Security Module

Table 8–2 documents the controlled-push Client Configuration properties for the Java Security Module.

Table 8–2 Java Security Module Controlled-Push Client Configuration

| Property Name | jps-config.xml Property |
|--------------------------|--|
| SM Name | oracle.security.jps.runtime.pd.client.sm_name |
| Policy Distribution Mode | oracle.security.jps.runtime.pd.client.policyDistributionMode |
| Client Configuration | <ul style="list-style-type: none"> ■ Local Policy Work Folder: oracle.security.jps.runtime.pd.client.localpolicy.work_folder ■ Incremental Distribution: oracle.security.jps.runtime.pd.client.incrementalDistribution ■ Registration Retry Interval: oracle.security.jps.runtime.pd.client.registrationRetryInterval ■ Wait Distribution Time: oracle.security.jps.runtime.policyDistributionWaitTime ■ Registration Server URL: oracle.security.jps.runtime.pd.client.RegistrationServerURL ■ Backup Registration Server URL: oracle.security.jps.runtime.pd.client.backupRegistrationServerURL ■ Distribution Service Port: oracle.security.jps.runtime.pd.client.DistributionServicePort ■ SSL Mode: oracle.security.jps.pd.client.sslMode ■ SSL Identity Key Store File Name: oracle.security.jps.pd.client.ssl.identityKeyStoreFileName ■ SSL Trust Key Store File Name: oracle.security.jps.pd.client.ssl.trustKeyStoreFileName ■ SSL Identity Key Store Key Alias: oracle.security.jps.pd.client.ssl.identityKeyStoreKeyAlias |

Table 8–3 documents the controlled-pull Client Configuration properties for the Java Security Module. The configuration properties are organized under the Client Configuration tab and the Policy Store tab.

Table 8–3 Java Security Module Controlled-Pull Client and Store Configuration

| Property Name | jps-config.xml Property |
|--------------------------|---|
| SM Name | oracle.security.jps.runtime.pd.client.sm_name |
| Policy Distribution Mode | oracle.security.jps.runtime.pd.client.policyDistributionMode |
| Client Configuration | <ul style="list-style-type: none"> ■ Local Policy Work Folder: oracle.security.jps.runtime.pd.client.localpolicy.work_folder ■ Incremental Distribution: oracle.security.jps.runtime.pd.client.incrementalDistribution ■ Registration Retry Interval: oracle.security.jps.runtime.pd.client.registrationRetryInterval ■ Wait Distribution Time: oracle.security.jps.runtime.policyDistributionWaitTime ■ Polling Timer: oracle.security.jps.pd.client.PollingTimerEnabled ■ Polling Timer Interval: oracle.security.jps.pd.client.PollingTimerInterval |
| Policy Store | <ul style="list-style-type: none"> ■ Policy Store Type: policystore.type takes a value of DB_ORACLE as controlled distribution works only with a database ■ Database Configuration Through URL <ul style="list-style-type: none"> ■ JDBC URL: jdbc.url ■ JDBC Driver: jdbc.driver ■ Username: security.principal ■ Password: security.credential ■ Database Configuration Through JNDI Name <ul style="list-style-type: none"> ■ Datasource JNDI Name: datasource.jndi.name ■ Maximum Search Filter Length: max.search.filter.length defines the maximum length of a search filter. Takes as a value an integer; for example, 1024. ■ Farm Name: oracle.security.jps.farm.name ■ Resource Type Enforcement Mode: oracle.security.jps.policystore.resourcetypeenforcementmode |

Table 8–4 documents the non-controlled distribution properties for the Java Security Module.

Table 8–4 Java Security Module Non-controlled Policy Store Configuration

| Property Name | jps-config.xml Property |
|--------------------------|--|
| SM Name | oracle.security.jps.runtime.pd.client.sm_name |
| Policy Distribution Mode | oracle.security.jps.runtime.pd.client.policyDistributionMode |

Table 8–4 (Cont.) Java Security Module Non-controlled Policy Store Configuration

| Property Name | jps-config.xml Property |
|---------------|---|
| Policy Store | <p>Policy Store Type: <code>polycystore.type</code> takes a value of <code>OID</code> or <code>DB_ORACLE</code>.</p> <p>DB</p> <ul style="list-style-type: none"> ■ Database Configuration Through URL <ul style="list-style-type: none"> ■ JDBC URL: <code>jdbc.url</code> ■ JDBC Driver: <code>jdbc.driver</code> ■ Username: <code>security.principal</code> ■ Password: <code>security.credential</code> ■ Database Configuration Through JNDI Name <ul style="list-style-type: none"> ■ Datasource JNDI Name: <code>datasource.jndi.name</code> ■ Maximum Search Filter Length: <code>max.search.filter.length</code> defines the maximum length of a search filter. Takes as a value an integer defining the maximum length; for example, 1024. ■ Farm Name: <code>oracle.security.jps.farm.name</code> ■ Resource Type Enforcement Mode: <code>oracle.security.jps.polycystore.resourcetypeenforcementmode</code> <p>LDAP</p> <ul style="list-style-type: none"> ■ LDAP URL: <code>ldap.url</code> defines the location of the LDAP policy store ■ Maximum Search Filter Length: <code>max.search.filter.length</code> defines the maximum length of a search filter. Takes as a value an integer; for example, 1024. ■ LDAP Root Name: <code>oracle.security.jps.ldap.root.name</code> ■ Farm Name: <code>oracle.security.jps.farm.name</code> ■ Resource Type Enforcement Mode: <code>oracle.security.jps.polycystore.resourcetypeenforcementmode</code> ■ Username: <code>security.principal</code> ■ Password: <code>security.credential</code> <p>FILE</p> <ul style="list-style-type: none"> ■ Policy Store File: location of the file used as the policy store |

Table 8–5 documents the Advanced configuration properties for the Java Security Module.

Table 8–5 Java Security Module Advanced Properties

| Property Name | jps-config.xml Property |
|--------------------------------|---|
| Rolemember Cache Type | <code>oracle.security.jps.polycystore.rolemember.cache.type</code> |
| Rolemember Cache Strategy | <code>oracle.security.jps.polycystore.rolemember.cache.strategy</code> |
| Rolemember Cache Size | <code>oracle.security.jps.polycystore.rolemember.cache.size</code> |
| Rolemember Cache Warmup Enable | <code>oracle.security.jps.polycystore.rolemember.cache.warmup.enable</code> |

Table 8–5 (Cont.) Java Security Module Advanced Properties

| Property Name | jps-config.xml Property |
|------------------------------------|--|
| Policy Lazy Load Enable | oracle.security.jps.policystore.policy.lazy.load.enable |
| Policy Cache Strategy | oracle.security.jps.policystore.policy.cache.strategy |
| Policy Cache Size | oracle.security.jps.policystore.policy.cache.size |
| Policy Cache Updatable | oracle.security.jps.policystore.cache.updateable |
| Refresh Enable | oracle.security.jps.policystore.refresh.enable |
| Refresh Purge Timeout | oracle.security.jps.policystore.refresh.purge.timeout |
| Refresh Purge Interval | oracle.security.jps.ldap.policystore.refresh.interval |
| Missing App Policy Query TTL | oracle.security.jps.pdp.missingAppPolicyQueryTTL |
| Decision Cache Enable | oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled |
| Decision Cache Eviction Capacity | oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionCapacity |
| Decision Cache Eviction Percentage | oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage |
| Decision Cache TTL | oracle.security.jps.pdp.AuthorizationDecisionCacheTTL |
| Anonymous Role Enable | oracle.security.jps.pdp.anonymousrole.enable |
| Authenticated Role Enable | oracle.security.jps.pdp.authenticatedrole.enable |

Table 8–6 documents the parameters for defining an attribute retriever as the Policy Information Point (PIP). After clicking New, the display contains the parameters for each attribute retriever type.

Table 8–6 Java Security Module PIP Parameters (Attribute Retrievers)

| Name | Definition |
|---------------------|--|
| Attribute Retriever | Type of attribute retriever is chosen from the drop down menu. Options include LDAP, DB and Custom. |
| LDAP | <ul style="list-style-type: none"> ■ Name: the Attribute Retriever's name as defined in the serviceInstance tag <pre><serviceInstance name="dbName" provider="pip.service.provider"></pre> ■ Description: an optional description as defined in the serviceInstance tag <pre><serviceInstance name="description" value="dbdescription"></pre> ■ LDAP URL: ldap.url defines the location of the LDAP policy store. Valid in JEE and JSE applications and only applies to LDAP stores. Takes as a value a URI in the format <code>ldap://host:port</code> ■ Failed Server Retry Interval: interval of time defined for the failed.server.retry.interval property when attempting to reach a failed server again ■ Username: security.principal ■ Password: security.credential |

Table 8–6 (Cont.) Java Security Module PIP Parameters (Attribute Retrievers)

| Name | Definition |
|--------|--|
| DB | <ul style="list-style-type: none"> ■ Name: the predefined Attribute Retriever's name ■ Description: an optional description ■ Database Configuration Through URL <ul style="list-style-type: none"> ■ JDBC URL: <code>jdbc.url</code> defines the location of the database policy store. Must be defined when using the Java Database Connectivity (JDBC) API to connect to a database. Takes as a value a list of comma-delimited URLs where the first is treated as primary and so on. For example, <code>jdbc:oracle:thin:@sc158116.domainexample.com:1521:orcl</code> ■ JDBC Driver: <code>jdbc.driver</code> defines the location of the driver when using JDBC API to connect to a database. Takes as a value <code>oracle.jdbc.driver.OracleDriver</code>, for example. ■ Username: <code>security.principal</code> ■ Password: <code>security.credential</code> ■ Database Configuration Through JNDI Name <ul style="list-style-type: none"> ■ Datasource JNDI Name: Data source JNDI name if you want the PIP instance working through data source rather than directly through JDBC. The data source scenario is supported on WebLogic Server and WebSphere Application Server only. Takes as a value the JNDI name of the pre-defined data source object. ■ Failed Server Retry Interval: After communication with a primary repository has failed, this attribute defines the interval of time during which the backup repository is used before switching back to the primary repository. Takes as a value the number of seconds; the default value is 15. |
| Custom | <ul style="list-style-type: none"> ■ Name: the custom Attribute Retriever's name ■ Description: an optional description ■ Class Names: one or more class names |

Table 8–7 documents the parameters that define the attribute which should be retrieved from the applicable Policy Information Point (PIP). It includes the parameters for both LDAP and database stores.

Table 8–7 Java Security Module PIP Parameters (Attributes)

| Name | jps-config.xml Property |
|---------------------|---|
| Attribute Retriever | Select the defined Attribute Retriever from the drop down menu. |

Table 8–7 (Cont.) Java Security Module PIP Parameters (Attributes)

| Name | jps-config.xml Property |
|------------------|--|
| Name | Name of the attribute as defined in the policy store. If using the predefined LDAP Attribute Retriever, the attribute name defined for Oracle Entitlements Server must be the same as the attribute name defined in the LDAP store. Currently, there is no name mapping functionality. |
| Query | This is an example of an LDAP query: <pre><property name="query" value="(cn=xUSERATTR)"/></pre> This is an example of a database query: <pre><property name="query" value="select description from bookstore where author='jimmy'"/></pre> |
| Search Base | The search base for an LDAP store; not displayed for a database |
| Time To Live | Time-to-live (in seconds) of any cached attribute values when cached is enabled. |
| Attribute Cached | Enables the caching of attribute values. |

8.4.2 Configuring the RMI Security Module

The following links document the parameters when configuring the RMI Security Module post-instantiation.

- [Table 8–2, "Java Security Module Controlled-Push Client Configuration"](#) documents the controlled-push Client Configuration properties for the RMI Security Module.
- [Table 8–3, "Java Security Module Controlled-Pull Client and Store Configuration"](#) documents the controlled-pull Client and Store Configuration properties for the RMI Security Module.
- [Table 8–4, "Java Security Module Non-controlled Policy Store Configuration"](#) documents the non-controlled Policy Store Configuration properties for the RMI Security Module.
- [Table 8–5, "Java Security Module Advanced Properties"](#) documents the Advanced configuration properties for the RMI Security Module.
- [Table 8–6, "Java Security Module PIP Parameters \(Attribute Retrievers\)"](#) and [Table 8–7, "Java Security Module PIP Parameters \(Attributes\)"](#) document the PIP Parameter properties for the RMI Security Module.

See [Appendix A, "Installation and Configuration Parameters"](#) for descriptions of the properties.

Tip: When using a JBOSS Security Module in Proxy Mode as the PEP and the RMI Security Module as the PDP, `jbossx.jar` must be added to the CLASSPATH of the RMI Security Module.

8.4.3 Configuring the Web Services Security Module

The following links document the parameters when configuring the Web Services Security Module post-instantiation.

- [Table 8–2, "Java Security Module Controlled-Push Client Configuration"](#) documents the controlled-push Client Configuration properties for the Web Services Security Module.

Note: The SSL properties in [Table 8–2](#) are not displayed or configurable for the Web Services Security Module.

- [Table 8–3, "Java Security Module Controlled-Pull Client and Store Configuration"](#) documents the controlled-pull Client and Store Configuration properties for the Web Services Security Module.
- [Table 8–4, "Java Security Module Non-controlled Policy Store Configuration"](#) documents the non-controlled Policy Store Configuration properties for the Web Services Security Module.
- [Table 8–5, "Java Security Module Advanced Properties"](#) documents the Advanced configuration properties for the Web Services Security Module.
- [Table 8–6, "Java Security Module PIP Parameters \(Attribute Retrievers\)"](#) and [Table 8–7, "Java Security Module PIP Parameters \(Attributes\)"](#) document the PIP Parameter properties for the Web Services Security Module.

See [Appendix A, "Installation and Configuration Parameters"](#) for descriptions of the properties. See [Section 8.4.4, "Configuring the WebLogic Server Security Module"](#) if using the Web Services Security Module on a WebLogic Server.

Tip: When using a JBOSS Security Module in Proxy Mode as the PEP and the Web Services Security Module as the PDP, `jbossx.jar` must be added to the CLASSPATH of the Web Services Security Module.

8.4.4 Configuring the WebLogic Server Security Module

The following links document the parameters when configuring the WebLogic Server Security Module post-instantiation. These parameters are also valid when using the Web Services Security Module on a WebLogic Server.

Note: If installed on a WebLogic Server, there is no need to configure the Web Service entry point.

- [Table 8–2, "Java Security Module Controlled-Push Client Configuration"](#) documents the controlled-push Client Configuration properties for the WebLogic Server Security Module. The following additional WLS Configuration Properties are specific to the WebLogic Server when the security providers have been enabled (as documented in [Section 9.4.1, "Integrating with WebLogic Server"](#)) and can be defined as *permit*, *abstain* or *deny*.
 - Undefined Application Effect
 - No Applicable Policy Effect
- [Table 8–3, "Java Security Module Controlled-Pull Client and Store Configuration"](#) documents the controlled-pull Client and Store Configuration properties for the WebLogic Server Security Module. The following additional WLS Configuration Properties are specific to the WebLogic Server when the security providers have been enabled (as documented in [Section 9.4.1, "Integrating with WebLogic Server"](#)) and can be defined as *permit*, *abstain* or *deny*.
 - Undefined Application Effect
 - No Applicable Policy Effect

- [Table 8–4, "Java Security Module Non-controlled Policy Store Configuration"](#) documents the non-controlled Policy Store Configuration properties for the WebLogic Server Security Module. The following additional WLS Configuration Properties are specific to the WebLogic Server when the security providers have been enabled (as documented in [Section 9.4.1, "Integrating with WebLogic Server"](#)) and can be defined as *permit*, *abstain* or *deny*.
 - Undefined Application Effect
 - No Applicable Policy Effect
- [Table 8–5, "Java Security Module Advanced Properties"](#) documents the Advanced configuration properties for the WebLogic Server Security Module.
- [Table 8–6, "Java Security Module PIP Parameters \(Attribute Retrievers\)"](#) and [Table 8–7, "Java Security Module PIP Parameters \(Attributes\)"](#) document the PIP Parameter properties for the WebLogic Server Security Module.

See [Appendix A, "Installation and Configuration Parameters"](#) for descriptions of the properties.

8.4.5 Configuring the SharePoint Server (MOSS) Security Module

The SMConfig UI does not configure parameters for the MOSS Security Module itself. It configures the Web Services Security Module that serves as the remote PDP for the SharePoint Security Module. See [Section 8.4.3, "Configuring the Web Services Security Module"](#) for information. The *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* contains additional information on configuring the MOSS Security Module.

8.4.6 Configuring the .NET Security Module

The SMConfig UI does not configure parameters for the .NET Security Module itself. It configures the Web Services Security Module that serves as the remote PDP for the .NET Security Module. See [Section 8.4.3, "Configuring the Web Services Security Module"](#) for information. The *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* contains additional information on configuring the MOSS Security Module.

8.4.7 Configuring the WebSphere, Tomcat and JBoss Security Modules

The following links document the parameters when configuring the WebSphere, Tomcat and JBoss Security Modules post-instantiation.

- [Table 8–2, "Java Security Module Controlled-Push Client Configuration"](#) documents the controlled-push Client Configuration properties.
- [Table 8–3, "Java Security Module Controlled-Pull Client and Store Configuration"](#) documents the controlled-pull Client and Store Configuration properties.
- [Table 8–4, "Java Security Module Non-controlled Policy Store Configuration"](#) documents the non-controlled Policy Store Configuration properties.
- [Table 8–5, "Java Security Module Advanced Properties"](#) documents the Advanced configuration properties.
- [Table 8–6, "Java Security Module PIP Parameters \(Attribute Retrievers\)"](#) and [Table 8–7, "Java Security Module PIP Parameters \(Attributes\)"](#) documents the PIP Parameter properties.

Tip: In order for the Security Modules to recognize JBOSS Principals, add `JBOSS_HOME/common/lib/jbosssx.jar` - which contains `org.jboss.security.SimplePrincipal` - into the CLASSPATH of the RMI/WS server.

See [Appendix A, "Installation and Configuration Parameters"](#) for descriptions of the properties.

8.4.8 Configuring the Oracle Service Bus Security Module

The Oracle Service Bus (OSB) Security Module works only when the Oracle Entitlements Server authorization providers are enabled using the WebLogic Server console (as defined in [Section 9.4.1, "Integrating with WebLogic Server"](#)). See [Table 8.4.4, "Configuring the WebLogic Server Security Module"](#) for details on configuring the OSB Security Module parameters post-instantiation. You can extend the OSB Domain to create OSB Security Module.

Note: When an Oracle Entitlements Server Security Module is installed into a JRF domain, only non-controlled mode is supported.

The following procedure is used to configure the OSB Security Module.

1. After installing and starting the OSB server and Oracle Entitlements Server, install the OESClient.

See *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

2. Apply Opatch to the installed OESClient and the `oracle_common` directory. The `oracle_common` directory is created during OSB installation.

3. Modify the `smconfig.prp` file.

`smconfig.prp` is located in the `OES_CLIENT_HOME/oessm/SMConfigTool` directory. See *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

4. Create an OSB Security Module using the SMConfig Tool.

Ensure the Oracle Entitlements Server is running. See *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

- a. Change to the `bin` directory.

```
cd OES_CLIENT_HOME/oessm/bin
```

- b. Run the SMConfig Tool.

```
./config.sh -smType wls -smConfigId osbSM -serverLocation
../wlserver_10.3/
```

- c. Input the name and password of the user with permission to access the Oracle Entitlements Server policy store in the command window.

- d. Select **Oracle Entitlements Server Security Module On Service Bus -11.1.2.0[oescient]** when prompted by the Fusion Middleware Configuration Wizard to Select Extension Source and click Next.

5. Modify the policy store configuration in the `jps-config.xml` file in the OSB Domain.

6. Enable the Oracle Entitlements Server authorization and role mapping providers using the WebLogic Server console.
See [Section 9.4.1, "Integrating with WebLogic Server."](#)
7. Restart the OSB server.

8.5 Configuring the PDP Proxy Client for RMI or Web Services

Oracle Entitlements Server supports a Proxy Mode that allow clients to invoke authorization services remotely. When the Oracle Entitlements Server PEP API are used by an application to make authorization calls, a PDP Proxy Client can be set up on the application's host to communicate with the remote Security Module (on another machine) for access decisions. The PDP Proxy Client provides local security services, including caching, logging, and failover support. A Remote Method Invocation (RMI) or Web Services call can be used as the method of communication between the PDP Proxy Client and the remote Security Module. The RMI and Web Services Security Modules are the only ones to invoke security services remotely.

Note: In XACML terminology, the proxy and remote Security Module are analogous to the PDP Proxy and PDP, respectively.

The Oracle Entitlements Server PEP API can be called from an application regardless of whether that application is calling an embedded PDP or a remote PDP. Proxy Mode can be configured to provide security services locally (including authorization caching, logging and failover) and can communicate with the PDP using RMI or SOAP.

There are configurations involved with both the local PDP Proxy Client and the remote Security Module. On the proxy side, client configurations are consolidated in the PDP Service instance inside the `jps-config.xml` configuration file. On the server side, configuration parameters for both the RMI and Web Services Security Modules are also consolidated in the PDP Service instance inside the `jps-config.xml` configuration file. See [Appendix A, "Installation and Configuration Parameters"](#) for details on the configuration parameters.

Securing Environment Specific Resources

This chapter contains information on how to secure resources using specific Security Modules. It contains the following sections.

- Section 9.1, "Choosing a Security Module Type"
- Section 9.2, "Securing Microsoft Office SharePoint Server Resources"
- Section 9.3, "Securing Oracle Service Bus Resources"
- Section 9.4, "Securing WebLogic Server Resources"
- Section 9.5, "Securing Oracle WebCenter Content Resources"

9.1 Choosing a Security Module Type

An Oracle Entitlements Server administrator chooses a Security Module type based on the type of resource being protected. The Security Module type is defined when the Security Module is instantiated using the OES Client's SMConfig Tool (as documented in Chapter 8, "Managing Security Module Configurations").

Note: See the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for OES Client installation instructions.

Instantiation of a Security Module using the SMConfig Tool defines parameters such as the Security Module type, configuration ID and a path to the appropriate container. Table 9–2 lists the Security Module types that can be instantiated. (The SMType attribute value is defined in parentheses in the Security Module column.)

The Security Module types documented in Table 9–1 do not protect resources specific to the environment. They are a Policy Decision Point (PDP) that receives Java calls for authorization. The Security Modules simply provide the authorization API for the application to call.

Table 9–1 General Protection Security Module Types

| Security Module | Purpose | Proxy Mode | Container Support |
|-----------------|---|------------|---|
| Java (java) | Policy Decision Point (PDP) that receives Java calls for authorization | Supported | Used for Java, Standard Edition (JSE) applications and complex integrations |
| WebSphere (was) | Java Security Module that receives authorization requests directly from the application | Supported | WebSphere Application Server |

Table 9–1 (Cont.) General Protection Security Module Types

| Security Module | Purpose | Proxy Mode | Container Support |
|-------------------|--|--|--|
| Web Services (ws) | Multi-Protocol Security Module that accepts Web Services calls; configure other Security Modules (Java, WLS) in proxy mode to communicate with Web Services Security Module using the XACML Gateway or SOAP. | Not supported | Supported as a JSE standalone process or as a web service running on a WebLogic Server container; can be used by other Security Modules in proxy mode; can be used as long as a Web Services request can be built or when an application is built in a non-standard programming language (Python, for example) |
| RMI (rmi) | Multi-Protocol Security Module is a Java Security Module that is enhanced to accept Remote Method Invocation (RMI) calls | Not supported | Use only for JSE applications if Web Services is too heavy |
| .NET (dotnet) | Allows applications written in C# to send authorization requests to the Web Services Security Module by calling the PEP API in C# | Supported in Proxy Mode only; .NET Security Module serves as a proxy that communicates with the Web Services Security Module | .NET containers |
| JBoss (jboss) | Java Security Module that receives authorization requests directly from the application | Supported | JBoss Application Server |
| Tomcat (tomcat) | Java Security Module that receives authorization requests directly from the application; does not support Oracle Platform Security Services authentication/login module or <code>checkPermission</code> | Supported | Apache Tomcat Application Server |

The Security Modules documented in [Table 9–2](#) allow the protection of resources that are specific to the environment in which they are deployed in addition to processing direct authorization calls from the application.

Table 9–2 Environment Specific Security Module Types

| Security Module | Purpose | Proxy Mode | Container Support |
|--------------------------|---|---|-------------------|
| Sharepoint (moss) | Protects Microsoft Sharepoint Server resources by intercepting Sharepoint requests for content; see Section 9.2, "Securing Microsoft Office SharePoint Server Resources" | Supported only in Proxy Mode; Sharepoint Security Module itself serves as a proxy (written in C#) that communicates with the Web Services Security Module | .NET containers |
| WebLogic Server (wls) | Security Module that behaves exactly as Java Security Module unless the Oracle Entitlements Server security providers are enabled (as documented in Section 9.4.1, "Integrating with WebLogic Server") in which case the Security Module can also process WebLogic Server calls; see Section 9.4, "Securing WebLogic Server Resources" | Supported - unless the Oracle Entitlements Server security providers are enabled to intercept WebLogic Server requests. | WebLogic Server |
| Oracle Service Bus (osb) | WebLogic Security Module with Oracle Entitlements Server security providers enabled that intercepts authorization requests from the Oracle Service Bus; see Section 9.3, "Securing Oracle Service Bus Resources" | Supported | |

See [Chapter 8, "Managing Security Module Configurations"](#) for details on these Security Modules and how to configure them. Details on how they work can be found in [Section 1.3, "Overview of the Oracle Entitlements Server Architecture"](#) and [Chapter 7, "Deploying the Policy Decision Point."](#)

9.2 Securing Microsoft Office SharePoint Server Resources

Oracle Entitlements Server enables enterprises to manage MOSS portal environments. Integration with MOSS is provided through the MOSS Security Module plug-in that intercepts authorization calls within the SharePoint Server and sends them to its integrated Web Services Security Module (the PDP). The PDP then returns the authorization decision back to the MOSS Security Module plug-in and the decision is enforced. The following sections have more information.

- [Section 9.2.1, "Protecting SharePoint Resources"](#)
- [Section 9.2.2, "Instantiating the MOSS and Web Services Security Modules"](#)
- [Section 9.2.3, "Integrating and Disintegrating the MOSS Security Module"](#)
- [Section 9.2.4, "Configuring for SharePoint Security"](#)

9.2.1 Protecting SharePoint Resources

SharePoint components that can be secured include web sites, web pages, web parts, list items, navigation bar items and the like. Based on the component, the resource is

protected differently. SharePoint resources are categorized according to the following list.

- *Items* are the smallest SharePoint components; for example, a Document, a Task, a Contact, a Page or an Announcement.
- *Lists* are a collection of a single type of SharePoint component. Document Lists, Contacts Lists, Task Lists and the like can be created.
- *Folders* exist in Lists and serve as a container for multiple Items and sub Folders.
- *Sites* are a collection of Lists. For example, the default SharePoint *Document Center* Site is made up of three Lists: Announcements, Documents and Tasks.
- *Navigation Bar Items* on SharePoint site pages can be used to manipulate MOSS components.

Note: There is only one Resource Type for all MOSS resources. In this section, we use the name `MossResourceType`.

The following sections contain more information.

- [Section 9.2.1.1, "Protecting Web Sites and Web Pages"](#)
- [Section 9.2.1.2, "Protecting Web Parts"](#)
- [Section 9.2.1.3, "Protecting Lists"](#)
- [Section 9.2.1.4, "Protecting Sensitive Content Within Web Pages"](#)

9.2.1.1 Protecting Web Sites and Web Pages

MOSS web sites are composed of one or more web pages. An organization generally organizes one web site in MOSS to denote one department in the company. MOSS comes with a main Web Site within which there are default sub sites. Sub sites appear on the top or side navigation bar or as links on other web pages. All these web sites have their own unique URLs.

The URL of a MOSS Web site or Web page defines the Resource instance created in Oracle Entitlements Server. In the case of a URL defined as `http://Sharepoint_Server_Name/TestSite`, the corresponding Resource is created by defining a `/TestSite` Resource as an instance of the `MossResourceType` Resource Type under the `MossApp` Application. Policies are then created using the Oracle Entitlements Server objects.

A Custom HTTP Module is implemented by Oracle Entitlements Server to secure the MOSS web sites. When a user tries to access a protected component, the request is intercepted by the Custom HTTP Module and forwarded to Oracle Entitlements Server for policy evaluation. The decision is returned to the Custom HTTP Module and if the user is denied access, a Custom Error Page with a message indicating a lack of permissions to view this location is displayed.

Note: Custom HTTP Modules are enabled by defining the `HttpModules` elements in the `web.config` MOSS Site configuration file. See [Section 9.2.4, "Configuring for SharePoint Security."](#)

9.2.1.2 Protecting Web Parts

A MOSS Web Part is similar to a portlet in that it is used to publish content within web pages. A Web page may contain one or more Web Parts. Web Parts are represented in Oracle Entitlements Server by defining their unique MOSS Display Name as the Resource instance name. The Resource instance is created as a child of the parent web page's Resource.

When a user tries to access these protected components the request is intercepted by a MOSS Delegate Control created for Oracle Entitlements Server. In short, a Delegate Control allows you to put any custom .NET code into a SharePoint page without modifying the page itself. This custom code is used to retrieve the decision from Oracle Entitlements Server and remove unauthorized Web Parts from the page. There are no error messages displayed in this case.

Note: Delegate OES Authorization Control is explicitly added to the Web Part pages or implicitly defined in the web site's master page. See [Section 9.2.4, "Configuring for SharePoint Security."](#)

9.2.1.3 Protecting Lists

A MOSS List is a collection of items within a Web Part on a Web page. When creating a MOSS Web site, a set of lists is also created depending upon the template used. Each list item is identified by a URL and represented as an Oracle Entitlements Server Resource. These lists are incorporated into Oracle Entitlements Server based on whether they are *document* lists or *non-document* lists.

- Document Lists can be displayed by going to `http://Sharepoint_Server_Name/TestSite/SharedDocuments/Forms/AllItems.aspx`. Create a top-level Resource named `/TestSite/SharedDocuments/Forms/AllItems.aspx`. Next create individual Resource objects for each item on the list as a sub resource to the top-level Resource. For example, a sub Resource named `/TestSite/SharedDocuments/Scott.sql` can be created for an item on the list named `Scott.sql`.
- Non-document Lists can be displayed by going to `http://Sharepoint_Server_Name/TestSite/Lists/Announcements/AllItems.aspx`. Create a Resource named `/TestSite/Lists/Announcements/AllItems.aspx`. Next create a `/TestSite/Lists/Announcements/EditForm.aspx` Resource and a `/TestSite/Lists/Announcements/DispForm.aspx` Resource at the same level. Now click on any item in the list; the URL appears as `http://Sharepoint_Server_Name/web1/Lists/Announcements/DispForm.aspx?ID=2&Source=http%3A%2F%2Fsharepoint01%2FTestSite%2FLists%2FAnnouncements%2FAllItems%2Easpx`. Note the ID defined as a URL parameter in the URL. This ID will be used as the name of the non-document item and is created as a sub Resource of both `EditForm.aspx` and `DispForm.aspx`. This must be done for all items within a Non-document List. Alternately, hover the mouse over the link of the item and note the ID from the URL displayed in the status bar of the browser.

Note: For list items only, you don't need to write policy on `EditForm.aspx`. You may grant view or ANY on the same `DispForm.aspx`. If view, ReadOnly access is granted; if ANY, full access (edit, delete, and the like) is granted.

9.2.1.4 Protecting Sensitive Content Within Web Pages

The SharePoint server allows administrators to publish custom pages which have sensitive information that need access control. The developer may enclose the sensitive information within ASP tags corresponding to the Oracle Entitlements Server Tag Library. The tag library communicates with Oracle Entitlements Server to retrieve the access decision and, as a result, the content is shown only to authorized users.

Note: The ASP tag library is a server side web control used by a MOSS page developer who registers the namespace, tag-prefix and assembly in the MOSS page and uses the tag to enclose the sensitive content. The library is invoked when an end user tries to access a custom content page on which the tags have been used to provide access control.

9.2.2 Instantiating the MOSS and Web Services Security Modules

The MOSS Security Module works with the Web Services Security Module to provide fine grained authorization for MOSS resources. Before instantiating the Security Modules, ensure that the pre-requisite MOSS environment is already setup. This includes installation of the MOSS and creation of the web application to be protected.

Note: Environment details of the web application (port number, URL and the like) will be needed in this procedure.

The MOSS Security Module and the Web Services Security Module can be deployed on the same or different servers. Instantiation of both Security Modules is achieved using the SMConfig Tool found in the `$ORACLE_CLIENT_HOME/oessm/SMConfigTool/bin` directory.

- To instantiate both the MOSS Security Module and the Web Services Security Module at once, run `config.sh` with the parameter `-smType mossws`.
- To instantiate the Security Modules separately, run `config.sh` twice, first with the parameter `-smType moss` and then with `-smType ws`.

Additionally, run the SMConfigTool based on your deployment choices. For example, to instantiate the Security Modules when they are deployed on the same Windows machine as the MOSS, use the following command:

```
config.sh -smType mossws -prpFileName file_name -mossprpFileName file_name  
-smConfigId -WSListeningPort -pdServer -pdPort
```

where `prpFileName` refers to the `smconfig.prp` used to create the Web Services Security Module and `mossprpFileName` refers to the properties file used to configure the MOSS server.

Note: The `mossprpFileName` template is located at `$ORACLE_CLIENT_HOME/oessm/mosssm /adm/configtool/moss_config.properties`. `moss_config.properties` has mandatory properties that must be defined according to your environment and optional properties that, if not defined, use default values.

To instantiate the Security Modules when they are on separate Windows machines, first instantiate the Web Services Security Module (no special instructions). Then use the following command to configure the MOSS Security Module.

```
config.sh -smType moss -prpFileName file_name -mossprpFileName file_name
```

See the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management* for detailed OES Client installation instructions.

9.2.3 Integrating and Disintegrating the MOSS Security Module

The value of the `moss.enableOES` property in the `mossprpFileName` template can be used to integrate Oracle Entitlements Server with, or disintegrate Oracle Entitlements Server from, the MOSS application.

- If `moss.enableOES=true`, executing `config.sh` with the `-smType moss` parameter will integrate the MOSS application with Oracle Entitlements Server.
- If `moss.enableOES=false`, executing `config.sh` with the `-smType moss` parameter will configure the MOSS application to use its default authorization process.

9.2.4 Configuring for SharePoint Security

The following procedure documents the steps to manually configure authorization for a MOSS application rather than the automatic configuration initiated by `SMConfigTool`. These steps are the same as those automatically executed by the `config.sh` script in [Section 9.2.2, "Instantiating the MOSS and Web Services Security Modules"](#) and can be used instead, by those who prefer not to use the `SMConfigTool`.

This procedure assumes that the Security Modules have been instantiated. After instantiation, note the generated configuration ID and service registry URL. In the following procedure, the `configID` is **MOSS** and the service registry URL is `http://hostname:port/ServiceRegistry`.

1. Use the Oracle Entitlements Server Administration Console to complete the following steps.
 - Create the Web Services Security Module definition.
See [Chapter 10, "Managing System Configurations."](#)
 - Create an Application policy object to represent the MOSS application being protected.
The name of the Application must be consistent with the value of the `moss.app.name` property defined in the `moss_config.properties` file.
See [Chapter 4, "Managing Policies and Policy Objects."](#)
 - Bind this Application to the Web Services Security Module profile.
See [Chapter 10, "Managing System Configurations."](#)
2. Drag and drop `OES.SharePoint.dll` and `log4net.dll` from the `$OES_CLIENT_HOME/oes_sm_instances/MOSS_SM_Name/lib` directory to the `C:/WINDOWS/assembly` directory.

This registers the assemblies in the Windows Global Assembly Cache and makes them available to all .NET applications on the host machine.

3. If using MOSS 2007 (IIS 6), declare the Oracle Entitlements Server Delegate Control by adding the following code to the HTML HEAD section of the `default.master` file.

```
<SharePoint:DelegateControl runat="server" ControlId="PageHeader" />
```

The default.master file is located in the *C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\GLOBAL* directory. This step is not required when using MOSS 2010 (IIS 7).

Caution: When default.master is opened with Wordpad, question mark (?) characters sporadically replace existing characters. Ensure that this is corrected before saving your modified file. Alternately, open the file with Notepad.

4. Add the Custom Error Page to display a message when the user is not authorized to access the MOSS component.

CustError.aspx and custError2010.aspx are the custom Oracle Entitlements Server error pages for MOSS. They are located in the *\$OES_CLIENT_HOME/oes_sm_instances/MOSS_SM_Name/adm/pages* directory.

- If using MOSS 2007 (IIS 6), copy custError.aspx to *C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\template\layouts*.
 - If using MOSS 2010 (IIS 7), copy custError2010.aspx to *C:\Program Files\Common Files\Microsoft Shared\web server extensions\14\template\layouts* and change the name to custError.aspx.
5. Edit the Sharepoint Server web.config configuration file to enable Oracle Entitlements Server-MOSS integration.

web.config is located in the virtual directory of the SharePoint application; for example, *C:\Inetpub\wwwroot\wss\VirtualDirectories\port-number* where *port-number* is the application's port.

Caution: When web.config is opened with Wordpad, question mark (?) characters sporadically replace existing characters. Ensure that this is corrected before saving your modified file. Alternately, open the file with Notepad.

- a. Add the properties documented in [Table 9-3](#) to the appSettings section. [Example 9-1](#) illustrates the appSettings section. Values are taken from the file defined as mossprpFileName.

Example 9-1 appSettings Section of Sharepoint web.config File

```
<add key="SsmUrl" value="{moss.SmUrl}/ServiceRegistry"/>
<add key="SsmId"
      value="{oracle.security.jps.runtime.pd.client.sm_name}"/>
<add key="ApplicationID" value="{application.id}"/>
<add key="PolicyDomain" value="{policy.domain}"/>
<add key="ResourceType" value="{moss.resourcetype}"/>
<add key="log4NetXmlfile" value="{moss.log4NetXmlfile}"/>
<add key="sharepointSite" value="{moss.sharepointSite}"/>
<add key="EnableOES" value="{moss.EnableOES}"/>
<add key="IgnoredExtensions" value="{moss.IgnoredExtensions}"/>
<add key="IgnoredURLExpression" value="{moss.IgnoredURLExpression}"/>
```

Table 9–3 *appSettings Properties for the MOSS Application*

| Property | Value |
|----------------------|---|
| SsmUrl | Registry URL of the Web Service SM; for example, <code>http://oesw2k8:9400/ServiceRegistry</code> |
| SsmId | The name of this Security Module; for example, MOSS |
| IdentityAsserterName | The name of the identity asserter configured in Oracle Entitlements Server. At this time, only <code>OESIdentityAssertion</code> is supported. |
| ApplicationID | The name of the configured Oracle Entitlements Server Application that represents the protected MOSS resource. |
| ResourceType | The Resource Type of all MOSS resources; for example, <code>MossResourceType</code> . The Resource Type of all MOSS components to be protected must be consistent with the value of the <code>moss.resource.type</code> property defined in the <code>moss_config.properties</code> file. |
| log4NetXmlfile | Fully qualified path to the <code>log4Net.xml</code> configuration file. The log file defined in the <code>log4Net.xml</code> file must be located in an existing directory for which Read/Write access has been given to Everyone to allow log messages to be written. |
| sharepointSite | Top level SharePoint site; for example, <code>http://alesw2k8:9581/</code> |
| Enable OES | Flag to enable Oracle Entitlements Server integration; takes true or false as a value |
| IgnoredExtensions | A comma-separated list of file extension patterns to be ignored by Oracle Entitlements Server Access Control; for example, <code>png, js, css, axd</code> Access will always be granted to these resources when requested. |
| IgnoredURLExpression | A comma-separated list of file name patterns to be ignored by Oracle Entitlements Server Access Control; for example, <code>/_layouts/Authenticate.aspx,/_login/default.aspx,/_forms/default.aspx</code> Access will always be granted to these resources when requested. |

- b.** Add the `SafeControl` Assembly entries documented in [Table 9–2](#) to the `SafeControls` section.

Example 9–2 *SafeControl Assembly Entries*

```
<SafeControls>
  ...
  <SafeControl Assembly="OES.Sharepoint, Version=1.0.0.0, Culture=neutral,
    PublicKeyToken=68b08a2fa869dfdc" Namespace="OES.Sharepoint.Controls"
    TypeName="*" Safe="True" />
  <SafeControl Assembly="OES.Sharepoint, Version=1.0.0.0, Culture=neutral,
    PublicKeyToken=68b08a2fa869dfdc" Namespace="OES.Sharepoint.Modules"
    TypeName="*" Safe="True" />
</SafeControls>
```

- c.** Define custom `httpModules` based on the server used.

If using MOSS 2007 (IIS 6), add the following to the `httpModules` section.

```
<add name="CustHTTPModule" type="OES.Sharepoint.Modules.CustHTTPModule,
  OES.Sharepoint, Version=1.0.0.0, Culture=neutral,
```

```
PublicKeyToken=68b08a2fa869dfdc " />
```

If using MOSS 2010 (IIS 7), add [Example 9–3](#) to the assemblies section and [Example 9–4](#) to the modules section (after the last <remove> and before the first <add>).

Example 9–3 add assembly Entry

```
<assemblies>
...
<add assembly="OES.Sharepoint, Version=1.0.0.0, Culture=neutral,
  PublicKeyToken=68b08a2fa869dfdc" />
...
</assemblies>
```

Example 9–4 add name Entry

```
<modules runAllManagedModulesForAllRequests="true">
...
<add name="CustHTTPModule" precondition="integratedMode"
  type="OES.Sharepoint.Modules.CustHTTPModule, OES.Sharepoint,
  Version=1.0.0.0, Culture=neutral, PublicKeyToken=68b08a2fa869dfdc" />
...
</modules>
```

- d. Update the `PageParserPaths` (in the `SafeMode` section) with the virtual path to which custom content is required to be published. The custom content may be authorized via the tag library provided with the solution. [Example 9–5](#) is an example.

Example 9–5 PageParserPaths Entry

```
<PageParserPaths>
  <PageParserPath VirtualPath="/Pages/*" CompilationMode="Always"
    AllowServerSideScript="true" IncludeSubFolders="true"/>
</PageParserPaths>
```

- e. Replace the MOSS `PortalSiteMapProvider` details (illustrated in [Example 9–6](#)) with the Oracle Entitlements Server `PortalSiteMapProvider` details (illustrated in [Example 9–7](#)).

The custom Oracle Entitlements Server `PortalSiteMapProvider` secures the Navigation Bar items.

Example 9–6 MOSS PortalSiteMapProvider

```
<SiteMap>
  <Providers>
    ...
    <add name="GlobalNavigation" description="Provider for MOSS Global Navigation"
      type="Microsoft.SharePoint.Publishing.Navigation.PortalSiteMapProvider,
      Microsoft.SharePoint.Publishing, Version=14.0.0.0, Culture=neutral,
      PublicKeyToken=71e9bce111e9429c" NavigationType="Combined" Version="14" />
    <add name="CurrentNavigation" description="Provider for MOSS Current Navigation"
      type="Microsoft.SharePoint.Publishing.Navigation.PortalSiteMapProvider,
      Microsoft.SharePoint.Publishing, Version=14.0.0.0, Culture=neutral,
      PublicKeyToken=71e9bce111e9429c" NavigationType="Current" Version="14" />
    ...
  </Providers>
```

```
</SiteMap>
```

Example 9–7 Oracle Entitlements Server PortalSiteMapProvider

```
<SiteMap>
  <Providers>
    ...
    <add NavigationType="Combined" Version="1" description="Provider for MOSS
      Global Navigation" name="GlobalNavigation"
      type="OES.Sharepoint.Controls.OESPortalSiteMapProvider, OES.Sharepoint,
      Version=1.0.0.0, Culture=neutral, PublicKeyToken=68b08a2fa869dfdc"/>
    <add NavigationType="Current" Version="1" description="Provider for MOSS
      Current Navigation" name="CurrentNavigation"
      type="OES.Sharepoint.Controls.OESPortalSiteMapProvider, OES.Sharepoint,
      Version=1.0.0.0, Culture=neutral, PublicKeyToken=68b08a2fa869dfdc"/>
    ...
  </Providers>
</SiteMap>
```

- f. Restart IIS server for above changes to reflect in IIS server.
6. Copy the OESAAuthorizationFeature directory to the MOSS FEATURES directory.
 - If using MOSS 2007 (IIS 6), copy the `$OES_CLIENT_HOME/oes_sm_instances/MOSS_SM_Name/lib/OESAAuthorizationFeature` directory to the `C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\TEMPLATE\FEATURES` directory.
 - If using MOSS 2010 (IIS 7), copy the `$OES_CLIENT_HOME/oes_sm_instances/MOSS_SM_Name/lib/OESAAuthorizationFeature2010` directory to the `C:\Program Files\Common Files\Microsoft Shared\web server extensions\14\TEMPLATE\FEATURES` directory and change the directory name to OESAAuthorizationFeature.
7. Install and activate OESAAuthorizationFeature for the specified site using one of the following commands.

The OES Authorization Feature can be activated separately for each web and sub-web site by going to Site Settings -> Modify All Site Settings -> Site Features. If it is activated against a sub-web, all web parts in the web pages inside the sub-web may be access controlled.

- If using MOSS 2007 (IIS 6), open a command prompt and execute the following commands.

```
"C:\Program Files\Common Files\Microsoft Shared\web server
extensions\12\BIN\STSADM.EXE" -o installfeature -name
OESAAuthorizationFeature
```

```
"C:\Program Files\Common Files\Microsoft Shared\web server
extensions\12\BIN\STSADM.EXE" -o activatefeature -name
OESAAuthorizationFeature -url http://alesw2k3:9581
```

- If using MOSS 2010 (IIS 7), open a command prompt and execute the following commands:

```
"C:\Program Files\Common Files\Microsoft Shared\web server
extensions\14\BIN\STSADM.EXE" -o installfeature -name
OESAAuthorizationFeature
```

```
"C:\Program Files\Common Files\Microsoft Shared\web server
```

```
extensions\14\BIN\STSADM.EXE" -o activatefeature -name
OESAuthorizationFeature -url http://aleswin2k8:9581
```

8. Restart the IIS Server.
9. Obtain a list of all the SharePoint server protected resources using `MOSSResourceDiscovery.exe` located in the `%OES_CLIENT_HOME%\oessm\mosssm\lib` directory.

Note: MOSS resources are mapped hierarchically to resources in Oracle Entitlements Server. Thus, all discovered resources need not to be defined in the policy store. For example, rather than copying 10,000 individual document names, copy the name of the folder in which these documents are located and write policies using a Resource Name Expression; for example, `/lib/*`.

The MOSS Security Module contains this executable to generate a plain text file named `object1` and an XML file named `discovered-jazn-data.xml`. Both files define the MOSS resources. The `MOSSResourceDiscovery.exe` executable prompts for the following information.

- The path to a directory in which the files will be created; for example, `c:\inetpub\wwwroot\wss\VirtualDirectories\9581\policy`. This directory must be created beforehand.
- The path to the directory in which the Admin Url file is located; for example, `$(OES_CLIENT_HOME)/oessm/mosssm/adm/Discovery/AdmUrls.txt`.
- The Sharepoint Server site URL; for example, `http://amw2k8:9581`. Do not append the URL with a forward slash (/).
- The name of the Oracle Entitlements Server Application object that represents the MOSS application; for example, `MossApp`.
- The name of the Oracle Entitlements Server Resource Type; this value should always be `MossResourceType`.

The XML file can be used by the policy migration tool. See [Section 13.5, "Migrating Policies"](#) for details. The text file is used to import the resources into the Oracle Entitlements Server policy store in the next step.

10. Import the MOSS resources into the Oracle Entitlements Server policy store by using the text file as input to `manage-policy.cmd|sh`, the policy management tool.

`manage-policy.cmd|sh` is located in the `%OES_CLIENT_HOME%\oessm\bin` directory. The import appends the MOSS resources to the policy store; any existing MOSS Applications (and related policies) will not be deleted. The input values (Application name, Resource Type and generated resource file) should be consistent with the input used by `MOSSResourceDiscovery.exe` in the previous step.

Before running `manage-policy.cmd|sh`, modify the script as follows:

- Change the `OES_CLIENT_HOME` and `OES_INSTANCE_NAME` variables to reflect the user's environment.
- Configure the `jps-config.xml` Policy Store attributes as defined in [Appendix A.4, "Policy Store Service Configuration."](#)

This tool is only run once. New resources are manually created using the Administration Console.

11. Distribute the policies using the Administration Console.

9.3 Securing Oracle Service Bus Resources

Oracle Service Bus (OSB) is designed to centrally manage and control many distributed service endpoints. Oracle Entitlements Server enables an enterprise to control access to OSB runtime resources, allowing them to become accessible only after authorization. In general, OSB runtime resources are those resources passed to the `isAccessAllowed()` authorization API.

Note: Oracle Entitlements Server does not secure resources used during OSB configuration such as the OSB console.

The following sections contain detailed information on the OSB resource object and how to map its values to Oracle Entitlements Server policy objects.

- [Section 9.3.1, "Examining the OSB Resource Object"](#)
- [Section 9.3.2, "Mapping Message Level OSB Resources to Oracle Entitlements Server"](#)
- [Section 9.3.3, "Mapping Transport Level OSB Resources to Oracle Entitlements Server"](#)
- [Section 9.3.4, "Enabling the WebLogic Server Providers"](#)

9.3.1 Examining the OSB Resource Object

OSB runtime resources are represented as objects. The object representing the resource contains a string array of `KEYS` that define values representing the object's context; for example, the OSB project or task. In order to secure OSB resources, the creation of Oracle Entitlements Server security objects used to define an Authorization Policy must mirror the values that will be passed in the resource object's `KEYS`. The following list are the `KEYS` that will be defined in an OSB resource object. The type of this OSB resource object is always `<alsb-proxy-service>`.

- **proxy** defines the name of the OSB proxy service associated with the protected resource. The value uniquely identifies one OSB proxy service.
- **path** defines the full path to the OSB proxy service; for example, `Project-name/Folder-name` where:
 - *Project-name* is the name of the OSB project with which the proxy service is associated.
 - *Folder-name* is an optionally defined directory structure for the proxy service. Multiple directories may be defined using the `/` string separator as in `/folder_name/sub_folder_name`.

The value uniquely identifies the same OSB proxy service as the one referenced for **proxy**.

- **action** defines whether entry to the OSB proxy service will be secure or not and takes one of the following values:
 - *invoke* represents access control on entry to an OSB proxy service.
 - *wss-invoke* represents secure access control on entry to an operation of an OSB proxy service. With this action, OSB Web Service Security is configured.

- **operation** defines the name of the Web service operation being invoked. If the **action** is *invoke*, this value is null.

Note: When the OSB proxy service uses Web Service Security, OSB performs security checks at the transport layer and the message layer. At the transport layer, OSB checks if the user is allowed to access the proxy service; at the message layer, it checks if the user is allowed to do the specified proxy service operation. Thus, if no user information is passed into the transport layer, an additional policy will be needed to grant access privileges to the Anonymous role.

Mapping OSB resources to Oracle Entitlements Server policy objects is dependent on the chosen secure or non-secure **action**. See [Section 9.3.2, "Mapping Message Level OSB Resources to Oracle Entitlements Server"](#) and [Section 9.3.3, "Mapping Transport Level OSB Resources to Oracle Entitlements Server"](#) for details.

9.3.2 Mapping Message Level OSB Resources to Oracle Entitlements Server

When the OSB resource object defines a *wss-invoke* action, the applicable OSB proxy service uses OSB Web Service Security. Let's assume an OSB proxy service named `SampleProxyService` is associated with the OSB project named `SampleProject` and is configured to use OSB Web Service Security. This service resource is in the `Mortgage/ProxyService` folder. Thus, the `KEYS` values are as follows:

- `path`: `SampleProject/Mortgage/ProxyService`
- `proxy`: `SampleProxyService`
- `action`: `wss-invoke`
- `operation`: `sayHello` (Suppose the Web Service action is `sayHello`)

Based on the `KEYS` values, the Oracle Entitlements Server object values are:

- **Application** - It is mandatory to name the Application used for securing OSB resources as `alsbProxyServices`.
- **Resource Type** - This value should always be the OSB object type `alsb-proxy-service`. Also select *yes* as the value of the `Supports Resource Hierarchy` parameter.

Note: It is not necessary to add `wss-invoke` as an action for the `alsb-proxy-service` Resource Type; just select the operation for the policy.

- **Resource** - `SampleProject/Mortgage/ProxyService/SampleProxyService/sayHello` (takes a value equal to the values of the OSB resource object's *path/proxy* `KEYS` values)
- **Action** - `access` (*access*, the default Oracle Entitlements Server privilege, is always used)

9.3.3 Mapping Transport Level OSB Resources to Oracle Entitlements Server

When the OSB resource object defines an *invoke* action, the applicable OSB proxy service does not use OSB Web Service Security. Let's assume an OSB proxy service resource named `SampleProxyService` that is associated with the OSB project named

SampleProject. This service resource is in the Mortgage/ProxyService folder. Thus, the KEYS values are as follows:

- path: SampleProject/Mortgage/ProxyService
- proxy: SampleProxyService
- action: invoke
- operation: null

Based on the KEY values, if not configured with OSB Web Service Security, the Oracle Entitlements Server object values are:

- Application - alsbProxyServices (the OSB resource object does not have a defined value so this default value is used)
- Resource Type - This value should always be the OSB object type `alsb-proxy-service`. Also select *yes* as the value of the Supports Resource Hierarchy parameter.
- Resource - SampleProject/Mortgage/ProxyService/SampleProxyService (takes a value equal to the values of the OSB resource object's *path/proxy* KEYS values)
- Action - `transport_level_access` (if *operation* has a value, this value is used; if not, access, the default Oracle Entitlements Server privilege, is used)

9.3.4 Enabling the WebLogic Server Providers

The Oracle Entitlements Server Proxy Provider must be enabled to secure and protect OSB runtime resources as well. [Section 9.4.1, "Integrating with WebLogic Server"](#) contains the procedure for accomplishing this.

9.4 Securing WebLogic Server Resources

Besides providing the authorization API to accept authorization requests, the WebLogic Server Security Module allows protection of WebLogic Server-specific resources after configuring the specific Oracle Entitlements Server Authorization and Role Mapping providers. The following high-level procedure documents the tasks to secure WebLogic Server resources.

1. Enable the Authorization and Role Mapping providers.
See [Section 9.4.1, "Integrating with WebLogic Server."](#)
2. Discover the resources to be protected with Discovery Mode.
See [Section 9.4.2, "Discovering WebLogic Server Resources."](#)
3. Define the WebLogic Server-specific resources as Oracle Entitlements Server objects.
See [Section 9.4.3, "Converting WebLogic Server Resources"](#) and [Section 9.4.4, "Mapping WebLogic Server Resources to Policy Objects."](#)
4. Configure the appropriate Authorization and Role Mapping policies.
See [Chapter 4, "Managing Policies and Policy Objects."](#)
5. Distribute the policies to the Security Module.
See [Chapter 6, "Managing Policy Distribution."](#)

9.4.1 Integrating with WebLogic Server

As discussed in [Section 1.3.2.2, "Security Module as Combination PDP / PEP,"](#) WebLogic Server can automatically intercept authorization requests after enabling the Role Mapping and Authorization providers. The following procedure explains how to do this; it assumes the WebLogic Server is installed in the \$WLS directory in the \$DOMAIN domain. Replace the values based on your installation when following the procedure.

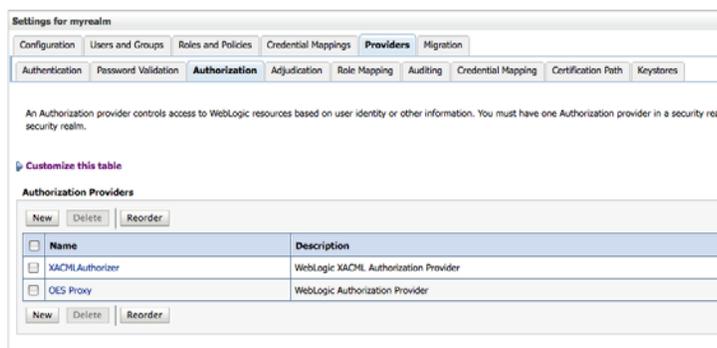
1. Start the \$DOMAIN domain using the following command.

```
$DOMAIN/startWeblogic.sh
```

2. Add the Authorization Proxy and Role Mapping providers to the realm that protects the domain.

[Figure 9–1](#) is a screenshot of the WebLogic Server console that illustrates this.

Figure 9–1 Adding Providers to the WebLogic Server Domain's Realm



3. Restart the domain.

After enabling the providers, see [Section A.2.5, "WebLogic Server Security Module"](#) for the configuration parameters.

9.4.2 Discovering WebLogic Server Resources

When writing policy to secure an application's resources, all resources that must be secured must be *discovered*. By running the WebLogic Server Security Module in Discovery Mode and opening one or more user sessions (to track usage), the application's resources can be defined. (Discovery Mode does not authorize; it discovers objects to be protected.) Based on the activities performed during the user session, Oracle Entitlements Server will generate an initial policy set (that defines all resources to be protected); this policy set can then be imported into the policy store.

Note: The generated files are meant to serve as a starting point for defining a policy set to fully secure the application. In particular:

- The recorded policy data is based only on requests made during the user session; no policy data will be generated for parts of the application that are not used.
 - Depending on the Resource hierarchy you use to define the application's resources, the imported policy set may contain more Resources than actually needed.
-
-

Resource discovery is enabled when the Authorization and Role Mapping providers run in Discovery Mode. In this mode, these providers always return *true* when evaluating user requests and generate the initial policy files based on those requests. Discovery Mode may find Applications, Resource Types (and corresponding actions), the Resource Type `matcherClass` name, and Resources. The following sections contain more information.

- [Section 9.4.2.1, "Enabling Discovery Mode"](#)
- [Section 9.4.2.2, "Loading Discovered Resources"](#)

9.4.2.1 Enabling Discovery Mode

By default, Discovery Mode is off. Setting the `oracle.security.jps.discoveryMode` property to `true` (in `jps-config.xml`) enables the feature. Adding a directory value for the `oracle.security.jps.discoveredPolicyDir` property defines where the policy set will be written.

Note: Discovery Mode does not generate parent Resources for hierarchical Resource Types. If the administrator knows that all Resource Types to be discovered are hierarchical, add the appropriate values to the optional `oracle.security.jps.discoveredResourceIsHierarchical` and `oracle.security.jps.discoveredResourceNameDelimiter` properties.

See [Appendix A, "Installation and Configuration Parameters"](#) for additional details on these configuration parameters.

9.4.2.2 Loading Discovered Resources

The resulting Discovery Mode file follows the `jazn-data.xml` schema and is a standard XML policy store file as illustrated in [Example 9–8](#). Use the Oracle Entitlements Server API to create the discovered objects as Authorization Policy objects in the policy store. See [Section 13.5, "Migrating Policies"](#) for information.

Example 9–8 Sample File Of Discovered Resources

```
<?xml version = '1.0' encoding = 'UTF-8' standalone = 'yes'?>
<jazn-data xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation=
    "http://xmlns.oracle.com/oracleas/schema/jazn-data-11_0.xsd">
<policy-store>
  <applications>
    <application>
```

```

<name>addConfRes#V2.0</name>
  <resource-types>
    <resource-type>
      <name>FileResourceType</name>
      <matcher-class>oracle.security.jps.JpsPermission</matcher-class>
      <actions-delimiter>,</actions-delimiter>
      <actions>delete,write,read</actions>
    </resource-type>
    <resource-type>
      <name>ResType1</name>=
      <actions-delimiter>,</actions-delimiter>
      <actions>write,read</actions>
    </resource-type>
  </resource-types>
  <resources>
    <resource>
      <name>EmpInfo</name>
      <type-name-ref>FileResourceType</type-name-ref>
    </resource>
    <resource>
      <name>resource1</name>
      <type-name-ref>ResType1</type-name-ref>
    </resource>
  </resources>
</application>
</applications>
</policy-store>
</jazn-data>

```

9.4.3 Converting WebLogic Server Resources

This section describes how Oracle Entitlements Server converts the different resource types supported by WebLogic Server and how they are represented in the Oracle Entitlements Server Administration Console. A WebLogic Server resource is an object that the WebLogic Security Service creates to represent an underlying WebLogic Server entity; it is used to determine who can access the entity.

An Authorization Policy defines, among other objects, a top-level Application, a Resource Type and the actual Resource to be protected. The objects may include those documented in [Table 9-4](#).

Table 9-4 WebLogic Server Authorization Policy Objects

| Node | Description |
|---------------|--|
| Application | The Application corresponds to the application with which the Resource is associated. Not every resource belongs to a specific Application; for example, a JDBC resource does not. In these cases, <i>shared</i> substitutes for the name of the Application. The Application name is defined when the Application is created using the Administration Console; for example, <i>MyEjbApplication</i> . |
| Resource Type | The Resource Type corresponds to the supported WebLogic Server resource types as defined in Section 9.4.4 . The Resource Type name is defined when the Resource Type is created using the Administration Console; for example, <i>ejb</i> . A Resource Type can be defined as hierarchical or flat. |
| Resource | The Resource is the instance of the Resource Type that is being protected. The Resource can be hierarchical (as a directory in which protection is afforded to all contents) or a specific file. The Resource Type from which the Resource instance is created must first be defined as hierarchical. |

9.4.4 Mapping WebLogic Server Resources to Policy Objects

This section describes how to map Oracle Entitlements Server policy objects to WebLogic Server resources defined for common external resources. WebLogic Server supports the following Resource Type values: `adm`, `app`, `com`, `eis`, `ejb`, `jdbc`, `jms`, `jndi`, `ld`, `svr`, `url`, `web`, `webservices`. It contains information on the following types of resources.

- Section 9.4.4.1, "Enterprise Java Bean Resources"
- Section 9.4.4.2, "Java Naming and Directory Interface Resources"
- Section 9.4.4.3, "URL Resources"
- Section 9.4.4.4, "JDBC Resources"
- Section 9.4.4.5, "JMS Resources"
- Section 9.4.4.6, "Web Services Resources"
- Section 9.4.4.7, "Server Resources"

9.4.4.1 Enterprise Java Bean Resources

When defining objects for a policy that will be used to protect an Enterprise Java Bean (EJB) resource, policy objects should be named based on values defined in the standard EJB deployment descriptor, `ejb-jar.xml`. [Example 9–9](#) illustrates how one EJB named `AccountService` might be defined.

Example 9–9 Defining an EJB Resource in `ejb-jar.xml`

```
<enterprise-beans>
<!-- Session Beans -->
  <session>
    <display-name>AccountService</display-name>
    <ejb-name>AccountService</ejb-name>
    <home>com.bea.security.examples.ejb.AccountServiceHome</home>
    <remote>com.bea.security.examples.ejb.AccountService</remote>
    <ejb-class>ejb.AccountServiceSession</ejb-class>
    <session-type>Stateless</session-type>
    <transaction-type>Bean</transaction-type>
  </session>
</enterprise-beans>
```

[Table 9–5](#) contains the mappings that should be used when defining policy objects for use with an EJB resource.

Table 9–5 Mapping EJB Definitions to Policy Objects

| Policy Object Name | EJB Definition |
|--------------------|---|
| Application | Same as the EJB name; in this case, <code>AccountService</code> |
| Resource Type | Use the value <code>ejb</code> |
| Resource name | <p><code>ejb_name/method_name</code> where:</p> <ul style="list-style-type: none"> ■ <code>ejb_name</code> is the name of the EJB ■ <code>method_name</code> is the name of the invoked method <p>The EJB method is part of the resource URL. The Resource action is always <code>execute</code>.</p> |

The following list documents the attributes supported by JNDI resources that can be used as a part of a Condition in an Authorization Policy. See [Section 4.6, "Using the Condition Builder"](#) for details.

- application: name of the application
- module: name of the module
- ejb: name of the EJB
- method: name of the method
- method interface: Takes as a value Home, Remote, LocalHome, or Local
- Param N : A value of the N th parameter in the method; for example, Param1, Param2...

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#) for more details.

9.4.4.2 Java Naming and Directory Interface Resources

When defining objects for a policy that will be used to protect Java Naming and Directory Interface (JNDI) based resources, policy objects should be named based on values defined in the WebLogic-specific deployment descriptor, `weblogic-ejb-jar.xml`. [Example 9–10](#) illustrates how an EJB named `AccountService` might be defined with a JNDI name.

Example 9–10 Defining a JNDI Resource in `weblogic-ejb-jar.xml`

```
<weblogic-ejb-jar>
  <weblogic-enterprise-bean>
    <ejb-name>AccountService</ejb-name>
    <stateless-session-descriptor></stateless-session-descriptor>
    <reference-descriptor></reference-descriptor>
    <jndi-name>AccountService</jndi-name>
  </weblogic-enterprise-bean>
</weblogic-ejb-jar>
```

[Table 9–6](#) contains the mappings that should be used when defining policy objects for use with a JNDI based resource.

Table 9–6 Mapping JNDI Definitions to Policy Objects

| Policy Object Name | JNDI Definition |
|--------------------|-----------------|
| Application | shared |
| Resource Type | jndi |
| Resource | Not used |

The action for a JNDI call is the JNDI action name. The value can be one of the following.

- `modify` is required whenever an application modifies (add, remove, change) the JNDI tree in any way. This includes the `bind()`, `rebind()`, `createSubContext()`, `destroySubContext()`, and `unbind()` methods.

- `lookup` is required whenever an application looks up an object in the JNDI tree. This includes the `lookup()` and `lookupLink()` methods.
- `list` is required whenever an application lists the contents of a context in JNDI. This includes the `list()` and `listBindings()` methods.

The following list documents the attributes supported by JNDI resources that can be used as a part of a Condition in an Authorization Policy. See [Section 4.6, "Using the Condition Builder"](#) for details.

- `application` - Always *shared*
- `path` - The JNDI resource path
- `action` - the JNDI action name (`modify` | `lookup` | `list`)

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#) for more details.

9.4.4.3 URL Resources

A URL (Web) resource is a specific WebLogic Server resource related to Web applications. To secure Web applications, create Authorization Policies for a Web Application archive (WAR) or for individual components of the Web application (such as servlets and JSPs). [Table 9–7](#) describes how to name the Oracle Entitlements Server objects when securing a URL resource. These values are defined when the objects are created using the Oracle Entitlements Server Administration Console.

Table 9–7 URL Resource Values Mapped to Oracle Entitlements Server Objects

| OES Object Name | URL Resource Value |
|-----------------|---|
| Application | Takes as a value the web application name (defined in the WebLogic Server configuration file) that is (or contains) the resource; for example, <code>bankapp</code> . |
| Resource Type | Takes as a value one of the supported resource types; in this case, <code>url</code> . |
| Resource parent | Takes as a value the context path of the web application as defined in the WebLogic Server configuration file. In the following examples, the context path is defined as <code>/currencyExchange</code> for the first two policies and <code>/mybroker</code> for the last two. |
| Resource | Takes as a value the resource URI after the context path. In this case, <code>currentRates.jsp</code> . |

To illustrate how to create an Authorization Policy for a URL resource, let's assume we want to protect Web resources accessible through different banking related JSP. The WebLogic Server configuration file references the web application name as `bankapp` with the context path `/currencyExchange` (for the first two policies) and `/mybroker` (for the last two policies). In the case of a URL resource, the action name is mapped to the HTTP request method name (`GET`, `POST`, `PUT`, `HEAD`, `DELETE`, `TRACE`, `CONNECT`, and the like).

The first Authorization Policy example grants any unauthorized user (anonymous) permission to view current currency exchange rates (`currentRates.jsp`) if the connection through which the page is being accessed is secure (HTTPS). Create the following objects using the Administration Console:

- Application = `bankapp`

- Resource Type = url
- Resource = currencyExchange/currentRates.jsp
- Action = GET
- User = anonymous (unauthorized)
- Condition = if issecure=yes

Notice the *GET* action is part of the Authorization Policy; it is not the action of the Authorization Policy. The full range of actions allowed on the Resource Type are always defined as part of the Resource Type profile. The policy action is always equal to GRANT or DENY.

The second Authorization Policy example grants any member of the Manager role permission to post new currency exchange rates (`postNewRates.jsp`) if the user updates the data from the local machine. Create the following objects using the Administration Console:

- Application = bankapp
- Resource Type = url
- Resource = currencyExchange/postNewRates.jsp
- Action = POST
- Role = Manager
- Condition = if remotehost="localhost"

Notice the *POST* action is part of the Authorization Policy; it is not the action of the Authorization Policy. The full range of actions allowed on the Resource Type are always defined as part of the Resource Type profile. The policy action is always equal to GRANT or DENY.

The third Authorization Policy example grants access to `buyStocks.jsp` if the customer has positive purchasing power. The page will not be displayed if a customer's purchasing power is not positive. To decipher purchasing power, when the customer clicks the `buyStocks.jsp` link, the browser sends an HTTP request mapped to a Java servlet. The servlet sets a request attribute named `purchasingPower` and forwards the request to a second page that is responsible for fetching balances from all of the customer's accounts, calculating the amount of money that can be spent on buying new stocks (purchasing power) and populating the `purchasingPower` attribute with a value. Create the following objects using the Administration Console:

- Application = bankapp
- Resource Type = url
- Resource = mybroker/buyStocks.jsp
- Action = GET
- Role = Client
- Condition = if purchasingPower>0

Notice the *GET* action is part of the Authorization Policy; it is not the action of the Authorization Policy. The full range of actions allowed on the Resource Type are always defined as part of the Resource Type profile. The policy action is always equal to GRANT or DENY.

The fourth Authorization Policy allows a customer to open an account for trading stocks only if the Trading Agreement has been accepted (by ticking the checkbox).

After clicking the `openAccount.jsp` link, the first page displayed contains the Trading Agreement and asks the customer to accept it. The checkbox is linked to an HTML form parameter named `customerAgreed`. When the HTML form is posted, this parameter is set to true if the customer has accepted the trading agreement. The policy checks for this value in the `customerAgreed` HTTP request parameter. Create the following objects using the Administration Console:

- Application = bankapp
- Resource Type = url
- Resource = mybroker/openAccount.jsp
- Action = POST
- Role = Client
- Condition = if Not customerAgreed="true"

Notice the `POST` action is part of the Authorization Policy; it is not the action of the Authorization Policy. The full range of actions allowed on the Resource Type are always defined as part of the Resource Type profile. The policy action is always equal to GRANT or DENY.

[Table 9–8](#) documents the dynamic attributes supported by URL resources that can be used as a part of a Condition in an Authorization Policy. See [Section 4.6, "Using the Condition Builder"](#) for details.

Table 9–8 Dynamic Attributes Supported by URL Resources

| Attribute Name | Value |
|--------------------|--|
| application | The name of the web application. |
| contextpath | The context path of the web application. |
| uri | The URI of the resource. |
| httpmethod | The HTTP method (same as action). |
| transporttype | The transport guarantee required to access the URL resource, as it appears in the corresponding <code><transport-guarantee></code> element in the deployment descriptor. The value can be one of INTEGRAL or CONFIDENTIAL. |
| authtype | The name of the authentication scheme used to protect the servlet. The value can be one of: BASIC, FORM, CLIENT_CERT or DIGEST. |
| pathInfo | Extra path information associated with the URL sent by the client when it made a request. |
| pathtranslated | Extra path information after the servlet name but before the query string is translated to a real path. |
| querystring | The query string that is contained in the request URL after the path. |
| remoteuser | The login of the user making the request, if the user has been authenticated. |
| requestedsessionid | The session ID specified by the client. |
| requesturi | The part of this request's URL from the protocol name up to the query string in the first line of the HTTP request. |
| requesturl | The URL used by the client to make the request. The returned URL contains a protocol, server name, port number, and server path, but it does not include query string parameters. |
| servletpath | The part of this request's URL that calls the servlet. |

Table 9–8 (Cont.) Dynamic Attributes Supported by URL Resources

| Attribute Name | Value |
|-------------------|---|
| characterencoding | The character encoding used in the body of the request. |
| contenttype | The MIME type of the body of the request. |
| locale | The preferred Locale of the client. |
| protocol | The name and version of the protocol, for example, HTTP/1.1. |
| remoteaddr | The Internet Protocol address of the client or last proxy that sent the request. |
| remotehost | The fully qualified name of the client or the last proxy that sent the request. |
| scheme | The name of the scheme used to make this request, for example, http, https, or ftp. |
| servername | The host name of the server to which the request was sent. |
| serverport | The port number to which the request was sent. |
| issecure | A boolean indicating whether this request was made using a secure channel, such as HTTPS. |

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#) for more details.

HTTP requests may contain elements such as servlet attributes, URL query parameters, HTTP request headers and cookies. These elements, available as name/value pairs, can be mapped to dynamic attributes.

Note: The attributes that correspond to servlet attributes, URL query parameters, HTTP request headers and cookies are case insensitive; however, an assumption that the attribute names are case sensitive will slightly improve the performance.

The order in which the framework searches for a matching attribute is:

1. URL query parameters - are name/value pairs appended to a URL. The attribute names that correspond to the parameters in a URL query string are the same as the parameter names. The names are represented as strings and are case insensitive. The attributes refer to the query string variable encoded within the request. For example, if a URL includes a query such as `?test=endcoded%20char`, the parameter can be accessed in the Condition of an Authorization Policy as: `"if test= "encoded char"`
2. Servlet attributes - are name/value pairs that can be added to a request internally by a servlet container. Usually this is accomplished by calling the `setAttribute` method of the `ServletRequest` interface. The policy attribute names correspond to the names of servlet attributes, and are represented as strings and case insensitive.
3. HTTP request headers - The attribute name of an HTTP request header corresponds to the name of the header. The name is returned as a string and is case

insensitive. Examples of the available headers are: date, if-modified-since, referrer, or user-agent. (The date header, usually a date type, is returned as a string.)

4. cookies - The attribute names that correspond to cookies in an HTTP request are the same as the cookie name in the request. The names are returned as strings and case insensitive. The value of the cookie returned is application-specific and may need further decoding.

Note: If the names of a servlet attribute, URL query parameter, HTTP request header or cookie collide, only one attribute will be available in policy constraints.

9.4.4.4 JDBC Resources

A Java DataBase Connectivity (JDBC) resource is a WebLogic Server resource that is related to JDBC. You can secure JDBC resources that are deployed as a service or as an application. To secure JDBC database access, create Authorization Policies for all data sources as a group, individual data sources, and multiple data sources. [Example 9–11](#) shows how a JDBC resource named `MyJDBCConnectionPool` could be defined in the WebLogic Server configuration file, `config.xml`.

Example 9–11 Defining a JDBC Resource in config.xml

```
<JDBCConnectionPool DriverName="oracle.jdbc.driver.OracleDriver"
    Name="MyJDBCConnectionPool"
    PasswordEncrypted="{3DES}B2B1+tp70Eh3D1pT53/anw=="
    Properties="user=wles" Targets="myserver"
    TestTableName="SQL SELECT 1 FROM DUAL"
    URL="jdbc:oracle:thin:@localhost:1521:ASI"/>
<JDBCTxDataSource JNDIName="MyDataSource"
    Name="MyJDBCDataSourceName"
    PoolName="MyJDBCConnectionPool"
    Targets="myserver"/>
```

[Table 9–9](#) describes how to name the Oracle Entitlements Server objects in the case of securing the JDBC resource, `MyJDBCConnectionPool`. These values are defined when the objects are created using the Oracle Entitlements Server Administration Console

Table 9–9 JDBC Values Mapped to Oracle Entitlements Server Objects

| OES Object Name | JDBC Value |
|-----------------|--|
| Application | A JDBC resource does not belong to a specific Application. In these cases, shared substitutes for the name of the Application. The Application, shared, is defined when the Application is created using the Administration Console. |
| Resource Type | Takes as a value one of the supported resource types; in this case, <code>jdbc</code> . |
| Resource parent | Takes as a value the module name (if any) plus the pool type (ConnectionPool or MultiPool); in this case, <code>ConnectionPool</code> . |
| Resource | Takes as a value the name of the JDBC resource as defined in <code>config.xml</code> . In this case, <code>MyJDBCConnectionPool</code> . |

To illustrate how to create policy objects using Oracle Entitlements Server for a JDBC resource, let's assume we want to grant members of the `ExternalApplication` role permission to reserve (open) a JDBC connection from a connection pool called `ExternalDataPool`. Create the following objects using the Administration Console:

- Application = shared
- Resource Type = jdbc
- Resource = ConnectionPool/ExternalDataPool
- Action = reserve

This second group of objects will be used in a policy to grant members of the Admin role permission to shut down any JDBC resource except the resource named `SystemJdbcPool`. Create the following objects using the Administration Console:

- Application = shared
- Resource Type = jdbc
- Resource = ConnectionPool/ExternalDataPool
- Action = admin
- Condition = if Not resource="SystemJdbcPool"

Notice the *reserve* and *admin* actions are part of the Authorization Policies; it is not the action of the Authorization Policy. The full range of actions allowed on the Resource Type are always defined as part of the Resource Type profile. The policy action is always equal to GRANT or DENY. [Table 9–10](#) documents the specific actions that can be performed on a JDBC resource and thus must be defined as actions of the Resource Type.

Table 9–10 JDBC Resource Action Options

| Action Name | Operation |
|-------------|---|
| admin | Action to perform the admin operations such as <code>clearStatementCache</code> , <code>suspend</code> , <code>forceSuspend</code> , <code>resume</code> , <code>shutdown</code> , <code>forceShutdown</code> , <code>start</code> , <code>getProperties</code> , and <code>poolExists</code> . |
| reserve | Action to reserve a connection in the data source by looking up the data source and then calling <code>getConnection</code> . |
| shrink | Action to shrink the number of connections in the data source. |
| reset | Action to reset the data source connections by shutting down and re-establishing all physical database connections. |

[Example 9–12](#) is sample code that uses the JDBC resource previously defined. It calls the `getConnection()` method on the data source instance. This initiates an authorization check to verify the reserve action against the `//app/policy/AppParentNode/shared/jdbc/ConnectionPool/MyJDBCConnectionPool` resource.

Example 9–12 Initiating Authorization on JDBC Resource

```

javax.naming.InitialContext initialContext = new javax.naming.InitialContext();
javax.sql.DataSource ds = (javax.sql.DataSource)
initialContext.lookup("MyDataSource");
java.sql.Connection conn = ds.getConnection();
PreparedStatement statement =
conn.prepareStatement("SELECT accountName FROM accounts WHERE balance < 0");
ResultSet result = statement.executeQuery();
if (result.next()) {
    String accountName = result.getString(1);
    System.out.println("The first account with negative balance is " +
accountName);
}
    
```

}

Table 9–11 documents the attributes supported by JDBC resources that can be used as a part of a Condition in an Authorization Policy. See Section 4.6, "Using the Condition Builder" for details.

Table 9–11 Dynamic Attributes Supported by JDBC Resources

| Attribute Name | Element |
|----------------|--|
| application | The name of an application that hosts the resource |
| module | The name of a module to which the resource belongs |
| category | The resource type (ConnectionPool MultiPool) |
| resource | The name of the resource |
| action | The JDBC operation name (admin reserve shrink reset) |

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See Section 4.5.9, "Managing Attributes and Functions as Extensions" for more details.

9.4.4.5 JMS Resources

A Java Messaging Service (JMS) resource is a WebLogic Server resource related to JMS. You can secure JMS resources that are deployed as a service or as an application. To secure JMS destinations, create Authorization Policies for all destinations (JMS queues and JMS topics) as a group, or individually (one JMS queue or JMS topic on a JMS server). Table 9–12 describes how to name the Oracle Entitlements Server objects in the case of securing a JMS resource. These values are defined when the objects are created using the Oracle Entitlements Server Administration Console.

Table 9–12 JMS Values Mapped to Oracle Entitlements Server Objects

| OES Object Name | JMS Value |
|-----------------|---|
| Application | A JMS resource does not belong to a specific Application. In these cases, shared substitutes for the name of the Application. The Application, shared, is defined when the Application is created using the Administration Console. |
| Resource Type | Takes as a value one of the supported resource types; in this case, jms. |
| Resource parent | The destination type (topic or queue) |
| Resource | The resource name |

Example 9–13 configures a JMS queue named `MyJMSQueue` in the WebLogic Server configuration file, `config.xml`.

Example 9–13 Defining a JMS Queue Resource in config.xml

```
<JMSServer Name="WSSStoreForwardInternalJMSServermyserver"
  Store="FileStore" Targets="myserver">
  <JMSQueue CreationTime="1150241964468"
    JNDIName="JMSQueue" Name="MyJMSQueue" />
</JMSServer>
```

```
<JMSConnectionFactory JNDIName="JmsConnectionFactory"
    Name="MyJMSConnectionFactory" Targets="myserver"/>
```

Example 9–14 illustrates a JMS client that uses the JMS queue previously declared. The client sends a text message to `MyJMSQueue`.

Example 9–14 JMS Client Example

```
//Instantiate the initial context
javax.naming.InitialContext initialContext = new javax.naming.InitialContext();

//Look up the JMS connection factory and the message queue
Queue messageQueue = (Queue) initialContext.lookup("JMSQueue");
JMSConnectionFactory factory =
    (JMSConnectionFactory) initialContext.lookup("JmsConnectionFactory");

//Create the queue connection and session
QueueConnection queueConnection = factory.createQueueConnection();
QueueSession session =
    queueConnection.createQueueSession(false, Session.AUTO_ACKNOWLEDGE);

//Create a text message
TextMessage textMessage = session.createTextMessage();
textMessage.setText("Hello from the client!");

//Send message to the queue
QueueSender sender = session.createSender(messageQueue);
sender.send(textMessage);
```

To illustrate how to create an Authorization Policy for a JMS resource, let's assume we want to grant members of the Client role permission to send messages to a JMS queue named `FeedbackQueue`. Create the following objects using the Administration Console:

- Application = shared
- Resource Type = jms
- Resource = queue/FeedbackQueue
- Action = send
- Role = Client

This second Authorization Policy grants the `FeedbackProcessor` user permission to receive messages from a JMS queue named `FeedbackQueue`.

- Application = shared
- Resource Type = jms
- Resource = queue/FeedbackQueue
- Action = send
- user = myusers/FeedbackProcessor

Notice the actions (send and receive) are part of the Authorization Policies. The policy outcome is always equal to GRANT or DENY. [Table 9–13](#) documents the specific actions that can be performed on a JMS resource.

Table 9–13 JMS Resource Action Options

| Action | Description |
|---------|---|
| send | Required to send a message to a queue or a topic. This includes calls to the <code>MessageProducer.send()</code> , <code>QueueSender.send()</code> , and <code>TopicPublisher.publish()</code> methods. |
| receive | Required to create a consumer on a queue or a topic. This includes calls to the <code>Session.createConsumer()</code> , <code>Session.createDurableSubscriber()</code> , <code>QueueSession.createReceiver()</code> , <code>TopicSession.createSubscriber()</code> , <code>TopicSession.createDurableSubscriber()</code> , <code>Connection.createConnectionConsumer()</code> , <code>Connection.createDurableConnectionConsumer()</code> , <code>QueueConnection.createConnectionConsumer()</code> , <code>TopicConnection.createConnectionConsumer()</code> , and <code>TopicConnection.createDurableConnectionConsumer()</code> methods. |
| browse | Required to view the messages on a queue using the <code>QueueBrowser</code> interface. |

Table 9–14 documents the attributes supported by JMS resources that can be used as a part of a Condition in an Authorization Policy. See Section 4.6, "Using the Condition Builder" for details.

Table 9–14 Dynamic Attributes Supported by JMS Resources

| Attribute Name | Description |
|-----------------|--|
| application | The name of an application that hosts the resource |
| destinationtype | The JMS destination type (queue topic) |
| resource | The name of the resource |
| action | The JDBC operation name (send receive browse). |

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See Section 4.5.9, "Managing Attributes and Functions as Extensions" for more details.

9.4.4.6 Web Services Resources

A Web Services resource is a WebLogic Server resource related to a Web service. To secure Web services, create Authorization Policies for the entire Web Service resource, for a subset of the Web Service resource operations, for the stateless session EJB that implements the Web Service resource, or for a subset of the methods within the stateless session EJB. Example 9–15 shows the configuration of a web application named `BasicWS` that contains a Web service implementation named `BasicWS_Component`.

Example 9–15 Web Application Configuration

```
<application Name="BasicWS"
  Path="applications/BasicWS.ear"
  StagedTargets="myserver"
  <WebServiceComponent Name="BasicWS_Component"
    Targets="myserver"
    URI="BasicWS.war" />
</application>
```

[Example 9-16](#) shows how the `application.xml` file within the `BasicWS.ear` defines the web application context.

Example 9-16 Web Application Context Configuration

```
<module>
  <web>
    <web-uri>basic_javaclass.war</web-uri>
    <context-root>myservices</context-root>
  </web>
</module>
```

[Example 9-17](#) shows the configuration of a Web Service named `HelloWorld`. It is defined in the `web-services.xml` descriptor file inside the web application WAR file.

Example 9-17 Web Service Configuration

```
<web-services>
  <web-service useSOAP12="false"
    name="HelloWorld"
    style="rpc"
    uri="/HelloWorld">
    <operations>
      <operation name="sayHello"
        method="sayHello(int,java.lang.String)"/>
    </operations>
  </web-service>
</web-services>
```

[Table 9-15](#) describes how to name the Oracle Entitlements Server objects in the case of securing a Web resource. These values are defined when the objects are created using the Oracle Entitlements Server Administration Console.

Table 9-15 Web Services Values Mapped to Oracle Entitlements Server Objects

| OES Object Name | Web Services Value |
|-----------------|--|
| Application | The name of the application as defined in the <code>web-services.xml</code> file; in this case, <code>BasicWS</code> . |
| Resource Type | Takes as a value one of the supported resource types; in this case, <code>webservices</code> . |
| Resource parent | Takes as a value the context path of the web service as defined in the <code><context-root></code> element of the <code>application.xml</code> configuration file; in this case, <code>myservices</code> . |
| Resource | The Web Service name as defined in <code>web-services.xml</code> . |

To call the `sayHello()` method in the `HelloWorld` Web service, the client must be granted the action `sayHello`. Some clients may also require access to the Web Services Definition Language (WSDL) file that defines the Web service; the WSDL file is defined as a URL resource. [Example 9-18](#) is code that allows the client to, before calling the `sayHello()` method, access the WSDL file at the defined URL.

Example 9-18 Client Code For Accessing WSDL

```
String wsdlUrl = "http://localhost:7001/HelloWorld?WSDL";
HelloWorld service = new HelloWorld_Impl(wsdlUrl);
HelloWorldPort port = service.getHelloWorldPort();
String result = port.sayHello(34, "Josh");
```

To successfully execute this code, the client must be granted GET permission on the WSDL file (URL resource). (Note that for the URL Resource name is lower case.) Additionally, the client must be granted GET permission on the Web Service resource. (Note that for the Web Services Resource name has initial capitalization.) Create the following objects for the URL Resource Authorization Policy using the Administration Console:

- Application = BasicWS
- Resource Type = url
- Resource = myservices/helloworld
- Action = GET
- Role = SomeUser

Create the following objects for the Web Services Resource Authorization Policy using the Administration Console:

- Application = BasicWS
- Resource Type = webservices
- Resource = myservices/HelloWorld
- Action = sayHello
- Role = SomeUser

Notice the actions (GET and sayHello) are part of the Authorization Policies. The policy outcome is always equal to GRANT or DENY.

Table 9–16 documents the attributes supported by Web Services resources that can be used as a part of a Condition in an Authorization Policy. See Section 4.6, "Using the Condition Builder" for details.

Table 9–16 *Dynamic Attributes Supported by Web Services Resources*

| Attribute Name | Value |
|----------------|---|
| application | The name of the application |
| contextpath | The context part of the web application |
| webservice | The name of the web service |
| method | The name of the web service operation called |
| Param N | A value of the N th parameter in the method, for example, Param1, Param2... |

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See Section 4.5.9, "Managing Attributes and Functions as Extensions" for more details.

9.4.4.7 Server Resources

A Server resource determines who can control the state of a WebLogic Server instance. When users start server instances by invoking the `weblogic.Server` class in a Java command, the policy on the Server resource is the only security check that occurs. You can create Authorization Policies that apply to all WebLogic Server instances in a

domain or to individual servers. [Example 9–19](#) is an example of how a WebLogic Server instance named `myserver` might be configured.

Example 9–19 Configuration of WebLogic Server Instance

```
<Server ListenAddress=" "
  ListenPort="7001"
  Machine="mymachine"
  Name="myserver"
  NativeIOEnabled="true"
  ReliableDeliveryPolicy="RMDefaultPolicy"
  ServerVersion="8.1.5.0">
  <SSL Enabled="false" HostnameVerificationIgnored="false"
    IdentityAndTrustLocations="KeyStores" Name="myserver" />
</Server>
```

[Table 9–17](#) describes how to name the Oracle Entitlements Server objects in the case of securing the a Server resource. These values are defined when the entities are created using the Oracle Entitlements Server Administration Console

Table 9–17 Server Resource Values Mapped to Oracle Entitlements Server Objects

| OES Object Name | Server Resource Value |
|-----------------|---|
| Application | A Server resource does not belong to a specific Application. In these cases, <code>shared</code> substitutes for the name of the Application. The Application, <code>shared</code> , is defined when the Application is created using the Administration Console. |
| Resource Type | Takes as a value one of the supported resource types; in this case, <code>svr</code> . |
| Resource | The server instance name. |

To illustrate how to create an Authorization Policy for a Server resource, let's assume we want to grant members of the Admin role permission to boot all WebLogic Server instances. Create the following objects using the Administration Console:

- Application = `shared`
- Resource Type = `svr`
- Resource = `/lib/*`
- Action = `boot`
- Role = Admin

This second Authorization Policy grants members of the Admin role permission to shutdown or suspend a WebLogic Server instance named `CentralServer`. The policy is constrained in that permission is granted only on Sundays or other days between 2 AM and 4 AM.

- Application = `shared`
- Resource Type = `svr`
- Resource = `CentralServer`
- Action = `shutdown / suspend`
- Role = Admin
- Condition = Only on Sunday or other days between 2 AM and 4 AM

Notice the actions (boot and shutdown/suspend) are part of the Authorization Policies. The policy outcome is always equal to GRANT or DENY. [Table 9–18](#) documents the specific actions that can be performed on a Server resource.

Table 9–18 Server Resource Action Options

| Action | Description |
|----------|---|
| boot | Action required to start a WebLogic Server instance, either an Administration Server or Managed Server. |
| shutdown | Action required to shut down a running WebLogic Server instance, either an Administration Server or Managed Server. |
| suspend | Action required to prohibit additional logins (logins other than for privileged administrative actions) to a running WebLogic Server instance, either an Administration Server or Managed Server. |
| resume | Action required to re-enable non-privileged logins to a running WebLogic Server instance, either an Administration Server or Managed Server. |

[Table 9–19](#) documents the attributes supported by Server resources that can be used as a part of a Condition in an Authorization Policy. See [Section 4.6, "Using the Condition Builder"](#) for details.

Table 9–19 Dynamic Attributes Supported by Server Resource

| Attribute Name | Value |
|----------------|---|
| server | Name of the server with which the resource is associated. |
| action | Name of an operation performed on the server instance (boot shutdown suspend resume). |

Note: Before using the Condition Builder, the dynamic attributes first have to be created using the Oracle Entitlements Server Administration Console. See [Section 4.5.9, "Managing Attributes and Functions as Extensions"](#) for more details.

9.5 Securing Oracle WebCenter Content Resources

Oracle Entitlements Server can be integrated with Oracle WebCenter Content to provide high performance fine grained access control for enterprise content management.

9.5.1 About the Oracle WebCenter Content and Oracle Entitlements Server Integration

Oracle WebCenter Content provides a unified application for delivering document management, Web content management, digital asset management and records and retention management. The suite of products offers a flexible, robust and scalable content management solution that allows employees, customers and partners to collaborate, contribute and access business content anywhere worldwide. Oracle WebCenter Content helps companies fully maximize the value of their information and intellectual assets by bringing content such as spreadsheets, contracts, marketing materials, CAD drawings, digital assets, records and catalogs, to the Web where it can be efficiently managed.

Oracle Entitlements Server (OES) is a standards-based, policy-driven security solution that provides real time fine-grained authorization in Application, Service-Oriented Architecture (SOA) and Database environments. Oracle Entitlements Server fills the need for granular, flexible, and externalized access control. The solution provides a comprehensive and centralized approach for managing access policies with distributed or centralized enforcement. Authorization policy management and runtime enforcement is provided for sensitive applications, databases, containers (such as Java™, .NET), portals and content management systems, development frameworks, object relational mapping technologies, intermediaries (such as XML gateways and ESB's), web services, and SOA infrastructure.

In an Oracle WebCenter Content and Oracle Entitlements Server integration, Oracle Entitlements Server can serve as the authorization engine for all the content managed by Oracle WebCenter Content using RBAC and ABAC policies. Oracle Entitlements Server can leverage an existing user attribute repository to enforce these policies by supplying user attributes, role membership, group membership, and other relevant attributes to drive coarse-grained and fine-grained access to content in Oracle WebCenter Content. Corporations would no longer require creating extensive permutations and management of complex Security groups and Accounts in Oracle WebCenter Content. The integration allows corporations to leverage rich policies that incorporate user, resource, and content metadata attributes in lieu of Oracle WebCenter Content's native model based solely on Security groups and Accounts.

After integration, Oracle Entitlements Server provides the controls summarized in [Table 9–20](#).

Table 9–20 Supported Oracle WebCenter Content Document Operations

| WebCenter Content Document Operation | Description | Oracle Entitlements Server Controls |
|---|--|---|
| Check-in | Creating new revision of the document | Who can perform document check-in operation |
| New Check-in | Uploading new document | Who can perform a new document check-in operation |
| Check-in similar | Similar to New Check-in. Inherits properties set during previous new document upload | Who can perform check-in similar document operation |
| Checkout | Checkout existing document for modifications | Who can perform document checkout operation |
| Undo Checkout | Discard checked-out document | Who can perform discard document checkout operation |
| Delete | Delete revision of the document | Who can perform document delete operation |
| Update | Update metadata or attributes of the document | Who can perform document update operation |
| Search | Perform document search operation | What user can see in the document search results |
| Read | Read content of the document | Who can perform document read operation |
| Download | Download the document | Who can perform document download operation |

9.5.2 Terminology for Oracle WebCenter Content and Oracle Entitlements Server Directories

This chapter uses the following terms when referring to variables in the directories associated with the Oracle Entitlements Server and Oracle WebCenter Content integration:

- *MW_HOME*: The container for the Oracle WebLogic Server home, and optionally an Oracle Common home and one or more Fusion Middleware suite-specific Oracle homes. When you install Oracle WebLogic Server, the Oracle WebLogic Server Installer creates a Middleware home directory (*MW_HOME*) that contains the Oracle WebLogic Server home directory (*WL_HOME*) and an Oracle Common home directory (*ORACLE_COMMON_HOME*), which contains the binary and library files required for Fusion Middleware Control and Java Required Files (JRF).
- *IAM_Home*: The Oracle Home directory created under your Middleware Home that includes Oracle Identity Manager, Oracle Access Management, Oracle Adaptive Access Manager, Oracle Entitlements Server, Oracle Identity Navigator, Oracle Privileged Account Manager, and Oracle Access Management Mobile and Social. You can specify any name for this Oracle Home directory.
- *ORACLE_HOME*: The home directory which contains the binary and library files required for a specific Oracle Fusion Middleware software suite.
- *MW_HOME/Oracle_ECMI*: The default WebCenter Content Oracle home.
- *WCC_DOMAIN_HOME*: The user-specified directory where an Oracle WebCenter Content application is deployed to run on an application server. The *WCC_DOMAIN_HOME/ucm/cs/bin* directory contains the executables. The default location for *WCC_DOMAIN_HOME* is *MW_HOME/user_projects/domains/base_domain*, but you can change the path and domain name (*base_domain*) during the deployment of an Oracle WebCenter Content application to an application server.
- *OES_CLIENT_HOME*: The Oracle Home Directory where the OES client is installed.
- *RCU_HOME*: A temporary staging directory for the Repository Creation Utility (RCU).

9.5.3 Integration Roadmap

Table 9–21 lists the high-level tasks for integrating Oracle WebCenter Content and Oracle Entitlements Server.

Table 9–21 Integration Roadmap

| No. | Task | Information |
|----------------------|---|--|
| Prerequisites | | |
| 1 | Review system requirements and Certification | For more information, see "Reviewing System Requirements and Certification." |
| 2. | Install the Oracle Database. | For more information, see "Installing the Oracle Database." |
| 3. | Install the Oracle WebLogic Server and Create the Oracle Middleware Home. | For more information, see "Installing the Oracle WebLogic Server and Creating the Oracle Middleware Home." |
| 4. | Install Oracle Identity and Access Management Suite 11g R2PS2 in the WebLogic Home. | For more information, see "Installing Oracle Identity and Access Management Suite 11g R2PS2 in the WebLogic Home." |

Table 9–21 (Cont.) Integration Roadmap

| No. | Task | Information |
|---|--|---|
| 5. | Obtain Oracle Entitlements Server Client software. | For more information, see "Obtaining Oracle Entitlements Server Client Software." |
| 6. | Install Oracle Entitlements Server Client. | For more information, see "Installing Oracle Entitlements Server Client." |
| WebCenter Content Base Installation | | |
| 7. | Install and configure WebCenter Content 11.1.1.8. | For more information, see "Installing Oracle WebCenter Content." |
| 8. | Create the Oracle WebCenter Content Schema with the Repository Creation Utility. | For more information, see "Creating the Oracle WebCenter Content Schema." |
| 9. | Create a Oracle WebCenter Domain. | For more information, see "Creating the WebCenter Domain." |
| 10. | Start the Servers in the WebCenter Domain. | For more information, see "Starting the Servers in the WebCenter Domain." |
| 11. | Configure WebCenter Content. | For more information, see "Configuring WebCenter Content." |
| Configuring Oracle Entitlements Server | | |
| 12. | Run RCU to create the OPSS Schema. | For more information, see "Running RCU to Create the OPSS Schema." |
| 13. | Create the OES Domain. | For more information, see "Creating the OES Domain using the IDM Configuration Wizard." |
| Configuring the Security Store | | |
| 14. | Configure the security store for Oracle Entitlements Server Administration Server. | For more information, see "Configuring the OES Security Store using the Security Store Configuration Tool." |
| Oracle Entitlements Server and WCC Integration | | |
| 15. | Integrate WCC and OES. | For more information, see "Integrating WebCenter Content with OES." |
| 16. | Update the config.cfg file of the WCC Domain | For more information, see "Updating the config.cfg File of the WCC Domain." |
| 17. | Add permission in JRE | For more information, see "Adding Permission in JRE for WebCenter Content Version is 11.1.1.7.0 or Lower." |
| 18. | Install the WCC-OES Connector. | For more information, see "Installing the WCC-OES Connector." |
| Post-Integration | | |
| 19. | Creating the Application, Resource Types, Resources, and Policies. | For more information, see "Creating the Application, Resource Types, Resources, and Policies." |
| 20. | Verify integration is working. | For more information, see "Verifying Oracle WebCenter Content Is Working." |

9.5.4 Prerequisites

Prior to integrating Oracle WebCenter Content and Oracle Entitlements Server, you must have installed all the required components, including any dependencies, and configured the environment in preparation of the integration tasks that follow.

This section contains the following topics:

- [Section 9.5.4.1, "Reviewing System Requirements and Certification"](#)
- [Section 9.5.4.2, "Installing the Oracle Database"](#)
- [Section 9.5.4.3, "Installing the Oracle WebLogic Server and Creating the Oracle Middleware Home"](#)
- [Section 9.5.4.4, "Installing Oracle Identity and Access Management Suite 11g R2PS2 in the WebLogic Home"](#)
- [Section 9.5.4.5, "Obtaining Oracle Entitlements Server Client Software"](#)
- [Section 9.5.4.6, "Installing Oracle Entitlements Server Client"](#)

9.5.4.1 Reviewing System Requirements and Certification

Before performing any installation, you should read the system requirements and certification documents to ensure that your environment meets the minimum installation requirements for the products you are installing.

- *Oracle Fusion Middleware System Requirements and Specifications*

This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.

- *Oracle Fusion Middleware Supported System Configurations*

This document contains information related to supported installation types, platforms, operating systems, databases, JDKs, and third-party products.

- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

9.5.4.2 Installing the Oracle Database

Ensure that you have an Oracle Database installed on your system before installing Oracle Identity and Access Management. The database must be up and running to install the relevant Oracle Identity and Access Management components.

For more information, see "Database Requirements" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

For information about certified databases, see the "Database Requirements" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

9.5.4.3 Installing the Oracle WebLogic Server and Creating the Oracle Middleware Home

Prior to installing the WebLogic Server, ensure that your machines meet the system, patch, kernel, and other requirements.

For WebLogic Server and Middleware Home requirements, see "WebLogic Server and Middleware Home Requirements" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*

For complete information about installing Oracle WebLogic Server, see *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

9.5.4.4 Installing Oracle Identity and Access Management Suite 11g R2PS2 in the WebLogic Home

Oracle Entitlements Server is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11g Installer to install Oracle Identity and Access Management Suite.

Note: When you are installing Oracle Identity and Access Management, only the Administration Server of Oracle Entitlements Server is installed. You must install and configure Oracle Entitlements Server Client separately.

Install and configure Oracle Entitlements Server according to the instructions in "Installing and Configuring Oracle Entitlements Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

9.5.4.5 Obtaining Oracle Entitlements Server Client Software

For more information on obtaining Oracle Entitlements Server Client 11g software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

9.5.4.6 Installing Oracle Entitlements Server Client

To install Oracle Entitlements Server Client, extract the contents of oesclient.zip to your local directory and then start the Installer by executing one of the following commands:

UNIX: <full path to the runInstaller directory>/runInstaller -jreLoc <full path to the JRE directory>

Windows: <full path to the setup.exe directory>\setup.exe -jreLoc <full path to the JRE directory>

To install Oracle Entitlements Server Client, follow the instructions in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

9.5.5 Oracle WebCenter Content Base Installation

This section contains instructions for installing Oracle WebCenter Content in an Oracle WebLogic Server domain on a single host. These instructions are for installing Oracle WebCenter Content for the first time.

Note: Key installation and configuration information is provided in this section. However, not all component prerequisite, dependency, and installation instruction is duplicated here. Adapt information as required for your environment.

For complete installation information, follow the instructions in *Oracle WebCenter Content Quick Installation Guide*.

The base installation of WebCenter Content consists of the following tasks:

- Section 9.5.5.1, "Installing Oracle WebCenter Content"
- Section 9.5.5.2, "Creating the Oracle WebCenter Content Schema"
- Section 9.5.5.3, "Creating the WebCenter Domain"
- Section 9.5.5.4, "Starting the Servers in the WebCenter Domain"
- Section 9.5.5.5, "Configuring WebCenter Content"

9.5.5.1 Installing Oracle WebCenter Content

Follow the instructions below to install Oracle WebCenter Content 11.1.1.8 in the WebLogic Home.

The installer binaries are as follows:

- ofm_wcc_generic_11.1.1.8.0_disk1_1of2.zip
 - ofm_wcc_generic_11.1.1.8.0_disk1_2of2.zip
1. Obtain the Oracle WebCenter Content binaries from the following download location and unzip them:

<http://www.oracle.com/technetwork/middleware/webcenter/content/downloads/index.html>
 2. Start the Oracle Fusion Middleware 11g WebCenter Content Installer from Disk 1 of the Oracle WebCenter Content media, as follows:


```
(UNIX) wc_content_media_loc/Disk1/runInstaller -jreLoc jre_location
(Windows) wc_content_installer_loc/Disk1/setup.exe -jreLoc jre_location
```
 3. In the Welcome screen, click **Next**.
 4. In the Install Software Updates screen, select **Skip Software Updates**, and then click **Next** to continue the installation.
 5. In the Prerequisite Checks screen, click **Next** to continue the installation if there are no errors.

If you want to stop the installation process while you fix a prerequisite error, click **Abort**.

If you want to continue the installation without fixing an error, click **Continue**.
 6. In the Specify Installation Location screen, specify your Oracle Middleware Home and Oracle Home Directory, and then click **Next**.
 - Oracle Middleware Home: Select the Middleware home directory (`MW_HOME`), which was created during the installation of Oracle WebLogic Server. For example, `/opt/oracle/Middleware`.

- Oracle Home Directory: Specify the directory where you want to install Oracle WebCenter Content, `Oracle_ECM1`.
7. In the Application Server screen, select **Weblogic Server** and click **Next**.
 8. In the Installation Summary screen, click **Install** to start the installation.
 9. In the Installation Progress screen, click **Next** when the installation is 100% complete.
 10. In the Installation Completed screen, click **Finish**.

9.5.5.2 Creating the Oracle WebCenter Content Schema

Oracle WebCenter Content requires that an application schema exists in the database before configuration of the application. You must run the Repository Creation Utility (RCU) to create the component schema in the database. The database must be up and running before you start RCU.

The Repository Creation Utility (RCU) can be obtained from the same location as the WebCenter Content 11.1.1.8.0 binaries from under **Required Additional Software** at:

<http://www.oracle.com/technetwork/middleware/webcenter/content/downloads/index.htm>
1

Note: The Repository Creation Utility (RCU) version has to match the WebCenter Content version.

To create the schema for WebCenter Content, proceed as follows:

1. Ensure the database is up and running.
2. After downloading the .zip file, extract the contents to a directory of your choice; this directory will be referred to as the `RCU_HOME` directory.
3. Start RCU from the bin directory inside the `RCU_HOME` directory.


```
cd RCU_HOME/bin
./rcu
```
4. In the Welcome screen, click **Next**.
5. In the Create Repository screen, click **Create** and then, **Next**.
6. In the Database Connection Details screen, specify the connection details for your database, then click **Next**. When the database checking has passed without errors, click **OK** to dismiss the dialog window and go to the next screen.

Database Type: You can keep the default, **Oracle Database**, selected.

For connecting to an Oracle Database instance, provide the following information:

- **Host Name:** Specify the name of the machine on which your database resides, in the format `identity.example.com`.
- **Port:** Specify the database listen port number. The default port number for an Oracle Database instance is 1521.
- **Service Name:** Specify the service name for the database, for example, `orcl.example.com`. Typically, the service name is the same as the global database name.

If you do not know the service name for your database, you can obtain it from the `SERVICE_NAMES` parameter in the database's initialization parameter file. If

this file does not contain the `SERVICE_NAMES` parameter, then the service name is the same as the global database name, which is specified in the `DB_NAME` and `DB_DOMAIN` parameters. Another way to find the service name is to log in to the database as `SYS` and run the following command:

```
show parameter service_name
```

- Username: Specify the user name of the database administrator.
Specify the name of an Oracle Database user with `SYSDBA` privileges. The default user name with `SYSDBA` privileges is `SYS`.
 - Password: Specify the password for your database user.
 - Role: Select a database user role from the list. `SYS` requires the `SYSDBA` role.
7. In the Select Components screen, specify a schema prefix. For example, `WC`, and expand **WebCenter Content** in the Component column, and select **Oracle WebCenter Content Server - Complete**. Click **Next**. The Checking Component Prerequisites dialog box appears. After the checking is complete with no errors, click **OK** to dismiss the dialog box and go to the next screen.
- A schema is created for WebCenter Content when you select **Oracle WebCenter Content Server - Complete**.
8. In the Schema Passwords screen, specify a password for the schema owner. For a development system, you might want to select **Use same passwords for all schemas**. Click **Next**.
- Note:** Record the Schema Owner (`WC_OCS`) and the schema passwords from this screen because you will need them later to configure your applications.
9. In the Map Tablespaces screen, configure the desired tablespace mapping for the schemas you want to create, then click **Next**.

For example:

- Component: Oracle WebCenter Content Server - Complete
- Schema Owner: `WC_OCS`
- Default Tablespace: `*WC_OCS`
- TEMP Tablespace: `*OCS_TEMP`

A separate dialog window will appear asking you to confirm that you want to create these tablespaces. Click **OK** to proceed and dismiss the dialog window. A second dialog window will appear showing the progress of tablespace creation. After this is complete, click **OK** to dismiss this window and go to the next screen.

10. In the Summary screen, review the information on this screen, then click **Create** to begin schema creation.
11. In the Completion Summary screen, note the location of the log files, then click **Close** to dismiss the screen.

For more information, refer to the instructions in *Oracle WebCenter Content Quick Installation Guide*.

9.5.5.3 Creating the WebCenter Domain

After you have successfully run the installer and created application schemas, you can deploy and configure the following Oracle WebCenter Content products as applications:

1. Start Oracle Fusion Middleware 11g WebCenter Content Installer with the configuration script:
 - (UNIX) `MW_HOME/Oracle_ECM1/common/bin/config.sh`
 - (Windows) `MW_HOME\Oracle_ECM1\common\bin\config.cmd`
2. In the Welcome screen, select **Create a new Weblogic domain** and click **Next**.
3. In the Domain Source screen, select **Oracle Universal Content Management - Content Server 11.1.1.0 [Oracle_ECM1]** and click **Next**.
4. In the Specify Domain Name and Location screen, specify:
 - Domain name: Name of the domain you want to create, for example, `wcc_domain`.
 - Domain location: Location for the domain. For example, `/opt/oracle/Middleware/user_projects/domains`.
 - Application location: Location for the application you are deploying. For example, `/opt/oracle/Middleware/user_projects/applications`.

Then, click **Next**.
5. Configure Administrator User Name and Password screen, specify:
 - User name: the default administrator user name is `weblogic`, which you can change to another administrator user name if you want
 - User password: password for the administrator user.

Then, click **Next**.
6. In the Configure Server Start Mode and JDK screen:
 - Under **WebLogic Domain Startup Mode**, leave **Development Mode** selected. For Production, you must select **Production Mode** and follow the steps accordingly.
 - Under **JDK Selection**, leave **Available JDKs** and the default JDK selected, which is **Sun SDK 1.6.0_29** for development mode or, on a 64-bit system, the JDK you installed.

Then, click **Next**.
7. In the Configure JDBC Component Schemas screen, configure the schema information for the component data source. When you make changes to any field on this screen, the changes are applied to the selected data sources.

For example,

 - Vendor: Oracle
 - Driver: * Oracle's Driver (Thin) for Service connections
 - Schema Owner: WC_OCS
 - DBMS/Service: orcl.example.com
 - Host Name: identity.example.com
 - Port: 1521

Select **UCM Schema**. Then, click **Next**.
8. In the Test Component Schema screen, select **UCM Schema**, verify that the connections to your data sources are successful, and click **Next**.

9. In the Select Optional Configuration screen, select **Administration Server** and **Managed Servers, Clusters and Machines**, and then, click **Next**.
10. In the Configure the Administration Server screen, select **SSL enabled** and fill in the fields.
For example:
 - Name: AdminServer
 - Listen Address: All Local Addresses
 - Listen Port: 8001
 - SSL Listen Port: 8002
 Then, click **Next**.
11. In the Configure Managed Server screen, fill in the fields and select **SSL enabled**.
For example:
 - Name: UCM_server1
 - Listen address: All Local Addresses
 - Listen port: 16200
 - SSL listen port: 16201
12. In the Configuration Summary screen, check your configuration and make any corrections or updates, and then click **Create**.
13. In the Creating Domain screen, click **Done** when the domain is successfully created.

9.5.5.4 Starting the Servers in the WebCenter Domain

When you configure Oracle WebCenter Content to create an Oracle WebLogic Server domain, a domain directory is created under the `MW_HOME/user_projects/domains` directory. The directory for the domain where you configure Oracle WebCenter Content contains the Administration Server and one or more Managed Servers, each hosting an Oracle WebCenter Content application.

The following commands assume that your current working directory is your domain directory, e.g., `MW_HOME/user_projects/domains/wcc_domain`.

Starting the WebCenter Domain Administration Server

Execute the following command to start the Administration Server:

```
MW_HOME/user_projects/domains/wcc_domain/bin/startWebLogic.sh
```

Starting the WebCenter Managed Servers

Execute the following command to start the Managed Server:

```
MW_HOME/user_projects/domains/wcc_domain/bin/startManagedWebLogic.sh UCM_server1
t3://localhost:8001/
```

Enter the username to start the WebLogic server. For example, `weblogic`.

Enter the password.

9.5.5.5 Configuring WebCenter Content

To complete the WebCenter Content configuration:

Browse to the Content Server postinstallation configuration page by accessing the Web Center Console:

```
http://managedServerHost:16200/cs/
```

Configure WebCenter Content according to the instructions in *Oracle WebCenter Content Quick Installation Guide*.

9.5.6 Configuring Oracle Entitlements Server

This section contains the following topics:

- [Section 9.5.6.1, "Running RCU to Create the OPSS Schema"](#)
- [Section 9.5.6.2, "Creating the OES Domain using the IDM Configuration Wizard"](#)

9.5.6.1 Running RCU to Create the OPSS Schema

To create the OPSS schema in an Oracle database with RCU, proceed as follows:

1. Start RCU from the bin directory inside the `RCU_HOME` directory.

```
cd RCU_HOME/bin
./rcu
```

2. In the Welcome screen, click **Next**.
3. In the Create Repository screen, click **Create** and then, **Next**.
4. In the Database Connection Details screen, specify the connection details for your database, then click **Next**. When the database checking has passed without errors, click **OK** to dismiss the dialog window and go to the next screen.

Database Type: You can keep the default, **Oracle Database**, selected.

For connecting to an Oracle Database instance, provide the following information:

- **Host Name:** Specify the name of the machine on which your database resides.
 - **Port:** Specify the database listen port number.
 - **Service Name:** Specify the service name for the database.
 - **Username:** Specify the user name of the database administrator.
Specify the name of an Oracle Database user with `SYSDBA` privileges. The default user name with `SYSDBA` privileges is `SYS`.
 - **Password:** Specify the password for your database user.
 - **Role:** Select a database user role from the list. `SYS` requires the `SYSDBA` role.
5. In the Select Components screen, specify a schema prefix. For example, `OES`, and expand the **AS Common Schemas** in the Component column, and select **Oracle Platform Security Services**. Click **Next**. The Checking Component Prerequisites dialog box appears. After the checking is complete with no errors, click **OK** to dismiss the dialog box and go to the next screen.
 6. In the Schema Passwords screen, specify a password for the schema owner. For a development system, you might want to select **Use same passwords for all schemas**. Click **Next**.

Note: Record the Schema Owner (i.e., OES_OPSS) and the schema passwords from this screen because you will need them later to configure your applications.

7. In the Map Tablespaces screen, configure the desired tablespace mapping for the schemas you want to create, then click **Next**.

Use one default tablespace and one temporary tablespace; the default tablespace names are PREFIX_IAS_OPSS and PREFIX_IAS_TEMP, respectively.

Note: In PREFIX_IAS_OPSS and PREFIX_IAS_TEMP, "PREFIX" was specified in Step 6.

A separate dialog window will appear asking you to confirm that you want to create these tablespaces. Click **OK** to proceed and dismiss the dialog window. A second dialog window will appear showing the progress of tablespace creation. After this is complete, click **OK** to dismiss this window and go to the next screen.

8. In the Summary screen, review the information on this screen, then click **Create** to begin schema creation.
9. In the Completion Summary screen, note the location of the log files, then click **Close** to dismiss the screen.

9.5.6.2 Creating the OES Domain using the IDM Configuration Wizard

After installing the OES Administration software, you must create a domain that contains the OES Administration domain and then configure it to work with a database security store.

Use the Oracle Fusion Middleware Configuration Wizard to create a WebLogic domain or extend an existing domain. Start the Oracle Fusion Middleware Configuration Wizard by running the `IAM_HOME/common/bin/config.sh` script (on UNIX), or `IAM_HOME\common\bin\config.cmd` (on Windows)

On Select Domain Source screen, select **Oracle Entitlements Server for Admin Server-11.1.1.0 [IAM_HOME]**.

On Specify Domain Name and Location screen, provide the Domain Name. For example, `oes_domain`.

On the Configure JDBC Component Schema screen, select **OPSS_Schema** and provide details for the Schema Owner (OES_OPSS), Schema Password, DBDS/Service, Host Name, and Port.

For instructions on configuring Oracle Entitlements Server in a new WebLogic domain, see "Configuring Oracle Entitlements Server in a New WebLogic Domain" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

9.5.7 Configuring the OES Security Store using the Security Store Configuration Tool

Each Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) domain must be configured to have a Database Security Store. You must run the `configureSecurityStore.py` script to configure the security store for Oracle Entitlements Server Administration Server. `configureSecurityStore.py` reassociates the domain security store and migrates policy data to the new repository. The security store is a repository of system and application-specific policies, credentials, and keys.

To run the OES security store configuration tool to configure the OES domain to use the security store:

1. Before running any reassociation, make a backup of the `jps-config.xml` file so you can revert it back later on if needed.
2. Move from your present working directory to the `MW_HOME/oracle_common/common/bin` directory by running the following command on the command line:

```
cd MW_HOME/oracle_common/common/bin
```

3. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

4. At the WLST prompt, run the following command:

```
MW_HOME/oracle_common/common/bin/wlst.sh
Oracle_IDM1/common/tools/configureSecurityStore.py
-d MW_Home/user_projects/domains/oes_domain
-t DB_ORACLE
-j cn=jpsroot
-m create
-p password
```

where

- `MW_Home/user_projects/domains/oes_domain` is the name and location of the OES Administration domain.
- `DB_ORACLE` is the type of security store to associate with the OES Administration Server. It is optional. The default value is `DB_ORACLE`.
- `cn=jpsroot` is the `jpsroot` value of the OES security store. The default value is `cn=jpsroot`.
- `create` is the tool mode, which indicates that the tool will create an OES database security store.
- `password` is the password to the OES database.

For instructions on configuring the security store, see "Configuring Security Store for Oracle Entitlements Server Administration Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

9.5.8 Integrating WebCenter Content with OES

Steps to integrate WebCenter Content with OES are described in the following sections:

- [Creating a Data Source in Oracle WebCenter Content Domain](#)
- [Reassociating Oracle WebCenter Content Domain Security Store](#)
- [Updating the config.cfg File of the WCC Domain](#)
- [Adding Permission in JRE for WebCenter Content Version is 11.1.1.7.0 or Lower](#)
- [Installing the WCC-OES Connector](#)

After integrating WCC and OES, you will need to create an application and other policy objects.

9.5.8.1 Creating a Data Source in Oracle WebCenter Content Domain

Start the WebCenter Content Administration Server and create a data source with the same configuration information for the `opss-DBDS` as the Oracle Entitlements Server

domain so that the OES domain and WebCenter Content domain can share the same policy store.

Target this data source to the Administration Server and all Managed Servers of WebCenter Content domain.

1. Check the configuration information of `opss-DBDS` of the OES domain.
 - a. Access the OES domain's WebLogic Administration Console.
 - b. In the Domain Structure tree, expand Services, then select Data Sources.
 - c. On the Summary of Data Sources page, click the data source name.
 - d. Select the Configuration: Connection Pool tab.
2. Create data source in WebCenter Content domain.
 - a. Access WebCenter Content domain's WebLogic Administration Console.
 - b. Create data source as the configuration in step 1

For example:

Name: `opss-DBDS`

Type: Generic

JNDI-Name: `jdbc/OPSSDBDS`

URL: `jdbc:oracle:thin:@orcl.example.com:1521/orcl`

Driver: `oracle.jdbc.OracleDriver`

User: `OES_OPSS`

Targets: `UCM_Server1`

For instructions on creating a data source, see "Create JDBC generic data sources" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

9.5.8.2 Reassociating Oracle WebCenter Content Domain Security Store

Reassociate the WebCenter Content domain's Security Store to the same as Oracle Entitlements Server using the WLST `reassociateSecurityStore` command, as follows:

1. Before running any reassociation, make a backup of the `jps-config.xml` file so you can revert it back later on if needed.
2. Start the WLST shell.

```
cd $MW_HOME/Oracle_ECM1/common/bin
./wlst.sh
```

3. Connect to the WebLogic Administration Server using the WLST `connect` command.

```
connect ("username", "password", "t3://hostname:port")
```

For example:

```
connect ("weblogic", "welcome1", "ADMINHOST:8001")
```

username is the administrator account name used to access the Administration Server

password is the administrator password used to access the Administration Server

hostname is the server name of the Administration Server

port is the port number of the Administration Server

4. Run the `reassociateSecurityStore` command:

```
reassociateSecurityStore(domain="oes_domain or IAM", servertype="DB_ORACLE",
datasourcename="datasource", jpsroot="cnSpecification", join="true")
```

For example:

```
reassociateSecurityStore(domain="oes_domain", servertype="DB_ORACLE",
datasourcename="jdbc/OPSSDBDS", jpsroot="cn=jpsroot", join="true")
```

5. When you have finished, use the `exit()` command to exit the WLST utility.

The script `reassociateSecurityStore` migrates the security store from a source to a target DB-based store, and it resets the default policy and credential services to the target repository. The values for `domain` and `jpsroot` must be same as the value for `farmname` in the `jps-config.xml` file. This file is located in the `$WCC_DOMAIN_HOME/config/fmwconfig` directory.

`datasourcename` is the name of the Data Source that you created in [Section 9.5.8.1, "Creating a Data Source in Oracle WebCenter Content Domain."](#)

9.5.8.3 Updating the `config.cfg` File of the WCC Domain

To protect the Web Location function, update the `config.cfg` file of the WebCenter Content domain. The `config.cfg` file is used to define global variables for the Content Server system.

1. Open the `config.cfg` file in a text editor.

It is located in the `$WCC_DOMAIN_HOME/ucm/cs/config/` directory.

2. Add the following line:

```
InternalAppExtensionWildcardTest=*
```

3. Restart the Administration and Managed servers.

9.5.8.4 Adding Permission in JRE for WebCenter Content Version is 11.1.1.7.0 or Lower

Add permissions in JRE which your web browser will use if your WebCenter Content version is 11.1.1.7.0 or lower.

For Windows (Only Internet Explorer works):

1. Typically, edit your `java.policy` file under `C:\Program Files\Java\jre7\lib\security`.
2. Add the permission `java.util.PropertyPermission "user.timezone", "write";` to the last section; grant default permissions to all domains.
3. Save this file using the Administrator permission.

9.5.8.5 Installing the WCC-OES Connector

The WCC-OES Connector is an OES Java Wrapper that transfers request parameters, document metadata, and user context data to the OES SM client.

To install the WCC-OES Connector, proceed as follows:

1. Launch the Universal Content Management Component Wizard.

```
cd $WCC_DOMAIN_HOME/ucm/cs/bin
./ComponentWizard
```

OES_CLIENT_HOME is where the OES Client software is installed.

WCC_DOMAIN_HOME is the WebLogic Domain where WebCenter Content is installed.

WCC_DOMAIN_HOME/ucm/cs/bin is the root directory for Content Server startup files. It contains the executable files that run Content Server services, applets, and utilities.

The Component List Screen is displayed.

2. From the Component List Screen, click **Install**.
3. Click **Select**.
4. Select the `ucmoesconnector.zip` file.
5. Click **OK** to install the WCC-OES Connector.
6. Click **Yes** to close the window.
7. Restart the WC Domain Managed Server.

9.5.9 Creating the Application, Resource Types, Resources, and Policies

This section contains the following topics:

- [Creating a New Application](#)
- [Creating the UCM Pre-Search Query Resource Type](#)
- [Creating the UCM CRUD Operation Resource Type](#)
- [Creating a Resource](#)
- [Creating Policies](#)

9.5.9.1 Creating a New Application

Create a new application UCM Application by following the steps below:

1. Open the **Authorization Management** tab.
2. Right-click **Applications** in the Navigation Panel and select **New** from the menu.

Note: Alternately, click **Create Application** under **Search and Create** in the Home area.

3. Enter UCM Application as the name of the application.

Note: Do not change the name.

4. Click **Save** at the top right-hand corner of the screen.

For instructions on creating an application, see [Section 4.5.1.1, "Creating an Application."](#)

9.5.9.2 Creating the UCM Pre-Search Query Resource Type

Create UCM Pre-Search Query Resource Type by following the steps below:

1. Open the **Authorization Management** tab.
2. Expand the **Applications** node and then expand the newly created **UCM Application** node.
3. Right-click **Resource Type**, and then select **New**.
4. Enter `UCM Pre-Search Query Resource Type` as the name of the Resource Type.

Note: Do not change the name.

5. Add an action allowed by UCM Pre-Search Query Resource Type.
 - a. Click **New** above the **Actions** table to display the New Action dialog.
 - b. Enter `search` as the name of the action.
 - c. Click **Save** to save the search action.
6. Click **Save** in the upper right to save the Resource Type.

For instructions to create a Resource Type, see [Section 4.5.2.1, "Creating a Resource Type."](#)

9.5.9.3 Creating the UCM CRUD Operation Resource Type

Create UCM CRUD Operation Resource Type by following the steps below:

1. Open the **Authorization Management** tab.
2. Expand the **Applications** node and then expand the newly created **UCM Application** node.
3. Right-click **Resource Type**, and then select **New**.
4. Enter `UCM CRUD Operation Resource Type` as the name of the Resource Type.

Note: Do not change the name.

5. Add actions allowed by UCM CRUD Operation Resource Type.
 - a. Click **New** above the **Actions** table to display the New Action dialog.
 - b. Enter `checkin` as the name of the action.
 - c. Click **Save** to save the checkin action.
 - d. Continue with adding the following actions: `checkin_processing`, `update_metadata`, `update_metadata_processing`, `delete`, `checkinnew`, `checkin_confirm_form`, `checkout`, `undo_checkout`, `checkin_new_processing`, `get_file`, `create_folder`, `retrieve_child_folders`, `read`, and `folder_browse`.
6. Click **Save** in the upper right to save the Resource Type.

For instructions to create a Resource Type, see [Section 4.5.2.1, "Creating a Resource Type."](#)

9.5.9.4 Creating a Resource

Create a Resource by following the steps below:

1. Expand the **Policy Domain** node in the **UCM Application** node and then the **Resource Catalog** node.
2. Right-click **Resources** from the Resource Catalog node and select **New** from the menu.
3. In the Home area, select **UCM Pre-Search Resource Type** from the **Resource Type** list.
4. Enter / as the name that the application will pass to determine whether the user is authorized to access this resource.

Other resource names must be consistent to the document IDs defined in WebCenter Content.

5. Click **Save** to save the Resource.

For instructions on creating resources, see [Section 4.5.3.1, "Creating a Resource."](#)

9.5.9.5 Creating Policies

Create new authorization policies for the integration by following the steps below:

For detailed instructions on creating policies, see [Section 4.5.5.1, "Creating an Authorization Policy."](#)

1. For search:
 - a. Double-click the **Authorization Policies** node.
 - b. Click the **New** button above the table showing the existing Authorization Policies.
 - c. Enter the name of the new policy.
 - d. Configure Principals (i.e. uses and/or roles) that can access the resource as needed.
 - e. Click the "plus" button to the right of the **Targets** table.
 - f. Click on the **Resources** tab on the Search Targets window.
 - g. Select **UCM Pre-Search Query Resource Type** in the **Resource Type** dropdown and click the **Search** button.
 - h. Select resource "/", and click "search" action.
 - i. Add any obligation for the policy, depending on your requirements.

The following is an example of an Obligation to the Search Policy:

```
New obligation: Name: Search_Obligation
New obligation attribute: Name:Attribute1 Value:dStatus <MATCHES>
`RELEASED`
```

Use the backtick (`) character, not the single quote (').

Note: If the metafield is WebCenter Content defined, add d before the field name; if the metafield is user defined through Configuration Manager, add an x before the field name. For example, the Status should be dStatus and ClearanceLevel which is user defined should be xClearanceLevel in the obligation.

Note: On a US layout keyboard, the backtick (`) character is typically below the tilde (~). An opening single quote/apostrophe (') should not be used in place of the backtick (`).

2. For new check in:
 - a. Click the “plus” button to the right of the **Targets** table.
 - b. Click on the **Resources** tab on the Search Targets window.
 - c. Select **UCM CRUD Operation Resource Type** in the **Resource Type** dropdown and click the **Search** button.
 - d. Choose resource expression. The expression is ".*".
 - e. Click "checkinnew", "checkin_confirm_form", and "checkin_new_processing".
3. For other policies:

Add corresponding principles, targets, actions, and conditions. [Table 9–22](#) shows an action comparison table using DOC1 as an example of the content you want to protect in WebCenter Content.

Table 9–22 Action Comparison

| WCC Operation | Resource in APM policy | Actions in APM policy |
|----------------------------------|---------------------------------------|--|
| Search | UCM Pre-Search Query Resource Type:/ | search |
| New Check In Check In Similar | UCM CRUD Operation Resource Type:.* | checkin_new_processing checkinnew checkin_confirm_form |
| Check Out | UCM CRUD Operation Resource Type:DOC1 | checkout |
| Undo Check Out | UCM CRUD Operation Resource Type:DOC1 | undo_checkout |
| Check In | UCM CRUD Operation Resource Type:DOC1 | checkin_processing checkin checkin_confirm_form |
| Update | UCM CRUD Operation Resource Type:DOC1 | update_metadata_ processing update_metadata |
| Delete | UCM CRUD Operation Resource Type:DOC1 | delete |
| Web Location | UCM CRUD Operation Resource Type:DOC1 | read |
| Folder Browse | UCM CRUD Operation Resource Type:.* | folder_browse retrieve_child_folders |
| Create Folder | UCM CRUD Operation Resource Type:.* | folder_browse create_folder |

9.5.10 Verification and Troubleshooting

This section contains the following topics:

- [Verifying Oracle WebCenter Content Is Working](#)
- [Troubleshooting Tips](#)

9.5.10.1 Verifying Oracle WebCenter Content Is Working

1. Test WebCenter Content by accessing Content Server with any user:
webcenter.example.com:16200/cs
2. Verify WebCenter Content is protected by Oracle Entitlements Server policies.

9.5.10.2 Troubleshooting Tips

This section provides tips for troubleshooting the Oracle WebCenter Content and Oracle Entitlements Server integration.

Changing the Log Level of Oracle WebCenter Content Server

Change the log level to `FINE` for the config logger

`oracle.security.oes.ucmconnector` on the WebLogic Server `UCM_server1` using the WLST `setLogLevel` command as follows:

1. Start the WLST shell.

```
cd $MW_HOME/Oracle_ECM1/common/bin
./wlst.sh
```

2. Connect to the WebLogic Administration Server using the WLST `connect` command.

```
connect("username", "password", "t3://hostname:port")
```

For example:

```
connect("weblogic", "welcome1", "webcenter.example.com:16200")
```

username is the administrator account name used to access the Administration Server

password is the administrator password used to access the Administration Server

hostname is the server name of the Administration Server

port is the port number of the Administration Server

3. Run the `setLogLevel` command.

For example:

```
setLogLevel(target="UCM_server1", logger="oracle.security.oes.ucmconnector",
level="FINE", persist=0)
```

target is the name of the WebLogic Server instance

logger is the full name of the logger to be modified. **Note:** the logger name is case-sensitive.

level specifies the log level. Some valid Java levels are: `SEVERE`, `WARNING`, `INFO`, `CONFIG`, `FINE`, `FINER`, or `FINEST`.

persist specifies if the level should be saved to the configuration file. The values are 0 (do not save the level) or 1 (save the level, which will persist across WebLogic re-starts). The default is 1.

4. When you have finished, use the `exit()` command to exit the WLST utility.

Oracle WebCenter Content Server Diagnostic Logs

It is helpful to tail the diagnostic logs in Oracle WebCenter Content Server to determine if the correct actions were taken.

Run the `tail` command.

For example:

```
tail -f $WCC_DOMAIN_HOME/servers/UCM_server1/logs/UCM_server1-diagnostic.log
```

Tail prints the last N number of lines from the given input. By default, it prints the last 10 lines of each given file. The `-f` option outputs the appended lines of the file.

Reduce Refresh Time of PEP

To reduce the refresh time of the PEP, you could add the following property to the `jps-config.xml` file:

```
<serviceInstance name="pdp.service" provider="pdp.service.provider">
  <description>Runtime PDP service instance</description>
  <property name="oracle.security.jps.ldap.policystore.refresh.interval"
    value="3000" />
```

9.5.11 Post-Integration Set Up (Example)

This section contains the following topics:

- [Creating Users in the OES Domain \(`oes_domain`\)](#)
- [Creating Users in the WebCenter Content Domain \(`wcc_domain`\)](#)
- [Adding Metadata Values Using the Configuration Manager in WebCenter Content](#)
- [Checking In Documents](#)

9.5.11.1 Creating Users in the OES Domain (`oes_domain`)

An example for creating users in the OES domain is shown below:

1. Start the `oes_domain` (OES Administration Server).
2. Log in to the Oracle WebLogic Server Administration Console.
3. Create users and groups in `oes_domain`. For example:
 - Create the user "Peter" and assign him to the "Junior Engineer" group.
 - Create the user "Sam" and assign him to the "Director" group.

9.5.11.2 Creating Users in the WebCenter Content Domain (`wcc_domain`)

An example for creating users in the WebCenter Content domain is shown below:

1. Log in to the Oracle WebLogic Server Administration Console.
2. Create users and groups in `wcc_domain`. For example:
 - Create the user "Peter" and assign him to the "Junior Engineer" group.
 - Create the user "Sam" and assign him to the "Director" group.

9.5.11.3 Adding Metadata Values Using the Configuration Manager in WebCenter Content

Metadata is data about data. To add metadata values using the Configuration Manager, proceed as follows:

1. Restart the Managed Server `UCM_server1`, stop the `wcc_domain` Administration and Managed Servers.
2. Navigate to:
`http://managedServerHost:16200/cs`
3. Choose **Administration** and then **Admin Applets** from the Main menu.
4. Click **Configuration Manager**.

5. In the Configuration Manager page, click **Add**.
6. When adding a metadata field, a **Add Metadata Field Name** dialog opens where you can enter the name. Duplicate names are not allowed. Maximum field length is 29 characters. Use only letters, numbers, and underscores (_). Do not use spaces or other special characters. Click **OK** when done.
7. Click **Enable Option List**, then click **Configure**.
8. In the Configure Option List dialog, click **Edit** next to Use Option List.
9. In the Option List dialog, enter the values available for the custom metadata field. Each value must be on a separate line, with a carriage return between values.
For example:
 - Public
 - Confidential
 - Secret
10. Click **OK** to save the list.
11. In the Configuration Manager, click **Update database design** and then **OK**.
12. In the Configuration Manager dialog top menu, click **Options, Publish Schema** and then **Close**.

9.5.11.4 Checking In Documents

To check in documents, proceed as follows:

1. Navigate to:
`http://managedServerHost:16200/cs`
2. Click the **New Check In** link.
3. Click **Browse** next to the **Primary File** field. Navigate to and select the file, then click **Open**.
4. If the Format field is displayed under the Primary File field, select the conversion format for the file.
5. Specify an alternate file by browsing or entering the path name and file name.
6. If the Format field is displayed under the Alternate File field and you specified an alternate file, select a conversion format for the file.
7. Accept the default revision in the Revision field. (You should change the revision only if there is a specific reason to do so.)
8. Enter any notes about the file in the Comments field.
9. Use the default release date, or enter a future release date in the Release Date field.
10. If you want the file to be unavailable as of a particular date, enter a date in the Expiration Date field.
11. If applicable, fill in any of your organization's custom metadata fields.
12. After you enter all the appropriate metadata values, click **Check In**.

Managing System Configurations

Security Module definitions and administrator configurations are defined within the top-level System Configuration tab in the Authorization Policy Manager Administration Console. This chapter contains the following topics.

- [Section 10.1, "Delegating With Administrators"](#)
- [Section 10.2, "Configuring Security Module Definitions"](#)
- [Section 10.3, "Configuring Identity Directory Service Profiles"](#)

10.1 Delegating With Administrators

Administrator Roles can be created to delegate management operations for policy objects. For example, Application and Policy Domain delegating administrators can be defined by creating an Administrator Role at the appropriate level and assigning the role Administration Privileges as well as a user, group, or another role. See [Chapter 11, "Delegating With Administrator Roles"](#) for more information. It includes a section on creating System Administrator Roles which can manage other types of Administrator Roles in any Application or Policy Domain.

10.2 Configuring Security Module Definitions

A Security Module is an Oracle Entitlements Server client that plays a key role in authorization. After an authorization request is generated, the Security Module evaluates policy data to determine if access to the resource will be granted or denied. An Application (the Oracle Entitlements Server object that represents the protected resource) must be *bound* to the Security Module that protects it. Binding Security Modules enables policy data to be transmitted to it for evaluation. The Policy Distribution Component (discussed in [Chapter 6, "Managing Policy Distribution"](#)) is the mechanism used to transmit policy data to the Security Modules.

Note: For more information about the authorization process, see [Section 1.4, "How Oracle Entitlements Server Processes Authorization Policies."](#)

The following sections document how to bind (and unbind) Security Module definitions to (and from) Application objects.

- [Section 10.2.1, "Creating a Security Module Definition"](#)
- [Section 10.2.2, "Binding an Application to a Security Module"](#)
- [Section 10.2.3, "Unbinding an Application From a Security Module"](#)

- Section 10.2.4, "Deleting a Security Module Definition"

Note: Before binding Security Module definitions, you must install and configure the Security Module. See Chapter 8, "Managing Security Module Configurations" for details.

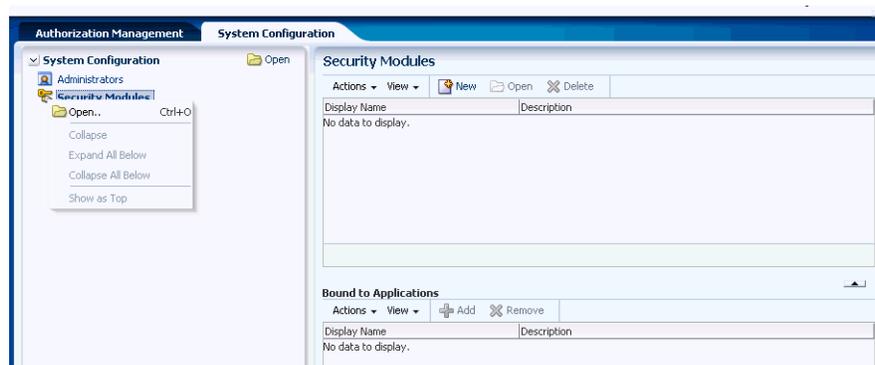
10.2.1 Creating a Security Module Definition

To create a security module, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click Security Modules in the Navigation Panel.

Alternately, right-click Security Modules and select Open. The Security Modules page is displayed as in Figure 10-1.

Figure 10-1 Security Modules in Home Area



3. Click New to create a new Security Module definition.
Alternately, select New from the Actions menu. The Security Module dialog is displayed.
4. Provide the following values for the new Security Module.
 - **Name:** The entry must be a unique.
 - **Display Name**
 - **Description**
5. Click Save.

10.2.2 Binding an Application to a Security Module

To bind an Application to a Security Module, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click Security Modules in the Navigation Panel.
Alternately, right-click Security Modules and select Open. The Security Modules page is displayed.
3. Select the name of the Security Module definition from the table.

4. Click Add in the Bound to Applications table to display the Add Applications dialog.
Alternately, select Add from the Bound to Applications Actions menu to display the Add Applications dialog.
5. Enter a search string in the text box and click the arrow to search.
Alternately, click the arrow with no search string to return all available Applications.
6. Select one or more applications from the list returned.
7. Click Add.
The selected applications are bound to the selected Security Module and displayed in the Bound to Applications table.

10.2.3 Unbinding an Application From a Security Module

To unbind an application from a Security Module, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click Security Modules in the Navigation Panel.
Alternately, right-click Security Modules and select Open. The Security Modules page is displayed.
3. Select the name of the applicable Security Module definition in the table.
4. Select the name of the applicable Application in the Bound to Applications table.
5. Click Remove or select Remove from the Actions menu.
A confirmation dialog is displayed.
6. Click Unbind.

10.2.4 Deleting a Security Module Definition

To remove a Security Module definition, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click Security Modules in the Navigation Panel.
Alternately, right-click Security Modules and select Open. The Security Modules page is displayed.
3. Select the name of the applicable Security Module definition in the table.
4. Click Delete or select Delete from the Actions menu.
A confirmation dialog is displayed.
5. Click Remove.

10.3 Configuring Identity Directory Service Profiles

When defining policies using Oracle Entitlements Server, users and groups need to be specified as the subject. This is done by searching an identity data store. The Identity Directory Service is a flexible and configurable service used by Oracle Entitlements Server as the means for accessing multiple identity data stores. The purpose of the

Identity Directory Service is to allow the management of policies that contain users or groups from identity stores not deployed with Oracle Entitlements Server itself.

An Application (the Oracle Entitlements Server object that represents the protected resource) must be *bound* to an Identity Directory Service profile to enable Oracle Entitlements Server to communicate with the identity store which the profile represents. By default, an Application is associated with the LDAP directory used for authentication when logging into the Administration Console. An administrator can change this association so that any identity data store configured with the Identity Directory Service can be used.

Note: Once an Identity Directory Service profile is bound to an Application, an Advanced or Simple Search can be initiated either globally (default option) or within the scope of the Application. The latter option searches in the identity data store configured for that Application. See [Chapter 5, "Querying Security Objects"](#) for more information.

The following sections document how to bind (and unbind) Identity Directory Service profiles to (and from) Application objects.

- [Section 10.3.1, "Creating an Identity Directory Service Profile"](#)
- [Section 10.3.2, "Binding an Application to an Identity Directory Service Profile"](#)
- [Section 10.3.3, "Unbinding an Application From an Identity Directory Service Profile"](#)
- [Section 10.3.4, "Deleting an Identity Directory Service Profile"](#)

Note: For information on the WebLogic Scripting Tool (WLST) commands for the Identity Directory Service, see *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

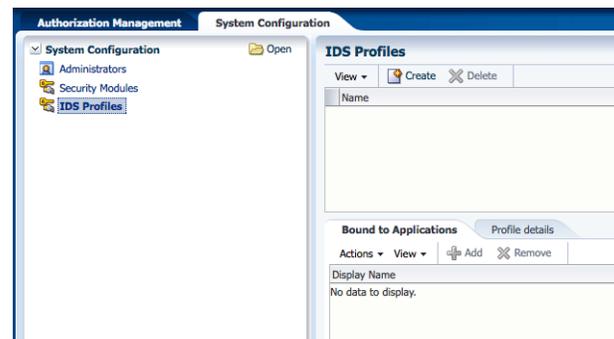
10.3.1 Creating an Identity Directory Service Profile

To create an Identity Directory Service profile, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click IDS Profiles in the Navigation Panel.

Alternately, select IDS Profiles and click Open. The IDS Profiles page is displayed as in [Figure 10-2](#).

Figure 10–2 IDS Profiles in Home Area



- Click Create to create a new Identity Directory Service profile.
The Create Identity Store Profile page is displayed as in Figure 10–3.

Figure 10–3 Create Identity Store Profile Page

 The screenshot shows the 'Create Identity Store Profile' dialog box. It has several sections:

- Name and Description:** Two text input fields.
- Repository Options:** Radio buttons for 'Create New' (selected) and 'Use Existing'. A 'Test Connection' button is on the right.
- Name and Directory Type:** A text field for 'Name' and a dropdown for 'Directory Type'.
- Host Information:** A table with columns 'Host Name', 'Port', and 'Load Weightage (%)'. The 'Port' is set to 3060 and 'Load Weightage (%)' is 100. There are '+ Add' and '- Remove' buttons.
- Availability:** Radio buttons for 'Failover' and 'Load balanced' (selected).
- SSL:** A checkbox for 'Enabled'.
- Bind Information:** Text fields for 'Bind DN', 'Bind Password', and 'Base DN'.
- User Section:**
 - 'Object Classes' with '+ Add' and '- Remove' buttons.
 - 'Object Class Name' dropdown set to 'inetorgperson'.
 - 'Name Attribute' text field set to 'loginid'.
 - 'Base DN' text field set to 'cn=users,dc=oracle,dc=com'.
- Group Section:**
 - 'Object Classes' with '+ Add' and '- Remove' buttons.
 - 'Object Class Name' dropdown set to 'groupofuniqueNames'.
 - 'Name Attribute' text field set to 'commonname'.
 - 'Base DN' text field set to 'cn=groups,dc=oracle,dc=com'.

 At the bottom right are 'Create' and 'Cancel' buttons.

- Provide the following values for the new Identity Directory Service profile.
 - Name: the entry must be a unique.
 - Description
- Select Create New or Use Existing and provide the applicable values to define the repository.
 - Name: the entry must be a unique.

- Directory Type - select from the drop-down menu
- Host Information - add Host name, Port number and Load Weightage percentage
- Availability - select Failover or Load balanced
- SSL - select to enable
- Bind DN
- Bind Password
- Base DN

Click Test Connection to confirm the values are correct.

6. Provide the applicable values to define how users can be found.

- Object Classes
- Name Attribute
- Base DN

7. Provide the applicable values to define how groups can be found.

- Object Classes
- Name Attribute
- Base DN

8. Click Create.

The profile is displayed in the IDS Profiles table.

10.3.2 Binding an Application to an Identity Directory Service Profile

To bind an Application to an Identity Directory Service profile, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click IDS Profiles in the Navigation Panel.
Alternately, select IDS Profiles and click Open.
3. Select the name of the Identity Directory Service profile from the upper table.
4. Click Add in the Bound to Applications table to display the Add Applications dialog.
Alternately, select Add from the Bound to Applications Actions menu to display the Add Applications dialog.
5. Enter a search string in the text box and click the arrow to search.
Alternately, click the arrow with no search string to return all available Applications.
6. Select one or more applications from the list returned.
7. Click Add.

The selected applications are bound to the selected Identity Directory Service profile(s) and displayed in the Bound to Applications table.

Note: If an Application is already bound to a Identity Directory Service profile and you want to bind it to a different Identity Directory Service profile, the Application will automatically be unbound from the first profile.

10.3.3 Unbinding an Application From an Identity Directory Service Profile

To unbind an application from an Identity Directory Service profile, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click IDS Profiles in the Navigation Panel.
Alternately, select IDS Profiles and click Open.
3. Select the name of the applicable Identity Directory Service profile in the table.
4. Select the name of the applicable Application in the Bound to Applications table.
5. Click Remove or select Remove from the Actions menu.
A confirmation dialog is displayed.
6. Click Unbind.

10.3.4 Deleting an Identity Directory Service Profile

To remove an Identity Directory Service profile, proceed as follows.

1. Select the System Configuration tab from the Home area.
2. Double-click IDS Profiles in the Navigation Panel.
Alternately, select IDS Profiles and click Open.
3. Select the name of the applicable Identity Directory Service profile in the table.
4. Click Delete.
A confirmation dialog is displayed.
5. Click OK.

Delegating With Administrator Roles

System administrative rights and policy management permissions can be delegated from one administrator to another by creating Administrator Roles with restricted rights, or by granting an existing Administrator Role to a user or existing External Role. This chapter documents information on how to delegate policy and system administrative tasks. It contains the following sections.

- [Section 11.1, "About Delegated Administrators"](#)
- [Section 11.2, "Delegating Using Scope and Granularity"](#)
- [Section 11.3, "Delegating Application Administration"](#)
- [Section 11.4, "Using Policy Domains to Delegate"](#)
- [Section 11.5, "Delegating Policy Domain Administration"](#)
- [Section 11.6, "Managing System Administrators Using Administrator Roles"](#)

11.1 About Delegated Administrators

Administration is when one or more authorized rights are granted to someone to do a certain job. Delegation is the ability for that someone to transfer the authorized right that has been granted them to another. In combination, we can define delegating administration as the transference of authorized rights from one to another. In Oracle Entitlements Server, administrators who are authorized to perform a task on policy objects and entities may transfer this right to others using Administration Roles. Administration Roles consist of a subject (the person to whom the role is granted), the resources (the objects to which the role pertains) and actions (view, manage/modify).

Note: See [Section 1.5.1, "Role-based Access Control \(RBAC\)"](#) for more details on roles.

Oracle Entitlements Server allows you to define delegating Administrator Roles by assigning Administration Privileges, and mapping external roles and users, to it. When a user is logged in as an Administrator, the Navigation Panel displays only the set of Applications the logged in user is authorized to administer. In point of fact, all objects that a delegating Administrator cannot administer are hidden. Any nondefault delegating Administrator Role can perform management operations if it is granted the Admin Role with VIEW and MANAGE privileges.

Note: A nondefault Administrator Role is any Administrator Role created manually. This would not include Administrator Roles automatically created when you create an Application or a Policy Domain.

The following restrictions also apply to Administrator Roles.

- Non-system level (delegating) Administration Roles can only manage other Administration Roles within its scope. For example, an Administration Role created for Application1 can manage Administration Roles in Application 1 Policy Domains but cannot manage peer Administration Roles in Application1, or any roles in Application2 and its Policy Domains. Scope and granularity are discussed further in [Chapter 11.2, "Delegating Using Scope and Granularity."](#)
- System level Administration Roles (as discussed in [Chapter 10, "Managing System Configurations"](#)) can manage delegating Administration Roles in any Application or Policy Domain.
- Nondefault Administration Roles (again, created manually) cannot manage default Administration Roles in any Application or Policy Domain.

11.2 Delegating Using Scope and Granularity

Delegated administration is all about transferring management of resources and policy objects from one person to another. The scope of the delegation (or range of objects covered by the delegation) is defined in levels. The granularity of administration defines the type of objects managed at each scope. A default Administration Role is automatically created when each scope is created; additional Administration Roles can be created later.

Note: The following is applicable to all default Administration Roles.

- Default Administrator Roles cannot be deleted individually.
 - If a Policy Domain is deleted, all Administration Roles (including the default) are deleted.
 - If the Application is deleted, all Administration Roles are deleted.
 - Privileges assigned to default Administrator Roles cannot be modified.
-
-

From highest to lowest, the scopes and applicable granularity are as follows:

- The top-level `SystemAdmin` has privileges to manage system-level resources as well as all policy-related objects. System resources include Administrator Roles, system configurations and Security Module bindings. Policy objects include the Application objects.

Note: System Administrators have rights to all policy objects, including all Application objects and child Policy Domains but they are primarily intended to manage configurations, Application objects, and the bindings between the two.

Information on managing system level Administrator Roles is in [Chapter 10, "Managing System Configurations."](#)

- Application administrators have privileges to manage all objects in the Application to which they are assigned. One `ApplicationPolicyAdmin` is generated for each Application that is created. They are primarily intended to delegate the management of policy objects within the Application (including the Policy Domains and its children, such as Functions, Attributes, Application Roles and Resource Types). For more information, see [Section 11.3, "Delegating Application Administration."](#)
- Policy Domain administrators have privileges to manage all child objects in the Policy Domain to which they are assigned. One `PolicyDomainAdmin` is generated for each Policy Domain that is created. They are primarily created to delegate the management of policies, permissions and resources within a Policy Domain. For an overview of this concept, see [Section 11.4, "Using Policy Domains to Delegate."](#) For additional information, see [Section 11.5, "Delegating Policy Domain Administration."](#)

11.3 Delegating Application Administration

The following sections explain how to manage administrators for an Application.

- [Section 11.3.1, "Adding a Delegated Administrator for An Application"](#)
- [Section 11.3.2, "Modifying or Deleting an Application's Delegated Administrator"](#)

11.3.1 Adding a Delegated Administrator for An Application

This procedure documents how to create a new Administrator Role and assign it to the applicable roles or users. To add a delegated administrator to an Application, proceed as follows.

1. Expand the Applications node in the Navigation Panel.
2. Select the Application to modify.
3. Right-click the Application name and select Open from the menu.

The General, Delegated Administrators, Policy Distribution and Simulation tabs are all active.

4. Click the Delegated Administrators tab.

The Application name is listed in the displayed table. Click the arrow next to the Application name to see the default `ApplicationPolicyAdmin` created when the Application object was created. Click the Administrator Role name to display its details, in tabs, below the Delegated Administrators table.

- Role Details
 - External Role Mapping
 - External User Mapping
5. Click New to create a new Administrator Role.

Be sure to select the name of the Application to activate New. Alternately, select the Application and select New from the Actions menu. A New Administrator Role dialog is displayed.

6. Provide the following values for the new Administrator Role and click OK.

- **Name:** The entry must be a unique.
 - **Display Name**
 - **Description**
7. Select the new Administrator Role to activate its configuration tabs.
The Role Details tab is active.
 8. Click Edit to define the role details.
An Edit Administrator Role dialog is displayed.
 9. Grant View or Manage privileges for the appropriate policy objects and click Save.

Figure 11–1 is the Edit Admin Role privileges pop up screen. Select View or Manage for the listed policy objects. For example, Admin Policy allows the administrator to assign new permissions to an Admin Role. Admin Role, however, allows the administrator to assign members to an Admin Role. See Section 2.3, "The Policy Object Glossary" for details on the other listed objects.

Figure 11–1 Edit Admin Role Pop Up Screen

Parent: AzUnionBank

Select the administration privilege level for each object below.

Set all privileges to: **No Privileges** | View Only | **View and Manage**

| Name | No Privileges | View Only | View and Manage |
|-------------------------------|----------------------------------|-----------------------|-----------------------|
| Admin Policy | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Application Role | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Policy Domain | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Extension | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Entitlement Set | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Admin Role | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Resource | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Policy | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Distribute Application Polic: | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Resource Type | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Role Category | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Save Cancel

10. Click the External Role Mapping tab to grant the Administrator Role to members of External Roles.
User and groups displayed are from the first LDAP provider with sufficient flag defined in WebLogic Server.
11. Click Add to display the Search Principals dialog.
12. Complete the query fields in the External Roles search box and click Search.
Empty strings fetch all roles. The results display in the Search Results table.
13. Select the external role to map to by clicking its name in the table.
Use Ctrl+click to select multiple roles.
14. Click Add Principals.
The selected roles display in the External Role Mapping tab.

15. Click the External User Mapping tab to grant the Administrator Role to External Users.
16. Click Add to display the Search Principals dialog.
17. Complete the query fields in the Users search box and click Search.
Empty strings fetch all roles. The results display in the Search Results table.
18. Select the user to map by selecting its name in the table.
Use Ctrl+click to select multiple roles.
19. Click Add Principals.
The selected roles display in the External User Mapping tab.

11.3.2 Modifying or Deleting an Application's Delegated Administrator

To modify or delete an Application's configured Administrator Role, proceed as follows.

1. Expand the Applications node in the Navigation Panel.
2. Select the Application to modify.
3. Right-click the Application name and select Open from the menu.
The General, Delegated Administrators, Policy Distribution and Simulation tabs are all active.
4. Click the Delegated Administrators tab.
5. Navigate to the Administrator Role you want to modify and select it.
The Role Details, External Role Mapping and External User Mapping tabs are displayed.
6. Select the tab which contains the configuration to modify or delete.
 - To modify the configuration, see [Section 11.3.1, "Adding a Delegated Administrator for An Application"](#) for details.
 - To remove a mapping from an Administrator Role, select the applicable Administrator Role and the appropriate Mapping tab. Select the mapping and click Remove.
 - To delete an Administrator Role, select the Administrator Role and click Delete.

11.4 Using Policy Domains to Delegate

Administration of the policies securing one protected application may be delegated using one or more (optional) Policy Domains. A Policy Domain contains the components of completed policy definitions. It is the amalgamation of a target Resource (an instance of the Resource Type), an Entitlement (the actions that can be performed on the Resource), and a Policy (a rule that assembles the controls and the principals they affect).

The use of multiple Policy Domains allows policies to be partitioned according to some defined logic, such as the architecture of the protected application or how administration of the policies are delegated. For example, one Policy Domain can be used to maintain all policies securing a Resource or multiple Policy Domains can be

used to reflect a particular characteristic of the Resource. Different administrators can then be placed in charge of different Policy Domains.

Note: Because the creation of a Policy Domain is optional, if there is no need to delegate policy administration, there is no need to create any Policy Domains. In this case, a default Policy Domain is created with each Application that will contain all the Application's policy objects.

The following sections contain the management procedures for Policy Domains.

- [Section 11.4.1, "Creating a Policy Domain"](#)
- [Section 11.4.2, "Modifying a Policy Domain"](#)
- [Section 11.4.3, "Deleting a Policy Domain"](#)

11.4.1 Creating a Policy Domain

To create a Policy Domain, proceed as follows.

1. Right-click the name of the Application in the Navigation Panel under which the Policy Domain will be created and select New from the menu.

An Untitled page displays in the Home area.

2. Provide the following information for the Policy Domain.
 - **Display Name**
 - **Name**
 - **Description:** Although optional, it is recommended to provide useful information about the entitlement.
3. Select one of the following from the Save menu.
 - Save and Close saves the configuration and renames the tab with the value provided for the Policy Domain's Display Name.
 - Save and Create Another saves the configuration to the information tree in the Navigation Panel but leaves the Untitled area open for you to create another Application.

11.4.2 Modifying a Policy Domain

To modify a Policy Domain, proceed as follows.

1. Navigate to the Application under which the Policy Domain you want to delete was created and expand the information tree.

2. Double click the name of the Policy Domain you want to modify.

The Policy Domain configuration displays in the Home area.

3. Modify as necessary and click Apply.

11.4.3 Deleting a Policy Domain

To delete a Policy Domain, proceed as follows.

1. Navigate to the Application under which the Policy Domain you want to delete was created and expand the information tree.

2. Double click the name of the Policy Domain you want to delete.
The Policy Domain configuration displays in the Home area.
3. Click Delete.
A confirmation dialog is displayed.
4. Click OK to delete.

11.5 Delegating Policy Domain Administration

The following sections describe how to manage administrators for Policy Domains.

- [Section 11.5.1, "Adding a Delegated Administrator to a Policy Domain"](#)
- [Section 11.5.2, "Modifying or Deleting a Policy Domain's Delegated Administrator"](#)

11.5.1 Adding a Delegated Administrator to a Policy Domain

This procedure documents how to create a new Administrator Role and assign it to the applicable roles or users. To add a delegated administrator to a Policy Domain, proceed as follows.

1. Expand the Applications node in the Navigation Panel.
2. Select the Application to modify.
3. Right-click the Application name and select Open from the menu.
The General, Delegated Administrators, Policy Distribution and Simulation tabs are all active.
4. Click the Delegated Administrators tab.
The Policy Domain names are listed in the displayed table. Clicking the arrow next to the Policy Domain expands the hierarchy and displays any Administrator Roles already configured; for example, the default `PolicyDomainAdmin`.
5. Select the Policy Domain under which you will create the Administrator Role.
6. Click New to create a new Administrator Role.
Be sure to select the name of the Policy Domain to activate New. Alternately, select the Policy Domain and select New from the Actions menu. A New Administrator Role dialog is displayed.
7. Provide the following values for the new Administrator Role and click OK.
 - **Name:** The entry must be a unique.
 - **Display Name**
 - **Description**
8. Select the new Administrator Role to activate its configuration tabs.
The Role Details tab is active.
9. Click Edit to define the role details.
An Edit Administrator Role dialog is displayed.
10. Grant View or Manage privileges for the appropriate Policy Domain objects and click Save.
11. Click the External Role Mapping tab.

- a. Click Add to display the Search Principals dialog.
 - b. Complete the query fields in the External Roles search box and click Search. Empty strings fetch all roles. The results display in the Search Results table.
 - c. Select the external role to map to by clicking its name in the table. Use Ctrl+click to select multiple roles.
 - d. Click Add Principals. The selected roles display in the External Role Mapping tab.
12. Click the External User Mapping tab.
- a. Click Add to display the Search Principals dialog.
 - b. Complete the query fields in the Users search box and click Search. Empty strings fetch all roles. The results display in the Search Results table.
 - c. Select the user to map by selecting its name in the table. Use Ctrl+click to select multiple roles.
 - d. Click Add Principals. The selected roles display in the External User Mapping tab.

11.5.2 Modifying or Deleting a Policy Domain's Delegated Administrator

To modify or delete a Policy Domain's configured Administrator Role, proceed as follows.

1. Expand the Applications node in the Navigation Panel.
2. Select the Application to modify.
3. Right-click the Application name and select Open from the menu. The General, Delegated Administrators, Policy Distribution and Simulation tabs are all active.
4. Click the Delegated Administrators tab.
5. Navigate to the Administrator Role you want to modify and select it. The Role Details, External Role Mapping and External User Mapping tabs are displayed.
6. Select the tab which contains the configuration to modify or delete.
 - To modify the configuration, see [Section 11.5.1, "Adding a Delegated Administrator to a Policy Domain"](#) for details.
 - To remove a mapping from an Administrator Role, select the applicable Administrator Role and the appropriate Mapping tab. Select the mapping and click Remove.
 - To delete an Administrator Role, select the Administrator Role and click Delete.

11.6 Managing System Administrators Using Administrator Roles

You can delegate system administration privileges to users by creating and configuring System Administrator Roles. By default, `SystemAdmin` is created during

installation and is displayed in the System Administrators table when you navigate to System Administrators under the main System Configuration tab. `SystemAdmin` manages system-level resources (including other Administrator Roles, and system configurations and bindings) and maps to the WebLogic Server `weblogic` user.

The following sections document the management operations for all Oracle Entitlements Server System Administrator Roles.

- [Section 11.6.1, "Creating a New Administrator Role"](#)
- [Section 11.6.2, "Assigning Privileges to an Administrator Role"](#)
- [Section 11.6.3, "Modifying Administrator Role Membership"](#)
- [Section 11.6.4, "Deleting an Administrator Role"](#)

11.6.1 Creating a New Administrator Role

To create a new Administrator Role, proceed as follows.

1. Select the System Configuration tab from the Home area.
The System Administrators tab is displayed in the Home area.
2. Click New under Administrator Roles to create a new Administrator Role.
A dialog is displayed.
3. Provide the following values for the new Administrator Role.
 - **Name:** The entry must be a unique.
 - **Display Name**
 - **Description**
4. Click Create.

11.6.2 Assigning Privileges to an Administrator Role

To assign privileges to an Administrator Role, map external roles, external users or both to the role as documented in this procedure.

1. Select the System Configuration tab from the Home area.
The System Administrators tab and configured Administrator Roles are displayed in the Home area. Alternately, right-click Administrators and select Open.
2. Select the name of the Administrator Role from the table.
3. Select the Modify or View option to define the Administrator Control.
Modify defines the administrator as having management (and by proxy viewing) privileges on all system administrator resources. View defines the administrator as having only viewing privileges.
4. Click the External Role Mapping tab.
 - a. Click Add or select Add from the Actions menu.
The Add Roles search dialog is displayed.
 - b. Enter a search string in the text box and click the arrow to search for External Roles.
Alternately, click Search with no search string to return all available External Roles.

4. Click Delete.
A confirmation dialog is displayed.
5. Click Remove.

Customizing the Administration Console

This chapter explains several customizations you can make to Oracle Authorization Policy Manager, the Oracle Entitlements Server Administration Console. It contains the following sections.

- Section 12.1, "Customizing Authorization Policy Manager"
- Section 12.2, "Customizing Headers, Footers, and Logo"
- Section 12.3, "Customizing Color Schemes"
- Section 12.4, "Customizing the Login Page"

12.1 Customizing Authorization Policy Manager

All customizations described in this chapter require modifying data in one or both of the following file archives:

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

Tip: Before you begin, it is recommended that you backup these Authorization Policy Manager EAR and WAR files.

Any customizations applied to a version of Authorization Policy Manager must be specified again every time a new version is installed. The following procedure specifies, from a high level, how to customize Authorization Policy Manager.

1. Unzip the EAR, WAR and view WAR files using the following commands:

```
$ unzip -d $tempDir/ear $ORACLE_IDM_HOME$/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 $ORACLE_IDM_HOME$/apm/modules/  
oracle.security.apm_11.1.1/oracle.security.apm.core.view.war
```

2. Modify one or more of the unzipped files as documented in one of the following sections of this chapter.
 - Section 12.2, "Customizing Headers, Footers, and Logo"
 - Section 12.3, "Customizing Color Schemes"
 - Section 12.4, "Customizing the Login Page"
3. Rearchive the modified EAR, WAR and view WAR files using the following commands:

```

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

```

4. Redeploy Authorization Policy Manager.

12.2 Customizing Headers, Footers, and Logo

Use the following procedure to customize headers, footers, and the logo.

1. Unzip the view WAR file.

```

$ORACLE_IDM_HOME$/apm/modules/oracle.security.apm_
  11.1.1/oracle.security.apm.core.view.war

```

2. Open AuthPolicyMgr.jspx file and apply any or all of the following modifications.

- Specify a new branding title (header) by modifying the branding facet.

```

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

```

- Specify a new footer by modifying the appAbout and appCopyright facets.

```

<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>

```

- Specify a new logo image as follows:

- a. Insert your resource in the metaContainer facet.

```

<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>

```

Be sure to leave all other content inside the metaContainer facet as is.

- b. Specify the style class name (defined in the previous step) as the attribute value of the pageTemplate tag.

```

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

```

Be sure to leave all other content inside the `pageTemplate` tag as is.

3. Rearchive the view WAR file.

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

4. Redeploy Authorization Policy Manager.

12.3 Customizing Color Schemes

You can develop a new skin to apply to a web application. Use the following procedure to customize the Authorization Policy Manager color scheme. It assumes that you have a new skin available to reference.

Note: Authorization Policy Manager uses the Oracle Application Development Framework (ADF) and supports ADF skinning. See the *Oracle Fusion Middleware Skin Editor User's Guide for Oracle Application Development Framework* for more information on ADF skins.

1. Unzip the EAR and WAR files.

```
$ unzip -d $tempDir/ear $ORACLE_IDM_HOME$/apm/modules/oracle.security.apm_
  11.1.1/oracle.security.apm.ear
$ unzip -d $tempDir/war $tempDir/ear/oracle.security.apm.war
```

2. Open the `Trinidad-config.xml` file.

This file is typically located in the decompressed WAR's `WEB-INF` folder.

3. Specify the value of the new skin location in the `skin-family` tag.

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

4. Rearchive the modified EAR and WAR files using the following commands:

```
$ zip $tempDir/ear/oracle.security.apm.war $tempDir/war/*
$ zip $ORACLE_IDM_HOME$/apm/modules/oracle.security.apm_
  11.1.1/oracle.security.apm.ear $tempDir/ear/*
```

5. Redeploy Authorization Policy Manager.

12.4 Customizing the Login Page

Use the following procedure to customize the login and login error pages.

1. Unzip the EAR file.

```
$ unzip -d $tempDir/ear $ORACLE_IDM_HOME$/apm/modules/oracle.security.apm_
  11.1.1/oracle.security.apm.ear
```

2. Open the `web.xml` file.

This file is typically located in the decompressed EAR's `WEB-INF` folder.

3. Specify the appropriate values for the `form-login-page` and `form-error-page` under the element `form-login-config`.

```
<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>
```

4. Rearchive the modified EAR file using the following commands:

```
$ zip $ORACLE_IDM_HOME$/apm/modules/oracle.security.apm_
    11.1.1/oracle.security.apm.ear $tempDir/ear/*
```

5. Redeploy Authorization Policy Manager.

Management Tasks

This chapter contains information on several management and configuration tasks including configuring Security Modules and the cache, auditing, and migrating policies from different types of policy stores. It contains the following sections.

- Section 13.1, "Moving from a Test Environment to Production (T2P)"
- Section 13.2, "Using the Policy Simulator"
- Section 13.3, "Using FIPS-compliant Security Providers"
- Section 13.4, "Managing Audit Tasks"
- Section 13.5, "Migrating Policies"
- Section 13.6, "Configuring Cache"
- Section 13.7, "Logging"
- Section 13.8, "Debugging"

13.1 Moving from a Test Environment to Production (T2P)

Test to Production (T2P) is the process of migrating the Oracle Entitlements Server Administration Console from a test environment to a production environment. The T2P process is only applicable to the console component (an application running in a WebLogic Server domain) as Security Modules do not maintain their own data. The following procedure documents the T2P process.

1. Move the Database, Middleware Homes, and Domain Configuration to the new production environment as documented in *Oracle Fusion Middleware Administrator's Guide*.
2. Install Oracle Entitlements Server in the new production environment.
3. Move Oracle Platform Security Services to the new production environment as documented in *Oracle Fusion Middleware Administrator's Guide*.

13.2 Using the Policy Simulator

Oracle Entitlements Server provides a feature to simulate a policy from the Administration Console. Policy simulation allows you to troubleshoot, test, analyze the effect of policy changes, and understand how policies on a given application are enforced. The following sections contain more information.

- Section 13.2.1, "Understanding Policy Simulation"
- Section 13.2.2, "Choosing the Policy Simulation Mode"

- [Section 13.2.3, "Running the Policy Simulator"](#)

13.2.1 Understanding Policy Simulation

In the simplest policy simulation case, a user and resource-action pair are specified and the following information is retrieved, based on the parameters:

- External Roles that would be granted to the principal, and a list of static role grants and Role Mapping Policies.
- List of attributes required to evaluate any relevant role or authorization policy.
- Value of any evaluation functions that were executed as part of a relevant role or authorization policy.
- Value of any dynamic attributes that is part of a relevant role, authorization policy, or obligation. If a dynamic attribute value is unknown, it should be returned as blank so the user can explicitly set it.
- The final authorization decision returned (*grant* or *deny*), obligations, and the Authorization Policies that were involved.

If attribute values are evaluated as part of the authorization decision, you can perform additional simulations using different values. The sequence of events is:

1. Specify a principal, resource and action.
The Principal can be a user, a set of External Roles or a set of Application Roles. If External Roles and Application Roles are explicitly specified with the user, role resolution will not be performed.
2. Simulate the policy.
3. Specify which attribute to override and provide values for the ones that they want to override.
4. Re-run the Policy Simulator to see any changed results.

13.2.2 Choosing the Policy Simulation Mode

The Policy Simulator has two modes: Simple and Advanced. The modes have different purposes. Simple mode is typically used for debugging purposes to determine the authorization result for a given Subject and Resource combination. It allows security administrators to understand why a particular user has (or does not have) access to the specified Resource. Advanced mode is for policy simulation - to see what happens, for example, if a user is made a member of a particular set of External Roles and Application Roles. Based on the simulation, security administrators can add or revoke a user's role membership based on the runtime authorization decisions for the specified Resource. Defining values in Simple Mode and clicking Check Access will:

- Display the results of the policy evaluation including the authorization decision, obligations (if any), and a list of attributes required to evaluate any relevant role or policy. If an attribute value cannot be retrieved, it will be returned as blank.
- Display the set of External Roles to which the specified user belongs. This list facilitates selecting a user's External Roles for running the Policy Simulator in Advanced mode.
- Display the Application Roles granted to (or denied) the specified user and the Role Mapping Policies in which the user is specified. The roles may include static and dynamic roles granted by Role Mapping Policies directly or indirectly (through inheritance).

- Display the Authorization Policies used for evaluating access.

Defining values in Advanced Mode involves providing 0 or 1 user, a set of External Roles, a set of Application Roles or any combination of the three as Principal. The results displayed are as in Simple Mode except if External Roles and Application Roles are specified; in this case, group resolution will not be computed.

13.2.3 Running the Policy Simulator

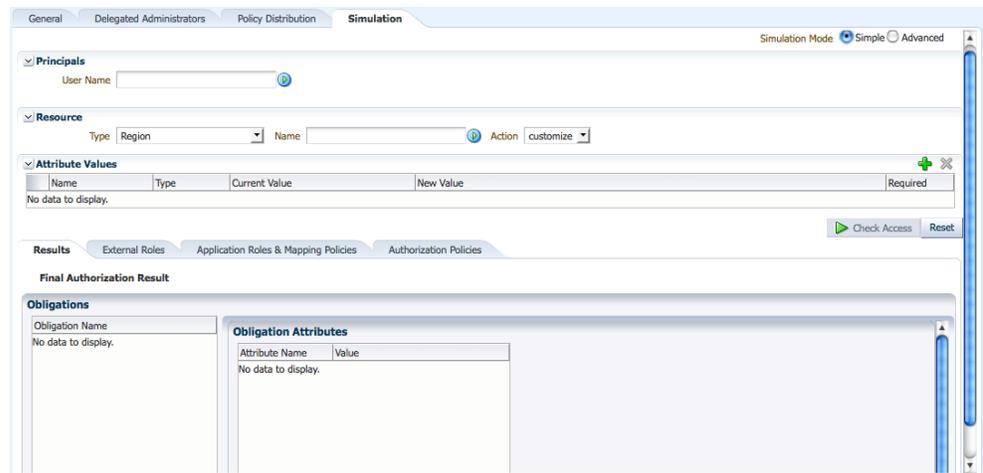
The Policy Simulator is displayed as a tab when a configured Application is open for the Administration Console. The tab is only enabled after an Application object has been created and only for the administrator with modify privileges for the Application. The following sections document how to run the Policy Simulator.

- [Section 13.2.3.1, "Running the Policy Simulator in Simple Mode"](#)
- [Section 13.2.3.2, "Running the Policy Simulator in Advanced Mode"](#)

13.2.3.1 Running the Policy Simulator in Simple Mode

Figure 13–1 is a screenshot of the Policy Simulator in Simple Mode. Use the procedure in this section to run the Policy Simulator in Simple Mode.

Figure 13–1 Policy Simulator User Interface in Simple Mode



1. Select the Application name that contains the policies and click Open.
2. Click the Simulation tab.
3. Click the Simple radio button.

A Simple run is used when defining one user as a Principal.
4. Search for and select one Principal.
 - a. Enter Search criteria in the User Name box and click the Search arrow.

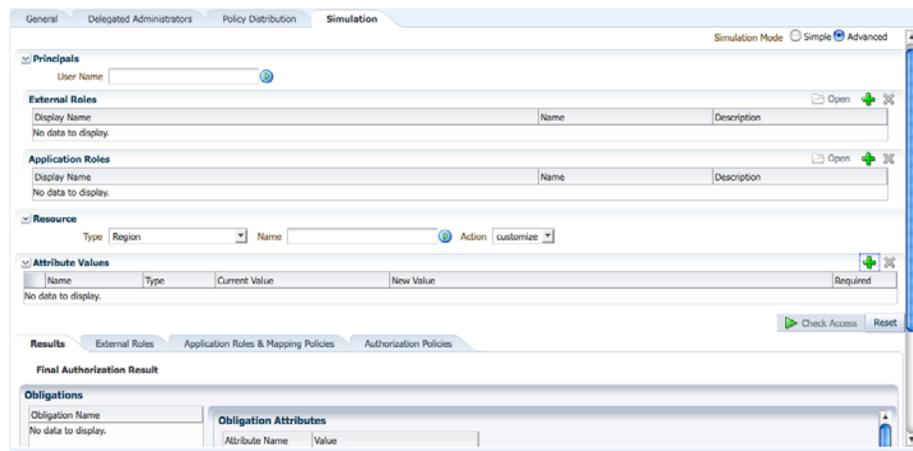
The User Search results are displayed.
 - b. Select the appropriate row in the User Search and click Add to select the user as a Principal.
5. Search for and select a Resource.
 - a. Choose the Resource Type (of which the Resource is an instance) from the drop down menu.

- b. Choose the appropriate Action Name from the drop down menu.
 - c. Enter search criteria for the Resource instance name and click the search arrow.
The Resources are displayed. Optionally, further refine the search results by selecting a Policy Domain, entering additional search criteria and clicking the Search arrow.
6. Add an attribute to the Policy Simulation test.
- Attributes are used in Conditions. To evaluate a policy, values are needed for the attributes. If the attribute has a default value, it will be used. (The default value can be overrode here as well.) If no default value, the Simulator will prompt for one.
- a. Click the Green Plus to add an attribute.
Use the search pop-up to select a defined attribute and specify the value based on its data type.
 - b. Enter a Name.
 - c. Enter a New Value.
7. Click Check Access.
The Policy Simulator executes. See [Section 13.2.2, "Choosing the Policy Simulation Mode"](#) for details on the results.

13.2.3.2 Running the Policy Simulator in Advanced Mode

Figure 13–2 is a screenshot of the Policy Simulator in Advanced Mode. In Advanced Mode, you can define only one user, as well as Application Roles or External Roles. Use the procedure in this section to run the Policy Simulator in Advanced Mode.

Figure 13–2 Policy Simulator User Interface in Advanced Mode



1. Select the Application name that contains the policies and click Open.
2. Click the Simulation tab.
3. Click the Advanced radio button.
4. Search for and select a User Name, an External Role or an Application Role as the Principal.
At least one of a User Name, External Role or Application Role must be defined.

- a. Enter Search criteria in the User Name box and click the Search arrow.
The User Search results are displayed.
 - b. Select the appropriate row in the User Search and click Add to select the user as a Principal.
 - c. Click the Green Plus to add an External Role.
The External Roles Search dialog is displayed.
 - d. Enter Search criteria and click the Search.
The Search Results are displayed.
 - e. Select the appropriate row(s) in the Search Results and click Add Selected or click Add All to add all results.
The roles are added. In Advanced Mode, the Policy Simulator will not compute the user's External Roles. If that computation is needed, you must specifically add them.
 - f. Click the Green Plus to add an Application Role.
The Application Roles Search dialog is displayed.
 - g. Enter Search criteria and click the Search.
The Search Results are displayed.
 - h. Select the appropriate row(s) in the Search Results and click Add Selected or click Add All to add all results.
The roles are added. In Advanced Mode, the Policy Simulator will not compute the user's Application Roles. If that computation is needed, you must specifically add them.
5. Search for and select a Resource.
 - a. Choose the Resource Type (of which the Resource is an instance) from the drop down menu.
 - b. Choose the appropriate Action Name from the drop down menu.
 - c. Enter search criteria for the Resource instance name and click the search arrow.
The results are displayed. Optionally, further refine the search results in the Resource Finder by selecting a Policy Domain, entering additional search criteria and clicking the Search arrow.
6. Add an attribute to the Policy Simulation test.

Attributes are used in Conditions. To evaluate a policy, values are needed for the attributes. If the attribute has a default value, it will be used. (The default value can be overrode here as well.) If no default value, the Simulator will prompt for one.

 - a. Click the Green Plus to add an attribute.
Use the search pop-up to select a defined attribute and specify the value based on its data type.
 - b. Enter a Name.
 - c. Enter a New Value.
7. Click Check Access.

The Policy Simulator executes. See Section 13.2.2, "Choosing the Policy Simulation Mode" for details on the results.

13.3 Using FIPS-compliant Security Providers

The Federal Information Processing Standard (FIPS) is developed by the United States government to standardize security requirements for cryptography modules. Support for the FIPS allows integration of Oracle Entitlements Server with disparate Java Cryptography Extension (JCE) security providers.

Note: Security services were limited to the container's default security providers in previous releases.

13.3.1 Installing the JCE Provider

Before configuring the JCE provider, it must be installed and registered. Detailed information on how to do this can be found in the *Java Cryptography Extension API Specification and Reference*.

Note: Java Cryptography Extension (JCE) documentation can be downloaded from Oracle Technology Network (OTN) web site by navigating to the following URL:

<http://www.oracle.com/technetwork/index.html>

13.3.2 Configuring JCE

The following `jps-config.xml` parameters are used for configuring the JCE security provider. Back up the policy cache files before modifying these JCE provider parameters.

- `oracle.security.jps.runtime.pd.client.localpolicy.JCEProviderName` indicates the JCE provider being used. It is optional and if not specified, the default JDK provider will be used. No default value is defined and any value used is case-sensitive.
- `oracle.security.jps.runtime.pd.client.localpolicy.CipherKeyLength` indicates the key length used for the Cipher class from the specified JCE provider. It is optional and the default value is 128. Only three key lengths (128, 192 and 256) are supported.
- `oracle.security.jps.runtime.pd.client.localpolicy.CipherModePadding` indicates the cipher algorithm name, mode and padding schema used for the Cipher class from the specified JCE provider. The format should be *algorithm-name/mode/padding*. It is optional, not case-sensitive and the default value is `AES/CBC/PKCS5Padding`.

13.4 Managing Audit Tasks

Oracle Entitlements Server audits all administrative activities and authorization requests, optionally recording the information to a file. The auditing framework is based on the framework developed for Oracle Platform Security Services. An overview of the Oracle Platform Security Services auditing framework can be found in *Oracle Fusion Middleware Application Security Guide*. The following information is specific to the auditing functionality in Oracle Entitlements Server.

- Section 13.4.1, "Auditing Oracle Entitlements Server Events"
- Section 13.4.2, "Enabling Audit"
- Section 13.4.3, "Loading the Audit Log to a Database"
- Section 13.4.4, "Configuring Oracle Entitlements Server Security Modules for Auditing"
- Section 13.4.5, "Additional Auditing Information"

Note: Oracle Entitlements Server will audit decisions resulting from policies configured by itself, Oracle Platform Security Services or any combination thereof.

13.4.1 Auditing Oracle Entitlements Server Events

If audit is enabled, all actions from the Authorization Policy Manager Console (policy artifacts CRUD, domain creation and deletion, Security Module creation and deletion, Policy distribution, Grant, Administrator Role management and so on) log audit events.

Table 13–1 lists the events (organized by functional category) that are audited by Oracle Entitlements Server.

Table 13–1 Events Audited in Oracle Entitlements Server

| Functional Category | Functional Task |
|--------------------------------|--|
| Administration Role Management | <ul style="list-style-type: none"> ■ AdminRoleCreation ■ AdminRoleDeletion ■ AdminRoleGrant ■ AdminRoleRevoke ■ AdminRoleResActionGrant ■ AdminRoleResActionRevoke |
| Application Management | <ul style="list-style-type: none"> ■ ApplicationDeletion |
| Grant Management | <ul style="list-style-type: none"> ■ PermissionSetGrant ■ PermissionSetRevocation |
| PermissionSetManagement | <ul style="list-style-type: none"> ■ PermissionSetCreation ■ PermissionSetModification ■ PermissionSetDeletion |
| PolicyDomainManagement | <ul style="list-style-type: none"> ■ PolicyDomainCreation ■ PolicyDomainDeletion |
| PolicyManagement | <ul style="list-style-type: none"> ■ PolicyCreation ■ PolicyModification ■ PolicyDeletion ■ PolicyGrant ■ PolicyRevoke |
| ResourceManagement | <ul style="list-style-type: none"> ■ ResourceCreation ■ ResourceModification ■ ResourceDeletion |

Table 13–1 (Cont.) Events Audited in Oracle Entitlements Server

| Functional Category | Functional Task |
|--------------------------------|---|
| Role Management | <ul style="list-style-type: none"> ■ RoleCreation ■ RoleModification ■ RoleDeletion ■ RoleMembershipAdd ■ RoleMembershipRemove |
| RolePolicyManagement | <ul style="list-style-type: none"> ■ RolePolicyCreation ■ RolePolicyModification ■ RolePolicyDeletion |
| Authorization | <ul style="list-style-type: none"> ■ CheckPermission ■ CheckSubject |
| ConfigurationBindingManagement | <ul style="list-style-type: none"> ■ SecurityModuleBinding ■ SecurityModuleUnbinding |
| ConfigurationManagement | <ul style="list-style-type: none"> ■ SecurityModuleCreation ■ SecurityModuleModification ■ SecurityModuleDeletion |
| PolicyDistributionManagement | <ul style="list-style-type: none"> ■ PolicyDistribution ■ purgeDistributionStatus |

Audit configuration changes log the following events:

- ConfigureAuditPolicy
- ConfigureAuditRepository

OES Audit Database Description for JPS.IAU_ACCESSRESULT and IAU_BASE.IAU_FAILURECODE Columns

The value of JPS.IAU_ACCESSRESULT can be:

(DecisionTime:xxx) (IsAllowed:[true|false])

or

(DecisionTime:xxx) (IsAllowed: [true|false])
 (ResponseAttributes([(Name:xxx) (value:xxx)] [responseAttribute2]
 [responseAttribute3]))

The value of IAU_BASE.IAU_FAILURECODE can be "success", error message key "JPS-XXXXX" or exception message.

13.4.2 Enabling Audit

To enable audit in Oracle Entitlements Server, perform the following steps:

1. Connect to the WebLogic Server using the following command:


```
connect('username', 'password', t3://hostname:adminPort')
```
2. Update the audit policy configuration by using the setAuditPolicy command:


```
setAuditPolicy(filterPreset="Low", componentType="JPS")
```

The audit level for Oracle Entitlements Server is controlled by the value of `filterPreset`. It can be `Low`, `Medium`, `High` and `All`.

3. Check the audit log file at:

```
$DOMAIN_HOME/servers/AdminServer/logs/auditlogs/JPS/audit.log
```

13.4.3 Loading the Audit Log to a Database

You can load audit log to a database if you want. This section explains how to set up the auditing database. It contains the following topics:

- Section 13.4.3.1, "Creating the Audit View Schema using RCU"
- Section 13.4.3.2, "Extending the OES Domain using the IDM Configuration Wizard"
- Section 13.4.3.3, "Configuring Audit Settings"

13.4.3.1 Creating the Audit View Schema using RCU

This section explains how to create the audit view schema. You must run the Repository Creation Utility (RCU) to create the Audit view schema in the database. The database must be up and running before you start RCU.

The Repository Creation Utility (RCU) is available on the Oracle Technology Network (OTN) Web site at:

<http://www.oracle.com/technology/software/products/middleware>

Take these steps to configure an audit view schema for the audit data store:

1. Ensure the database is up and running.
2. After downloading the .zip file, extract the contents to a directory of your choice; this directory will be referred to as the `RCU_HOME` directory.
3. Start RCU from the bin directory inside the `RCU_HOME` directory.

```
cd RCU_HOME/bin
./rcu
```

4. In the Welcome screen, click **Next**.
5. In the Create Repository screen, click **Create** and then, **Next**.
6. In the Database Connection Details screen, specify the connection details for your database, then click **Next**. When the database checking has passed without errors, click **OK** to dismiss the dialog window and go to the next screen.
7. In the Select Components screen, specify a schema prefix.

For example:

For the OPSS Audit Schema: `prefix_IAU_APPEND`

For the OPSS Audit Viewer Schema: `prefix_IAU_VIEWER`

Expand and select Oracle AS Repository Components in the Component column, and select **Audit Services** with the Schema Owner **IAU**. Click **Next**. Then select Identity Management. The Checking Component Prerequisites dialog box appears. After the checking is complete with no errors, click **OK** to dismiss the dialog box and go to the next screen.

8. In the Schema Passwords screen, specify a password for the schema owner. For a development system, you might want to select **Use same passwords for all schemas**. Click **Next**.
9. In the Map Tablespaces screen, configure the desired tablespace mapping for the schemas you want to create, then click **Next**.
A separate dialog window will appear asking you to confirm that you want to create these tablespaces. Click **OK** to proceed and dismiss the dialog window. A second dialog window will appear showing the progress of tablespace creation. After this is complete, click **OK** to dismiss this window and go to the next screen.
10. In the Summary screen, review the information on this screen, then click **Create** to begin schema creation.
11. In the Completion Summary screen, note the location of the log files, then click **Close** to dismiss the screen.

13.4.3.2 Extending the OES Domain using the IDM Configuration Wizard

Use the Oracle Fusion Middleware Configuration Wizard to extend the existing OES domain. Start the Oracle Fusion Middleware Configuration Wizard by running the `ORACLE_HOME/common/bin/config.sh` script (on UNIX), or `ORACLE_HOME\common\bin\config.cmd` (on Windows)

On Select Domain Source screen, select **Extend my domain automatically to support the following added products**. Then choose, **Oracle Platform Security Services for Audit 11.1.1.0 [oracle_common]**.

On Specify Domain Name and Location screen, provide the Domain Name.

On the Configure JDBC Component Schema screen, select the OPSS Audit Schema and the OPSS Audit Viewer Schema.

For example:

For the OPSS Audit Schema: `prefix_IAU_APPEND`

For the OPSS Audit Viewer Schema: `prefix_IAU_VIEWER`

Then, provide details for the Schema Owner, Schema Password, DBMS/Service, Host Name, and Port. Use the information from the Audit View Schema you created earlier.

13.4.3.3 Configuring Audit Settings

After extending the domain, configure the audit settings using the WLST script.

1. Navigate to `ORACLE_HOME/common/bin` and run the `setAuditRepository` script:

```
> connect('username', 'password', 't3://hostname:adminPort')
> setAuditRepository(redirectToDB="true", jdbcString =
"jdbc:oracle:thin:@host:port/service", dbUser = "prefix_IAU_APPEND",
dbPassword = "database_password")
```

2. Check the `jps-config.xml` file. The audit setting should look similar to the following:

```
<serviceInstance name="audit" provider="audit.provider"
location="./audit-store.xml">
  <description>Audit Service</description>
  <property name="audit.filterPreset" value="None"/>
  <property name="audit.maxDirSize" value="0"/>
  <property name="audit.maxFileSize" value="104857600"/>
```

```

<property name="audit.timezone" value="utc"/>
<property name="audit.loader.jndi" value="jdbc/AuditDB"/>
<property name="audit.loader.interval" value="15"/>
<property name="audit.loader.repositoryType" value="DB"/>
<property name="auditstore.type" value="file"/>
</serviceInstance>

```

Table 13–2 contains details about the configuration parameters.

Table 13–2 Auditing Parameters in `jps-config.xml`

| Parameter | Description |
|-----------------------------|---|
| audit.filterPreset | Enable auditing by choosing from the following values: None (default), Low, Medium, All or Custom |
| audit.maxDirSize | Controls the size of the directory in which the audit files are written. Takes an integer in bytes. |
| audit.maxFileSize | Controls the size of the bus stop file in which audit events are written. Takes an integer in bytes. |
| audit.loader.jndi | When a database is in use, takes a path to the JNDI data source to which audit events are uploaded. |
| audit.loader.interval | When a database is in use, controls the frequency of the audit loader's upload. Takes an integer in seconds. |
| audit.loader.RepositoryType | Defines the audit repository type. Takes a value of File or Db . <ul style="list-style-type: none"> ■ Use Db if loading audit records from a file to a data base. If type is database (Db), <code>audit.loader.jndi</code> must also be defined. ■ Use File if loading audit records from a data base to a file. |
| auditstore.type | Takes as a value <code>file</code> or <code>db</code> depending on the audit store type. |

13.4.4 Configuring Oracle Entitlements Server Security Modules for Auditing

To configure auditing for Oracle Entitlements Server Security Modules, first apply the Oracle Entitlements Server Bundle Patch 1 (BP1) and then create the audit database.

Note: See the *Oracle Fusion Middleware Release Notes for Microsoft Windows x64 (64-Bit)* for information on completing Oracle Entitlements Server audit schema definitions. The procedure can be done before or after creating the audit database.

After completing these steps, use one of the following procedures depending on the deployed Security Module.

- [Section 13.4.4.1, "Configuring the WebLogic Server Security Module"](#)
- [Section 13.4.4.2, "Configuring Other Security Modules"](#)

13.4.4.1 Configuring the WebLogic Server Security Module

1. Create and configure the data source to the audit database, and deploy the data source to the server using the WebLogic Server console.

See *Oracle Fusion Middleware Application Security Guide* for details.

2. Restart the server.

3. Add the following content before the final `</serviceInstances>` tag in the `jps-config.xml` file.

In a non JRF domain, `jps-config.xml` is located in the `WLSSM_Client_Domain\config\oeswlssmconfig\AdminServer\` directory. In a JRF domain, `jps-config.xml` is located in the `WLSSM_Client_Domain\config\fmwconfig\` directory.

```
<serviceInstance name="audit" provider="audit.provider">
  <property name="audit.filterPreset" value="All"/>
  <property name="audit.maxDirSize" value="0"/>
  <property name="audit.maxFileSize" value="104857600"/>
  <property name="audit.loader.jndi" value="auditdb"/>
  <property name="audit.loader.interval" value="15" />
  <property name="audit.loader.repositoryType" value="Db" />
</serviceInstance>
```

4. Restart the servers.

`audit.log` is created under the `WLSSM_Client_Domain/servers/AdminServer/logs/auditlogs/JPS/` directory.

5. Run the database `set password` command to set a password for the audit database.

When prompted, enter the password for your audit schema. See *Oracle Fusion Middleware Application Security Guide* for details.

6. Run the audit loader to load the events and actions from the `audit.log` file to the audit database.

A message that confirms the number of events transferred is displayed after a successful action. See *Oracle Fusion Middleware Application Security Guide* for details.

13.4.4.2 Configuring Other Security Modules

1. Add the following content before the final `</serviceInstances>` tag in the `jps-config.xml` file (located in the `OES_Client11115\oes_sm_instances\SM_Name\config\` directory) to set up the audit database loader.

```
<serviceInstance name="audit" provider="audit.provider"
  location="./audit-store.xml">
  <description>Audit Service</description>
  <property name="audit.loader.jndi" value="jdbc/AuditDB"/>
  <property name="audit.loader.interval" value="15"/>
  <property name="audit.loader.repositoryType" value="Db"/>
```

where:

- The value of `audit.loader.repositoryType` must be `Db`.
 - The database schema for the audit loader should be created using the Repository Creation Utility (RCU).
 - The datasource being connected to the database should be configured as the value of `audit.loader.jndi`.
2. Run the database `set password` command to set a password for the audit database.

When prompted, enter the password for your audit schema. See *Oracle Fusion Middleware Application Security Guide* for details.

3. Run the audit loader to load the events and actions from the `audit.log` file to the audit database.

A message that confirms the number of events transferred is displayed after a successful action. Be sure to define the `-Doracle.instance` parameter with the path to the Security Module instance and database details. See *Oracle Fusion Middleware Application Security Guide* for details.

13.4.5 Additional Auditing Information

The following list collects chapter links in other documents with information regarding the auditing framework.

- Introductory material can be found in *Oracle Fusion Middleware Security Guide*.
- For descriptions of common audit attributes, such as failure code, see the "Event Attribute Descriptions" section in the Oracle Fusion Middleware Audit Framework Reference chapter of *Oracle Fusion Middleware Application Security Guide*, 11g Release 1 (11.1.1).
- For authorization and policy management attributes, see the "Oracle Platform Security Services Events and their Attributes" section in the Oracle Fusion Middleware Audit Framework Reference chapter of *Oracle Fusion Middleware Application Security Guide*, 11g Release 1 (11.1.1).
- For information on the audit schema, see the "The Audit Schema" section in the Oracle Fusion Middleware Audit Framework Reference chapter of *Oracle Fusion Middleware Application Security Guide*, 11g Release 1 (11.1.1).
- You can manage audit policies with the Enterprise Manager user interface or with the WebLogic Scripting Tool (WLST) command-line interface. See *Oracle Fusion Middleware Application Security Guide* for guidance.
- The Oracle Fusion Middleware Audit Framework Reference is in *Oracle Fusion Middleware Application Security Guide*.
- Additional configuration information is in *Oracle Fusion Middleware Security Guide*.

13.5 Migrating Policies

This section contains information regarding migrating policies from one type of store to another. It contains procedures for the following:

- Section 13.5.1, "Migrating From XML to LDAP"
- Section 13.5.2, "Migrating From LDAP to XML"
- Section 13.5.3, "Migrating From XML to Database"
- Section 13.5.4, "Migrating From Database to XML"

13.5.1 Migrating From XML to LDAP

Following is the procedure to migrate policies from an XML-based policy store to an LDAP-based directory.

1. Modify `jps-config.xml` as described in this sub procedure.
 - a. Create a `serviceInstance` for both the source and destination policy stores as illustrated in [Example 13-1](#).

The location of the source policy store instance must be defined as relative to the location of `jps-config.xml` defined as the value of `configFile` when using the `migrateSecurityStore` command. [Example 13–1](#) assumes that `jps-config.xml` and `jazn-data.xml` (the source policy store) are located in the same directory.

Example 13–1 XML to LDAP serviceInstances for Source and Destination Policy Stores

```
<!-- Source XML-based policy store instance -->
  <serviceInstance name="src.xml" provider="policystore.xml.provider"
    location="./jazn-data.xml">
    <description>File Based Policy Store Service Instance</description>
  </serviceInstance>

<!-- Destination LDAP-based policy store instance -->
  <serviceInstance provider="ldap.policystore.provider"
    name="policystore.ldap.destination">
  <description>Replace: A. myDestDomain and myDestRootName to appropriate
    values according to your destination LDAP directory structure;
    B. ldap://myDestHost.com:3060 with the URL and port
    number of your destination LDAP</description>
  <property value="OID" name="policystore.type"/>
  <property value="bootstrap" name="bootstrap.security.principal.key"/>
  <property value="cn=myDestDomain" name="oracle.security.jps.farm.name"/>
  <property value="cn=myDestRootName"
    name="oracle.security.jps.ldap.root.name"/>
  <property value="ldap://myDestHost.com:3060" name="ldap.url"/>
</serviceInstance>
```

- b. Create a `serviceInstance` corresponding to the bootstrap credential used to access the destination LDAP directory as illustrated in [Example 13–2](#).

Example 13–2 XML to LDAP serviceInstance for Bootstrap Credential

```
<!-- Bootstrap credentials to access destination LDAP -->
  <serviceInstance location="./bootstrap" provider="credstoressp"
    name="bootstrap.cred">
  <description>Replace location with the full path of the directory
    where the bootstrap file cwallet.sso is located;
    typically found in destinationDomain/config/fmwconfig/bootstrap
  </description>
</serviceInstance>
```

- c. Create a `jpsContext` for both source and destination stores as illustrated in [Example 13–3](#).

Example 13–3 XML to LDAP jpsContext for Source and Destination Policy Stores

```
<jpsContext name="sourceContext">
  <serviceInstanceRef ref="src.xml"/>
</jpsContext>

<jpsContext name="destinationContext">
  <serviceInstanceRef ref="policystore.ldap.destination"/>
</jpsContext>

<jpsContext name="bootstrap_credstore_context">
  <serviceInstanceRef ref="bootstrap.cred"/>
</jpsContext>
```

2. Start the WebLogic Scripting Tool.

There is no need to connect the WebLogic Scripting Tool to the WebLogic Server as the migration command is an offline command.

3. Run the WebLogic Scripting Tool `migrateSecurityStore` command to migrate the policy store and application as follows.

- To migrate the policy store, run:

```
migrateSecurityStore
  (type="policyStore", src="sourceContext",
   dst="destinationContext",
   configFile="myDir/jps-config.xml")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.

- To migrate the application, run:

```
migrateSecurityStore
  (type="appPolicies", src="sourceContext",
   dst="destinationContext",
   configFile="myDir/jps-config.xml",
   srcApp="sourceApplication", dstApp="destinationApplication",
   overWrite="true")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.
- The name of the application being migrated is the value of the `srcApp` parameter. `srcApp` is a required parameter for `type="appPolicies"`. Without this value, an error message reading *The source application is undefined but required to migrate application-specific policies.* is displayed and the migration will fail.
- The name that is assigned to the application in the destination policy store is the value of the `dstApp` parameter. If this parameter is not passed, the name of the application in the destination store is the same as the name used in the source store.
- If the `overWrite` parameter is defined as `true`, policies specific to the destination application are replaced by policies from the source application. The default value of this parameter is `false` which migrates only the additive changes.

13.5.2 Migrating From LDAP to XML

Following is the procedure to migrate policies from an LDAP-based directory to an XML-based policy store.

1. Modify `jps-config.xml` as described in this sub procedure.
 - a. Create a `serviceInstance` for both the source and destination policy stores as illustrated in [Example 13-4](#).

Example 13-4 LDAP to XML `serviceInstances` for Source and Destination Policy Stores

```
<!-- Source LDAP-based policy store instance -->
<serviceInstance provider="ldap.policystore.provider"
  name="policystore.ldap.source">
  <description></description>
  <property value="OID" name="policystore.type"/>
  <property value="bootstrap" name="bootstrap.security.principal.key"/>
  <property value="cn=mySourceDomain" name="oracle.security.jps.farm.name"/>
  <property value="cn=mySourceRootName"
    name="oracle.security.jps.ldap.root.name"/>
  <property value="ldap://mySourceHost.com:3060" name="ldap.url"/>
</serviceInstance>

<!-- Destination XML-based policy store instance -->
<serviceInstance name="dst.xml" provider="policystore.xml.provider"
  location="/scratch/example_user/WithPSR/jazn-data-fscm.xml">
  <description>File Based Policy Store Service Instance</description>
</serviceInstance>
```

- b. Create a `serviceInstance` corresponding to the bootstrap credential used to access the destination LDAP directory as illustrated in [Example 13-5](#).

Example 13-5 LDAP to XML `serviceInstance` for Bootstrap Credential

```
<!-- Bootstrap credentials to access source LDAP -->
<serviceInstance location="./bootstrap" provider="credstoressp"
  name="bootstrap.cred">
  <description>Replace location with the full path of the directory where the
    bootstrap file cwallet.sso is located; typically found in
    destinationDomain/config/fmwconfig/bootstrap</description>
</serviceInstance>
```

- c. Create a `jpsContext` for both source and destination stores as illustrated in [Example 13-6](#).

Example 13-6 LDAP to XML `jpsContext` for Source and Destination Policy Stores

```
<jpsContext name="sourceContext">
  <serviceInstanceRef ref="policystore.ldap.source"/>
</jpsContext>

<jpsContext name="destinationContext">
  <serviceInstanceRef ref="dst.xml"/>
</jpsContext>

<jpsContext name="bootstrap_credstore_context">
  <serviceInstanceRef ref="bootstrap.cred"/>
</jpsContext>
```

2. Start the WebLogic Scripting Tool.

There is no need to connect the WebLogic Scripting Tool to the WebLogic Server as the migration command is an offline command.

3. Run the WebLogic Scripting Tool `migrateSecurityStore` command to migrate the policy store and application as follows.

- To migrate the policy store, run:

```
migrateSecurityStore
  (type="policyStore", src="sourceContext",
   dst="destinationContext",
   configFile="myDir/jps-config.xml")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.

- To migrate the application, run:

```
migrateSecurityStore
  (type="appPolicies", src="sourceContext",
   dst="destinationContext",
   configFile="myDir/jps-config.xml",
   srcApp="sourceApplication", dstApp="destinationApplication",
   overWrite="true")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.
- The name of the application being migrated is the value of the `srcApp` parameter. `srcApp` is a required parameter for `type="appPolicies"`. Without this value, an error message reading *The source application is undefined but required to migrate application-specific policies.* is displayed and the migration will fail.
- The name that is assigned to the application in the destination policy store is the value of the `dstApp` parameter. If this parameter is not passed, the name of the application in the destination store is the same as the name used in the source store.
- If the `overWrite` parameter is defined as `true`, policies specific to the destination application are replaced by policies from the source application. The default value of this parameter is `false` which migrates only the additive changes.

13.5.3 Migrating From XML to Database

Following is the procedure to migrate policies from an XML-based policy store to a database.

Note: The value of the `bootstrap.security.principal.key` property needs to be populated with the key generated during reassociation of the policy, credential, and key stores from one repository type to another.

1. Modify `jps-config.xml` as described in this sub procedure.
 - a. Create a `serviceInstance` for both the source and destination policy stores as illustrated in [Example 13-7](#).

Example 13-7 XML to Database `serviceInstances` for Source and Destination Policy Stores

```
<!-- Source XML-based policy store instance -->
<serviceInstance name="src.xml" provider="policystore.xml.provider"
  location="/scratch/example_user/WithPSR/jazn-data-fscm.xml">
  <description>File Based Policy Store Service Instance</description>
</serviceInstance>

<!-- Destination DB-based policy store instance -->
<serviceInstance provider="ldap.policystore.provider"
  name="policystore.db.destination">
<description>DB Based Policy Store Service Instance</description>
<property name="policystore.type" value="DB_ORACLE"/>
<property name="jdbc.url"
  value="jdbc:oracle:thin:@sc.domainexample.com:1722:orcl"/>
<property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver"/>
<property name="bootstrap.security.principal.key"
  value="bootstrap_DWgpEJgXwhDIoLYVZ2OWd4R8wOA=" />
<property name="oracle.security.jps.ldap.root.name" value="cn=jpsTestNode"/>
<property name="oracle.security.jps.farm.name" value="cn=view_steph.atz"/>
</serviceInstance>
```

- b. Create a `serviceInstance` corresponding to the bootstrap credential used to access the destination LDAP directory as illustrated in [Example 13-8](#).

Example 13-8 XML to Database `serviceInstance` for Bootstrap Credential

```
<!-- Bootstrap credentials to access source DB -->
<serviceInstance location="./bootstrap" provider="credstoressp"
  name="bootstrap.cred">
<description>Replace location with the full path of the directory
  where the bootstrap file wallet.sso is located;
  typically found in destinationDomain/config/fmwconfig</description>
</serviceInstance>
```

- c. Create a `jpsContext` for both source and destination stores as illustrated in [Example 13-9](#).

Example 13-9 XML to Database `jpsContext` for Source and Destination Policy Stores

```
<jpsContext name="sourceContext">
  <serviceInstanceRef ref="src.xml"/>
</jpsContext>

<jpsContext name="destinationContext">
  <serviceInstanceRef ref="policystore.db.destination"/>
</jpsContext>
```

```
<jpsContext name="bootstrap_credstore_context">
  <serviceInstanceRef ref="bootstrap.cred"/>
</jpsContext>
```

2. Start the WebLogic Scripting Tool.

There is no need to connect the WebLogic Scripting Tool to the WebLogic Server as the migration command is an offline command.

3. Run the WebLogic Scripting Tool `migrateSecurityStore` command to migrate the policy store and application as follows.

- To migrate the policy store, run:

```
migrateSecurityStore
  (type="policyStore", src="sourceContext",
   dst="destinationContext",
   configFile="/scratch/example_user/WithPSR/jps-config.xml")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.

- To migrate the application, run:

```
migrateSecurityStore
  (type="appPolicies", src="sourceContext",
   dst="destinationContext",
   configFile="/scratch/example_user/WithPSR/jps-config.xml",
   srcApp="sourceApplication", dstApp="destinationApplication",
   overWrite="true")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.
- The name of the application being migrated is the value of the `srcApp` parameter. `srcApp` is a required parameter for `type="appPolicies"`. Without this value, an error message reading *The source application is undefined but required to migrate application-specific policies.* is displayed and the migration will fail.
- The name that is assigned to the application in the destination policy store is the value of the `dstApp` parameter. If this parameter is not passed, the name of the application in the destination store is the same as the name used in the source store.
- If the `overWrite` parameter is defined as `true`, policies specific to the destination application are replaced by policies from the source application. The default value of this parameter is `false` which migrates only the additive changes.

13.5.4 Migrating From Database to XML

Following is the procedure to migrate policies from a database to an XML-based policy store.

Note: The value of the `bootstrap.security.principal.key` property needs to be populated with the key generated during reassociation of the policy, credential, and key stores from one repository type to another.

1. Modify `jps-config.xml` as described in this sub procedure.
 - a. Create a `serviceInstance` for both the source and destination policy stores as illustrated in [Example 13–10](#).

Example 13–10 Database to XML serviceInstances for Source and Destination Policy Stores

```
<!-- Source DB-based policy store instance -->
<serviceInstance provider="policystore.provider"
  name="policystore.db.source">
  <description>DB Based Policy Store Service Instance</description>
  <property name="policystore.type" value="DB_ORACLE" />
  <property name="jdbc.url"
    value="jdbc:oracle:thin:@sc.domainexample.com:1722:orcl" />
  <property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver" />
  <property name="bootstrap.security.principal.key"
    value="bootstrap_DWgpEJgXwhDIOLYVZ2OWd4R8wOA=" />
  <property name="oracle.security.jps.ldap.root.name" value="cn=jpsTestNode" />
  <property name="oracle.security.jps.farm.name" value="cn=view_steph.atz" />
</serviceInstance>

<!-- Destination XML-based policy store instance -->
<serviceInstance name="dst.xml" provider="policystore.xml.provider"
  location="/scratch/example_user/WithPSR/jazn-data-fscm.xml">
  <description>File Based Policy Store Service Instance</description>
</serviceInstance>
```

- b. Create a `serviceInstance` corresponding to the bootstrap credential used to access the destination XML directory as illustrated in [Example 13–11](#).

Example 13–11 Database to XML serviceInstance for Bootstrap Credential

```
<!-- Bootstrap credentials to access source and destination stores -->
<serviceInstance location="./bootstrap" provider="credstoressp"
  name="bootstrap.cred">
  <description>Replace location with the full path of the directory where
    the bootstrap file cwallet.sso is located; typically found in
    destinationDomain/config/fmwconfig</description>
</serviceInstance>
```

- c. Create a `jpsContext` for both source and destination stores as illustrated in [Example 13–12](#).

Example 13–12 Database to XML jpsContext for Source and Destination Policy Stores

```
<jpsContext name="sourceContext">
  <serviceInstanceRef ref="policystore.db.source" />
</jpsContext>
```

```
<jpsContext name="destinationContext">
  <serviceInstanceRef ref="dst.xml"/>
</jpsContext>

<jpsContext name="bootstrap_credstore_context">
  <serviceInstanceRef ref="bootstrap.cred"/>
</jpsContext>
```

2. Start the WebLogic Scripting Tool for the migration.

There is no need to connect the WebLogic Scripting Tool to the WebLogic Server as the migration command is an offline command.

3. Run the WebLogic Scripting Tool `migrateSecurityStore` command to migrate the policy store and application as follows.

- To migrate the policy store, run:

```
migrateSecurityStore
  (type="policyStore", src="sourceContext",
   dst="destinationContext",
   configFile="/scratch/example_user/WithPSR/jps-config.xml")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.

- To migrate the application, run:

```
migrateSecurityStore
  (type="appPolicies", src="sourceContext",
   dst="destinationContext",
   configFile="/scratch/example_user/WithPSR/jps-config.xml",
   srcApp="sourceApplication", dstApp="destinationApplication",
   overwrite="true")
```

where the following applies:

- The name of the corresponding `jpsContext` (previously created in Step 1) should be passed to the `src` and `dst` parameters.
- The name of the `jps-config.xml` file (previously modified in Step 1) should be passed to the `configFile` parameter. The value must be a fully qualified file name with complete path information.
- The name of the application being migrated is the value of the `srcApp` parameter. `srcApp` is a required parameter for `type="appPolicies"`. Without this value, an error message reading *The source application is undefined but required to migrate application-specific policies.* is displayed and the migration will fail.
- The name that is assigned to the application in the destination policy store is the value of the `dstApp` parameter. If this parameter is not passed, the name of the application in the destination store will be the same as the name used in the source store.

- If the `overWrite` parameter is defined as `true`, policies specific to the destination application are replaced by policies from the source application. The default value of this parameter is `false` which migrates only the additive changes.

13.6 Configuring Cache

Oracle Entitlements Server offers caching capabilities. The cache settings are configured in the `jps-config.xml` file. The following sections contain the appropriate information.

- [Section 13.6.1, "Configuring Decision Caching"](#)
- [Section 13.6.2, "Configuring Attribute Caching"](#)

13.6.1 Configuring Decision Caching

Authorization decision caching allows Oracle Entitlements Server to cache the result of an authorization call and use that decision in the future, if an identical call is made. The decision cache consists of two hierarchical levels.

- The first level (L1) caches subjects used in the authorization calls.
- The second level (L2) caches authorization and role mapping decisions for the given subject.

Note: The decision cache automatically invalidates itself if there is a change in the policy.

The key of the cache is the incoming Subject, Permission and attributes used during policy evaluation. The value of the cache is the decision and obligations.

All parameter names are prefixed with `oracle.security.jps.pdp`. [Example 13–13](#) illustrates how the decision cache parameters might be set in `jps-config.xml`.

Example 13–13 XML To Configure Decision Caching

```
<serviceInstance name="pdp.service" provider="pdp.service.provider">
  ...
  <property name="oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled"
    value="true"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheEvictionCapacity"
    value="1000"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheEvictionPercentage"
    value="15"/>
  <property name="oracle.security.jps.pdp.AuthorizationDecisionCacheTTL"
    value="180"/>
  ...
</serviceInstance>
```

[Table 13–3](#) documents the decision caching parameters.

Table 13–3 Decision Caching Parameters

| Name | Description | Accepted Values |
|--|---|--|
| oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled | Optional parameter that specifies whether the policy decision cache should be enabled. | true (default) false |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionCapacity | Optional parameter that specifies the maximum capacity of the L1 cache. If the number of entries exceeds the value, some entries are evicted. | Integer representing number of entries 500 (default) |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage | Optional parameter that specifies the percentage of entries in L1 cache that have to be evicted when the maximum capacity has been reached. For example, if the maximum capacity is 200 and the value of this parameter is 10 then 20 entries are evicted from the cache. | Integer representing percent of entries 10 (default equals 10%) |
| oracle.security.jps.pdp.AuthorizationDecisionCacheTTL | Optional parameter that specifies a time-to-live value (in seconds) for entries in the L2 cache. It defines how long an authorization decision is cached. | Integer representing time in seconds 60 (default equals 1 minute) |

13.6.2 Configuring Attribute Caching

Each passed attribute can be cached if the cached property is defined for it. A corresponding time-to-live (TTL) value must also be defined if cached is enabled. The key of the cache is the attribute URI. The value of the cache is the attribute object.

[Example 13–14](#) illustrates how the attribute cache might be set in `jps-config.xml`.

Example 13–14 XML To Configure Attribute Caching

```
<propertySet name="ootb.pip.attribute.age.based.on.myattr.rdbms">
  <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
  <property name="ootb.pip.ref" value="pip.service.ootb.db"/>
  <property name="name" value="myattr"/>
  <property name="query" value=
    "select myattr from test where username=%SYS_USER%"/>
  <property name="cached" value="true"/>
  <property name="TTL" value="60"/>
</propertySet>
```

Note: If `cached` is not defined for the attribute, it will not be cached.

13.7 Logging

Oracle Entitlements Server uses the standard Java package `java.util.logging` for logging. The name of the logging setup file is `logging.properties`. It is the standard configuration file for the Java Development Kit (JDK) and it is located (by default) in `$JAVA_HOME/jre/lib/`.

Note: Configure the location of `logging.properties` by running the following on the command line with the actual path based on your install.

```
-Djava.util.logging.config.file=/path/filename
```

Java logging defines log levels to control output ranging from FINEST (indicating a highly detailed tracing message) to SEVERE (indicating fatal program errors and the like). Enabling logging at a given level also enables logging at all higher levels. [Table 13–4](#) contains the specific logger properties that can be set to FINE (details for debugging and diagnosing problems) to provide information for purposes of troubleshooting server issues.

Table 13–4 Logging Server Issues

| To Troubleshoot... | Set These Properties To FINE |
|---|--|
| Policy management issues | <ul style="list-style-type: none"> ■ <code>oracle.jps.policymgmt</code> |
| Basic authorization issues | <ul style="list-style-type: none"> ■ <code>oracle.jps.authorization</code> |
| Policy distribution issues | <ul style="list-style-type: none"> ■ <code>oracle.oes.pd</code> ■ <code>oracle.oes.common</code> |
| Security Module issues | <ul style="list-style-type: none"> ■ <code>oracle.oes.sm</code> |
| Specific tool issues (for example, <code>enroll.sh</code>) | <ul style="list-style-type: none"> ■ <code>oracle.oes.tool</code> |

After modifying `logging.properties`, ensure the `java.util.logging.config.file` system property is set by running the following command:

```
-Djava.util.logging.config.file=<directory>/logging.properties
```

[Example 13–15](#) is the default Oracle Entitlements Server `logging.properties` file.

Example 13–15 Default logging.properties Configuration File

```
#####
# Default Logging Configuration File
# You can use a different file by specifying a filename
# with the java.util.logging.config.file system property.
# For example java -Djava.util.logging.config.file=myfile
#####
# Global properties
#####
# "handlers" specifies a comma separated list of log Handler
# classes. These handlers will be installed during VM startup.
# Note that these classes must be on the system classpath.
# By default we only configure a ConsoleHandler, which will only
# show messages at the INFO and above levels.
handlers= java.util.logging.ConsoleHandler, java.util.logging.FileHandler
# To also add the FileHandler, use the following line instead.
#handlers= java.util.logging.FileHandler, java.util.logging.ConsoleHandler
# Default global logging level.
# This specifies which kinds of events are logged across
# all loggers. For any given facility this global level
# can be overridden by a facility specific level
# Note that the ConsoleHandler also has a separate level
# setting to limit messages printed to the console.
```

```

.level= WARNING
#####
# Handler specific properties.
# Describes specific configuration info for Handlers.
#####
# default file output is in user's home directory.
java.util.logging.FileHandler.pattern = /logs/java%u.log
java.util.logging.FileHandler.limit = 50000000
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.XMLFormatter
# Limit the message that are printed on the console to INFO and above.
java.util.logging.ConsoleHandler.level = FINE
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter
#####
# Facility specific properties.
#####
# Provides extra control for each logger.
#####
# For example, set the com.xyz.foo logger to only log SEVERE
# messages:
oracle.oes.sm.level=FINE
oracle.oes.common.level=FINE
oracle.oes.tool.level=FINE
oracle.oes.pd.level=FINE
oracle.jps.policymgmt.level=FINE
oracle.jps.authorization.level=FINE
oracle.jps.common.level=FINE

```

13.8 Debugging

Policy debugging allows for analysis of the policy evaluation process for a given authorization call. The debugging capabilities of the Oracle Entitlements Server runtime are collected in the DebugStore which provides (among other information):

- Authorization and Role Mapping Policies (and the appropriate policy objects) involved during the evaluation process
- Attributes that were evaluated and their values
- Results of function invocations
- Roles granted or denied the requesting subject
- Policy evaluation result (GRANT, DENY, NOT APPLICABLE)
- Obligations and Conditions (if applicable)
- Failed authentications, missing group memberships and other incorrect identity values

A client can access debugging information in either of the following ways. The first option entails configuring debugging parameters to see the information in a standard debug log. The second option entails overloading the `isAccessAllowed_debug()` and `getRoles_debug()` methods. These two methods return an additional `DebugInfo` parameter which is populated with debug information during policy evaluation. This second option is used by end users as well as the policy simulation tool. The following sections have more information on these options.

- [Section 13.8.1, "Enabling Debugging By Defining Parameters"](#)
- [Section 13.8.2, "Enabling Debugging Using Methods"](#)

Section 13.8.3, "Debugging Policy Distribution" contains information on debugging the policy distribution process.

13.8.1 Enabling Debugging By Defining Parameters

The following sections contain information on how to configure debugging parameters and read the debugging logs.

- [Configuring Logging for Debugging](#)
- [Searching Logs to Debug Authorization Policies](#)

13.8.1.1 Configuring Logging for Debugging

When policy outcomes are other than expected, it may be useful to enable debugging so that the Security Module's logs will capture all events related to policy decisions. The following sections contain information on how to debug Authorization Policies created using Oracle Entitlements Server and how to debug the Policy Distribution process.

Oracle Entitlements Server uses the standard Java logging framework for capturing debugging details. Logging is the process of notifying an entity of a particular event. In the case of Oracle Entitlements Server, the entity can be a file or the Administration Console, and the event can be debugging information, runtime exceptions, or a record of actions taken by a user. The logging framework is configured based on the Oracle Entitlements Server deployment. More information is in the following sections.

- [Section 13.8.1.1.1, "Configuring Logging for a Java Security Module"](#)
- [Section 13.8.1.1.2, "Configuring Logging for a WebLogic Server Security Module"](#)

Note: The `java.util.logging` package provides the classes and interfaces of the platform's core logging facilities.

13.8.1.1.1 Configuring Logging for a Java Security Module The following configurations must be made to enable logging when the Java Security Module is deployed.

- Run the following command when you start the Security Module to specify the logging configuration file:

```
-Djava.util.logging.config.file=logging.properties
```

- Set the logging level by adding the following lines to the configuration file:

```
oracle.jps.authorization.level=FINEST
oracle.jps.openaz.level=FINEST
oracle.jps.authorization.debugstore.level=FINEST
```

Keep the default level of the first property and set the level of the last two to FINEST; this configuration will log the result of a policy evaluation. Logging levels define the complexity of the logging record and include (from the least complex to the most) FINEST (simple information), FINER, FINE, CONFIG, INFO, WARNING and SEVERE (complex information).

If you don't specify a configuration file, the `logging.properties` file in `$JAVA_HOME/jre/lib/` is used. [Example 13–16](#) illustrates how to configure `logging.properties` to log information to the Administration Console.

Example 13–16 Configuration for Administration Console Logging

```
#The messages will we printed to the standard output
handlers=java.util.logging.ConsoleHandler

#The default level for all loggers is INFO
.level=INFO

#Override the default level for OES authorization to FINEST
oracle.jps.authorization.level=FINEST
oracle.jps.openaz.level=FINEST

#Use default formatter to print the messages
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter
```

[Example 13–17](#) illustrates how to configure logging.properties to log information to a file.

Example 13–17 Configuration for File Logging

```
#The messages will be written to a file
handlers=java.util.logging.FileHandler

#The default level for all loggers is INFO
.level=INFO

#Override the default level for OES authorization to FINEST
oracle.jps.authorization.level=FINEST
oracle.jps.openaz.level=FINEST

#Configure file information. %h - is the user home directory
java.util.logging.FileHandler.pattern = %h/java%u.log
java.util.logging.FileHandler.limit = 50000
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter
```

13.8.1.1.2 Configuring Logging for a WebLogic Server Security Module To enable logging when the WebLogic Server Security Module is deployed, run the following command to specify the logging configuration file when you start the WebLogic Server domain.

```
startWeblogic.sh -Djava.util.logging.config.file=logging.properties
```

Tip: If you specify a relative path, the base directory is the domain home - not the directory where startWeblogic.sh is located

Other configurations relevant to the WebLogic Server Security Module are similar to those defined in [Section 13.8.1.1.1, "Configuring Logging for a Java Security Module."](#)

13.8.1.2 Searching Logs to Debug Authorization Policies

The following sections explain how to search for information recorded to the logging file. They include the commands to be run and, in many sections, sample output.

- [Section 13.8.1.2.1, "Searching for PEP Request Information"](#)
- [Section 13.8.1.2.2, "Searching Against DebugStore Output"](#)
- [Section 13.8.1.2.3, "Searching for Security Module Cache Configuration Parameters"](#)

- Section 13.8.1.2.4, "Searching for Principals"
- Section 13.8.1.2.5, "Searching for Resources and Actions"
- Section 13.8.1.2.6, "Searching for the Value of an Attribute"
- Section 13.8.1.2.7, "Searching for an Authorization Decision"
- Section 13.8.1.2.8, "Searching for the Value of an Obligation"
- Section 13.8.1.2.9, "Searching for Static Application Roles"

13.8.1.2.1 Searching for PEP Request Information Run the following command against the logging file to output PEP Request related information (including the Authentic Identity, the Runtime Resource, the Runtime Action and the Application Context).

```
grep "PepRequestImpl"
```

13.8.1.2.2 Searching Against DebugStore Output Example 13–18 is sample output illustrating what you might find in a log file when the DebugStore logger is enabled. The output includes the name of the Application, the requested Resource, Action, Subject and policies that were evaluated.

Example 13–18 DebugStore Sample Logging Output

```
===== Start Of Policy Evaluation Info =====
Application: Library
Requested Resource Type: LibraryResource
Requested Resource: books/CrimeAndPunishment
Requested Resource Present: false
Requested Action: borrow
Request Subject Principals:
    class weblogic.security.principal.WLSUserImpl:John
Effective Roles Granted: [authenticated-role, Member, PrivilegedMember]
Role-Mapping Policies:
    1.Policy Name: GrantPrivilegedMemberPolicy
    Matched Policy Principals:
        class weblogic.security.principal.WLSUserImpl:John
    Policy Principals Semantics: OR
    Policy Roles: [PrivilegedMember]
    Matched Policy Resources: NONE
    Policy Evaluation Result: NOT_APPLICABLE
    Policy Rules:
        Rule Name: GrantPrivilegedMemberRule
        Rule Effect: GRANT
        Rule Condition: (MembershipLength >= 5)
        Evaluated Rule Attributes and Functions:
            MembershipLength(Dynamic, Integer) = 4
            Rule Evaluation Result: NOT_APPLICABLE
    2.Policy Name: DenyMemberPolicy
    Matched Policy Principals:
        class weblogic.security.principal.WLSUserImpl:John
    Policy Principals Semantics: OR
    Policy Roles: [Member]
    Matched Policy Resources: [.*]
    Policy Evaluation Result: NOT_APPLICABLE
    Policy Rules:
        Rule Name: DenyMemberRule
        Rule Effect: DENY
        Rule Condition: (MemberState = MA)
        Evaluated Rule Attributes and Functions:
```

```

MemberState(Dynamic, String) = CA
Rule Evaluation Result: NOT_APPLICABLE

Static Role Grants:
Principal= class oracle.security.jps.service.policystore.ApplicationRole:
Member, Roles= [PrivilegedMember]
Principal= class weblogic.security.principal.WLSUserImpl:John,
Roles= [Member]

Denied Static Role Grants: NONE

Authorization Policies:
1.Policy Name: DenyBorrowLibResourcesPolicy
Matched Policy Principals:
class oracle.security.jps.service.policystore.ApplicationRole:Member
class weblogic.security.principal.WLSUserImpl:John
Policy Principals Semantics: AND
Matched Policy Resource-Actions:
Resource = books/.*, Action = borrow
Policy Obligations: NONE
Policy Evaluation Result: NOT_APPLICABLE
Policy Rules:
Rule Name: DenyBorrowLibResourcesRule
Rule Effect: DENY
Rule Condition: (NumBorrowedBooks >= 6)
Evaluated Rule Attributes and Functions:
NumBorrowedBooks(Dynamic, Integer) = 2
Rule Evaluation Result: NOT_APPLICABLE

2.Policy Name: GrantBorrowLibResourcesPolicy
Matched Policy Principals:
class oracle.security.jps.service.policystore.ApplicationRole:Member
Policy Principals Semantics: OR
Matched Policy Resource-Actions:
Resource = .*books.*, Action = ANY
Resource = .*, Action = borrow
Policy Obligations: NONE
Policy Evaluation Result: GRANT
Policy Rules:
Rule Name: GrantBorrowLibResourcesRule
Rule Effect: GRANT
Rule Condition: ((NumBorrowedBooks < 4) && (age() >= 12))
Evaluated Rule Attributes and Functions:
NumBorrowedBooks(Dynamic, Integer) = 2
age(Function, Integer) = 24
Rule Evaluation Result: GRANT
===== End Of Policy Evaluation Info =====

```

13.8.1.2.3 Searching for Security Module Cache Configuration Parameters Run the following command against the logging file to output the cache configuration parameters for a particular Security Module.

```
grep "AuthorizationDecisionCacheTTL"
```

The following properties may be returned for this search. If a property does not appear in the log, it is not specified in `jps-config.xml`. In cases like this, the default value of the property is used.

- `AuthorizationDecisionCacheTTL` defines the time-to-live (in seconds) for the Authorization Decision cache. The default value is 60.
- `AuthorizationDecisionCacheEvictionPercentage` defines the percentage of authorization decisions to drop when the Authorization Decision cache has reached maximum capacity. The default value is 10.
- `AuthorizationDecisionCacheEvictionCapacity` defines the number used to evict the Authorization Decision cache if the decision cache size reaches this size. The default value is 500.
- `AuthorizationDecisionCacheEnabled` specifies whether the Authorization Decision cache is enabled. The default value is `true`.

Example 13–19 illustrates output for this search.

Example 13–19 Sample Output for Cache Configuration Parameters Search

```
oracle.security.jps.az.internal.runtime.service.AbstractPDPService
```

```
FINE: properties : {
oracle.security.jps.pdp.AuthorizationDecisionCacheTTL=60,
oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage=10,
oracle.securirty.jps.pdp.AuthorizationDecisionCacheEvictionCapacity=1000,
oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled=true}
```

13.8.1.2.4 Searching for Principals Run the following command against the logging file to output the names of Principals that have been received by Oracle Entitlements Server in the form of an authorization request.

```
grep "Principal:"
```

Example 13–20 illustrates the output for a Principal search.

Example 13–20 Sample Output for Principal Search

```
com.bea.security.providers.authorization.asi.AuthorizationProviderImpl
isAccessAllowed
```

```
FINE:subject: Subject:
Principal: John
Principal: Employee
Principal: Administrator
Principal: Principal Developer
```

13.8.1.2.5 Searching for Resources and Actions Run the following command against the logging file to output the Resources and Actions that have been received by Oracle Entitlements Server in the form of an authorization request.

```
grep "Resource:"
```

Example 13–21 illustrates how the information is returned. The defined values are the name of the policy object.

- Application = Lib
- Resource Type = libraryresourcetype
- Resource = Book
- Action = borrow

Example 13–21 Sample Output for Resource and Action Search

```
com.bea.security.providers.authorization.asi.AuthorizationProviderImpl
isAccessAllowed
```

```
FINE: Resource: resource=Lib/libraryresourcetype/Book, action=borrow
```

13.8.1.2.6 Searching for the Value of an Attribute Run the following command against the logging file to output the value of an attribute that has been received by Oracle Entitlements Server in the form of an authorization request.

```
grep "<name-of-the-attribute>:"
EXAMPLE: grep "NumberOfBorrowedBooksAttribute:"
```

[Example 13–22](#) illustrates the returned information where the name of the attribute is `NumberOfBorrowedBooksAttribute` and the value is 2.

Example 13–22 Sample Output for the Value of an Attribute Search

```
com.bea.security.providers.authorization.asi.ARME.evaluator.EvalSession logDebug
FINE: getAttributeInternal: name: NumberOfBorrowedBooksAttribute; value: 2;
type: 3
```

13.8.1.2.7 Searching for an Authorization Decision Run the following command against the logging file to retrieve an authorization decision that has been stored.

```
grep "AccessResultLogger"
```

[Example 13–23](#) illustrates the returned information and confirm that the authorization decision was affirmative.

Example 13–23 Sample Output for Authorization Decision Search

```
com.bea.security.providers.authorization.asi.AccessResultLogger log
FINE: Subject Subject:
Principal: John
Principal: Employee
Principal: Administrator
Principal: Principal Developer
privilege borrow resource //app/policy/Lib/Book result PERMIT
```

13.8.1.2.8 Searching for the Value of an Obligation On a UNIX system, run the following command against the logging file to output the value of a specific obligation: `grep <string_to_find> <filename>`.

For example,

```
grep "adding response attribute:" | grep "obligations"
```

[Example 13–24](#) illustrates the returned information indicating that the obligation (named `DenyObligation`) denies the request when the amount of library books the Principal currently has checked out is more than three; in this case, the Principal has five books checked out.

Example 13–24 Sample Output for Obligation Value Search

```
com.bea.security.providers.authorization.asi.AuthorizationProviderImpl
ARMEisAccessAllowed
```

```
FINE: adding response attribute: namespace=oracle.security.oes.authorization.
      name=obligations value={DenyObligation=
      { reason_part1=Too many borrowed books (max=3), reason_part2=5, }}
```

13.8.1.2.9 Searching for Static Application Roles Run the following command against the logging file to output the names of Application Roles granted statically.

```
grep "AbstractRoleManager" | grep "getGrantedStaticAppRoles"
```

Example 13–25 illustrates how two static roles are added to the list of principals: an authenticated-role – build-in role and Reader, an Application Role defined in the Application named Library.

Example 13–25 Sample Output for Static Role Search

```
oracle.security.jps.az.internal.runtime.entitymanager.AbstractRoleManager
getGrantedStaticAppRoles(Set)
FINER: RETURN [authenticated-role,
ApplicationRoleLibrary/Readeruname:
cn=Writer,cn=Roles,cn=Lib,cn=akapisni_dwps1_
view1.atzsrq,cn=JPSTextContext,cn=jpsTestNode,guid:
411EBF807CD411E0BF887FB1A0F3878F]
```

13.8.2 Enabling Debugging Using Methods

`isAccessAllowed_Debug` and `getRoles_Debug` are the methods that can be used in your code to return debugging information. `DebugInfo` is the object returned by the `isAccessAllowed_Debug` and `getRoles_Debug` calls. The following information has to be provided to the consumers of the policy debug feature (including the Policy Simulation tool) when overloading these methods:

- Roles granted to the requesting subject
- Roles denied the requesting subject
- Effective roles granted to the requesting subject
- Role Mapping and Authorization Policies that match the requesting subject(s), Resource Type, Resource and action (when applicable). Each policy must contain a name, a principal (that matches the user or role subject), a Resource or Resource Expression (that matches the input resource), action or role (depending on the policy type), policy rule (including a rule name, a GRANT or DENY effect, a string representation of the Condition, evaluated attributes and their values (including dynamic, function, and Resource Types) and a rule evaluation result (Grant, Deny, Not Applicable).
- Policy evaluation result (Grant, Deny, Not Applicable)
- Obligations (for Authorization Policies only)

See the *Oracle Fusion Middleware Management Java API Reference for Oracle Entitlements Server* for more details.

13.8.3 Debugging Policy Distribution

The Policy Distribution Component uses the policy management `Logger` interface. To enable debugging for the Policy Distribution Component, change the logging level of the `oracle.jps.policymgmt.level` property in the logging configuration file to `FINEST`. The procedure is documented in [Section 13.8.1.1, "Configuring Logging for](#)

Debugging. The following should also be verified when debugging policy distribution.

- Check that the Security Module distribution mode parameter, `oracle.security.jps.runtime.pd.client.policyDistributionMode`, is correctly defined. See [Appendix A.1, "Policy Distribution Configuration."](#)
- When distributing policies in controlled-push or controlled-pull mode, check for the presence of a local cache file. The local cache directory is defined as the value of the `oracle.security.jps.runtime.pd.client.localpolicy.work_folder` parameter. Within this directory, see sub directories for each policy's `XML_CACHE_FILE` such as `policyA/` and `policyB/`. Ensure that the time stamp in the cache file matches the time when the last distribution was initiated. See [Appendix A.1, "Policy Distribution Configuration."](#)
- When distributing policies in controlled-push mode, ensure that the instance of the Security Module to which the policies are being distributed is displayed on the Application's Policy Distribution page, and that it is synchronized.
- Verify that the correct policies are being evaluated by debugging the Security Module side.

Configuring a Disaster Recovery Solution

The Oracle Fusion Middleware Disaster Recovery solution for enterprise deployments makes use of storage replication technology using Oracle Data Guard. This technology supports components from various Oracle product suites, including Oracle Entitlements Server installed as a stand-alone distribution. This chapter describes how to set up for Oracle Entitlements Server to use Oracle Data Guard to synchronize data for disaster recovery in a multi-site deployment.

This chapter includes the following sections:

- [Section 14.1, "Overview of a Multi-Site Deployment"](#)
- [Section 14.2, "Multi-Site Deployment Topology"](#)
- [Section 14.3, "Task Roadmap"](#)
- [Section 14.4, "Prerequisites"](#)
- [Section 14.5, "Configuring Disaster Recovery for Oracle Entitlements Server"](#)

Note: Review the information about the Oracle Fusion Middleware Disaster Recovery solution in *Oracle Fusion Middleware Disaster Recovery Guide* before setting up a disaster recovery solution for Oracle Entitlements Server in a multi-site deployment.

14.1 Overview of a Multi-Site Deployment

Disaster protection for Oracle databases is provided through Oracle Data Guard. In a multi-site deployment, you install and configure a database for both a primary site and a standby site. In this release, Oracle Entitlements Server supports Oracle Data Guard as the high availability solution for the database service. Oracle Data Guard provides the capability to create and maintain one or more synchronized *replicas* (standby databases) of a production database (primary database). An Oracle Data Guard standby database is open read-only while and Oracle Data Guard primary database is both readable and writable. For information on recommendations for Oracle Data Guard configuration, see Section 2.5, "Recommendations for Oracle Identity Management" in *Oracle Fusion Middleware Disaster Recovery Guide*.

In a multi-site deployment, the Oracle Entitlements Server Administration Server will configure the Oracle Data Guard primary database in its policy store to support MAPI operations. The Oracle Entitlements Server Security Modules will configure either the primary database or one of the standby databases in their policy store for policy distribution.

Oracle Entitlements Server Administration Servers are deployed on a read-only Oracle Data Guard standby database in order to provide policy query services. In the case of

an Oracle Data Guard database role transition (where a standby database becomes the new primary database), the Oracle Entitlements Server Administration Server can provide management services on the new primary database without restarting WebLogic Server.

An Oracle Entitlements Server multi-site deployment includes:

- **Oracle Entitlements Server Administration Console:** A single master for policy management across data centers.
- **Security Modules:** The SMs connect to the
 - Local site database (Master or Slave) for reading data.
 - Master site database (Master) for writing data.
- **Policy Data Replication:** The mode of data replication.

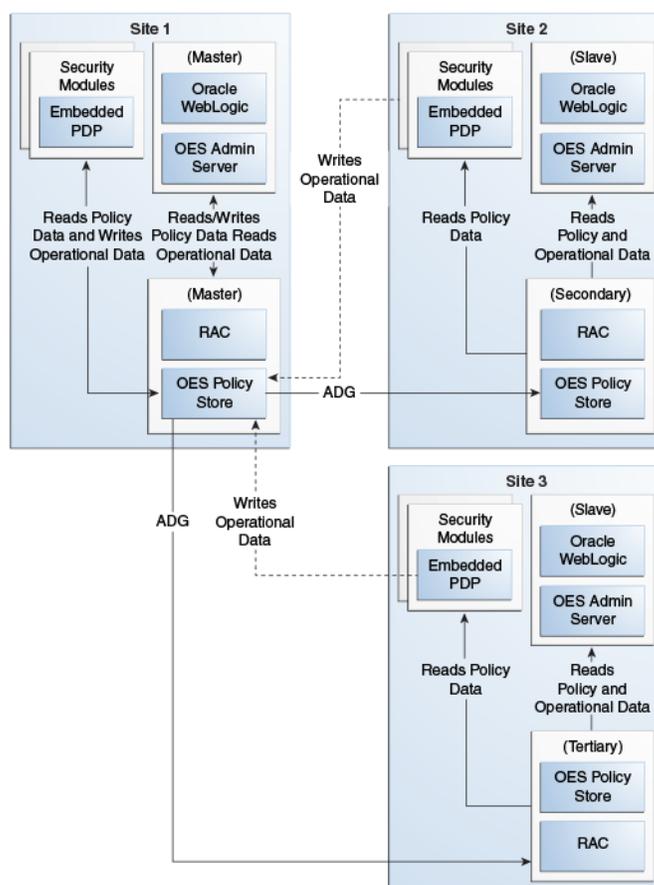
14.2 Multi-Site Deployment Topology

In this release, the following configuration is required:

- One site is acting as Master at any time. All the write operations are against the policy store configured for the current Master site.
- All the Security Modules are configured in controlled-pull mode. Non-controlled and controlled push modes are not supported.
- A policy store configured in mixed mode is not supported.
- The Oracle Entitlements Server Administration Console in the IDM domain cannot leverage multi-site functionality
- Oracle Entitlements Server is installed as a stand-alone distribution.

Figure 14–1 illustrates the relationship between the Oracle Entitlements Server components when configured in a multi-site deployment:

Figure 14–1 Multi-Site Deployment Topology



As seen in the figure, when in a multi-site deployment the following relationships exist:

- Policy Distribution:** Security Modules are configured in controlled-pull mode on all the sites. The snapshot is generated by the Administration Server at the Master site and replicated to the secondary and tertiary sites using Oracle Data Guard. The PDP on the secondary and tertiary sites retrieve the snapshot from the local policy store.
- Configuration:** PDP are configured with multiple JDBC URL's. The primary JDBC URL is configured to the local policy store. In an event of failure to connect to the local Policy Store, a connection attempt to the secondary JDBC URL is made. This ensures that the policy store is accessible in an event of a failure.
- SM ConfigUI:** Can be used to configure the JDBC URLs that are required to support failover functionality.

14.3 Task Roadmap

Table 14–1 lists the high-level tasks for configuring Oracle Entitlements Server to use Oracle Data Guard to synchronize data for disaster recovery in a multi-site deployment.

Table 14–1 Configuration Flow for Disaster Recovery Solution

| No. | Task | Information |
|-----|--|---|
| 1 | Review the information about the Oracle Fusion Middleware Disaster Recovery solution | <i>Oracle Fusion Middleware Disaster Recovery Guide</i> |
| 2 | Ensure you have complied with the prerequisites. | Section 14.4, "Prerequisites" |

Configuring Oracle Data Guard

| | | |
|----|--|---|
| 3 | Configure the Primary Server site | <ul style="list-style-type: none"> ■ Section 14.5.1, "Setting Up the Primary Server" ■ "Setting Up and Managing Disaster Recovery Sites" chapter in <i>Oracle Fusion Middleware Disaster Recovery Guide</i> |
| 4 | Configure the Standby Server site | <ul style="list-style-type: none"> ■ Section 14.5.2, "Setting Up the Standby Server (Duplicate)" ■ "Setting Up and Managing Disaster Recovery Sites" chapter in <i>Oracle Fusion Middleware Disaster Recovery Guide</i> |
| 5 | Force a switchover from Primary Server to Standby Server to test log file transfer | Section 14.5.3, "Test Log Transfer" |
| 6 | Configure Oracle Data Guard Broker | <ul style="list-style-type: none"> ■ Section 14.5.4, "Configuring the Oracle Data Guard Broker" ■ "Setting Up and Managing Disaster Recovery Sites" chapter in <i>Oracle Fusion Middleware Disaster Recovery Guide</i> |
| 7 | Test manual and switchover failover between Primary Server and Standby Server | Section 14.5.5, "Testing Failover and Switchover" |
| 8 | Configure a virtual device for Oracle ASM | Section 14.5.6, "Configuring a Virtual Device for Oracle ASM" |
| 9 | If necessary, install Oracle Grid Infrastructure for a Standalone Server | <ul style="list-style-type: none"> ■ Section 14.5.7, "Installing Oracle Grid Infrastructure for a Standalone Server" ■ <i>Oracle Database Installation Guide</i> |
| 10 | Configure Oracle Restart | Section 14.5.8, "Configuring Oracle Restart" |

Configuring Oracle Entitlements Server

| | | |
|----|---|---|
| 11 | Create an OPSS database schema using RCU for Oracle Entitlements Server | <ul style="list-style-type: none"> ■ Section 14.5.9, "Installing OPSS Schema" ■ "Database Requirements" section in <i>Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management</i> |
|----|---|---|

Table 14–1 (Cont.) Configuration Flow for Disaster Recovery Solution

| No. | Task | Information |
|-----|---|--|
| 12 | Install Oracle Entitlements Server Administration Console on the Primary Server | <ul style="list-style-type: none"> ■ Section 14.5.10, "Installing the Primary Administration Server" ■ "Installing and Configuring Oracle Entitlements Server" chapter in <i>Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management</i> |
| 13 | Install Oracle Entitlements Server Administration Console on the Standby Server | <ul style="list-style-type: none"> ■ Section 14.5.11, "Installing the Secondary Administration Server" ■ "Installing and Configuring Oracle Entitlements Server" chapter in <i>Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management</i> |
| 14 | Configure the Security Module for multi-site deployment | <ul style="list-style-type: none"> ■ Section 14.5.12, "Configuring the Security Module" ■ "Configuring Oracle Entitlements Server Client" section in <i>Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management</i> |

14.4 Prerequisites

1. Two servers with Oracle database installed. 11gR2 (11.1.2) is the minimum version required in order to provide Oracle Data Guard support.

In the following examples, the Primary Site server name is `primary_host`. The Standby Site server name is `standby_host`.

2. The Primary Site server (`primary_host`) has a running instance. In the examples, the database name and unique name are both `db11g`.
3. The Standby Site server (`standby_host`) has a software only installation. In the examples, the database name is `db11g` and the database unique name is `db11g_stby`.

The `DB_NAME` of the standby database is the same as that of the primary, but it must have a different `DB_UNIQUE_NAME` value.

4. The `primary_host` and `standby_host` both have the same `ORACLE_HOME` directory and structure.

This is not a limitation but is recommended to simplify installation.

5. 11gR2 (11.1.2) Oracle Grid Infrastructure for standalone server is installed on both `primary_host` and `standby_host`.

Both Oracle Restart and Oracle Automatic Storage Management (Oracle ASM) are required and will be configured. They are both included when Oracle Grid Infrastructure for a standalone server is installed.

14.5 Configuring Disaster Recovery for Oracle Entitlements Server

This section contains the following topics:

- [Section 14.5.1, "Setting Up the Primary Server"](#)

- Section 14.5.2, "Setting Up the Standby Server (Duplicate)"
- Section 14.5.3, "Test Log Transfer"
- Section 14.5.4, "Configuring the Oracle Data Guard Broker"
- Section 14.5.5, "Testing Failover and Switchover"
- Section 14.5.6, "Configuring a Virtual Device for Oracle ASM"
- Section 14.5.7, "Installing Oracle Grid Infrastructure for a Standalone Server"
- Section 14.5.8, "Configuring Oracle Restart"
- Section 14.5.9, "Installing OPSS Schema"
- Section 14.5.10, "Installing the Primary Administration Server"
- Section 14.5.11, "Installing the Secondary Administration Server"
- Section 14.5.12, "Configuring the Security Module"

14.5.1 Setting Up the Primary Server

To install the database that will serve as the Primary Server:

1. Configure forced logging. Check the primary database is in archive log mode. If it is in noarchive log mode, switch to archive log mode and enable forced logging. For example:

```
sqlplus sys/welcome1 as sysdba
select log_mode from v$database;
shutdown immediate;
startup mount;
alter database archive log;
alter database open;
alter database force logging;
```

2. Check the setting for the DB_NAME and DB_UNIQUE_NAME parameters. In this example, they are both set to db11g on the primary database. The DB_NAME of the standby database is the same as that of the primary, but it must have a different DB_UNIQUE_NAME value. Set the initialization parameters to redo log apply. For example:

```
show parameter db_name;
show parameter db_unique_name;
ALTER SYSTEM SET LOG_ARCHIVE_CONFIG='DG_CONFIG=(db11g,db11g_stby)';
ALTER SYSTEM SET LOG_ARCHIVE_DEST_2='SERVICE=db11g_stby NOAFFIRM ASYNC VALID_
FOR=(ONLINE_LOGFILES,PRIMARY_ROLE) DB_UNIQUE_NAME=db11g_stby';
ALTER SYSTEM SET LOG_ARCHIVE_DEST_STATE_2=ENABLE;
ALTER SYSTEM SET LOG_ARCHIVE_FORMAT='%t_%s_%r.arc' SCOPE=SPFILE;
ALTER SYSTEM SET LOG_ARCHIVE_MAX_PROCESSES=5;
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE SCOPE=SPFILE;
ALTER SYSTEM SET FAL_SERVER=db11g_stby;
ALTER SYSTEM SET STANDBY_FILE_MANAGEMENT=AUTO;
```

3. Shut down the database. For example:

```
shutdown immediate;
startup mount;
```

4. Provide values for the primary and standby databases in the \$ORACLE_HOME/network/admin/tnsnames.ora files. They are needed on both servers. For example:

```

db11g =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = primary_host)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = db11g.example.com)
    )
  )

db11g_stby =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = standby_host)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = db11g.example.com)
    )
  )

```

5. Set the following values for listener.ora on the primary server:

```

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = db11g_DGMGRL.example.com)
      (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
      (SID_NAME = db11g)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = db11g_DGB.example.com)
      (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
      (SID_NAME = db11g)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = db11g.example.com)
      (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
      (SID_NAME = DB11G)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = primary.example.com)(PORT =
1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )

ADR_BASE_LISTENER = /scratch/example_user/app/example_user

ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER=ON # line added by Agent

```

6. Create a control file and a parameter file for the standby database. Amend the PFILE to make the entries relevant for the standby database. For example:

```
ALTER DATABASE CREATE STANDBY CONTROLFILE AS '/tmp/db11g_stby.ctl';
CREATE PFILE='/tmp/initdb11g_stby.ora' FROM SPFILE;

*.db_unique_name='db11g_stby'
*.fal_server='db11g'
*.log_archive_dest_2='SERVICE=db11g ASYNC VALID_FOR=(ONLINE_LOGFILES,PRIMARY_
ROLE) DB_UNIQUE_NAME=db11g'
```

14.5.2 Setting Up the Standby Server (Duplicate)

Before setting up the standby server, make sure the Oracle Database is installed on standby_host with the "software only installation" option.

To install the database that will serve as the Standby Server (duplicate):

1. Create the necessary directories on the Standby Server and copy the files from the Primary Server (primary_host) to the Standby Server (standby_host). In this example, the database name is db11g and database unique name is db11g_stby:

```
$ mkdir -p /scratch/example_user/app/example_user/oradata/db11g
$ mkdir -p /scratch/example_user/app/example_user/fast_recovery_area/db11g
```

Note: Here fast_recovery_area may be flash_recovery_area depending on the Oracle Database version. You should check the file structure on the primary_host to see whether the folder is called fast_recovery_area or flash_recovery_area.

```
$ mkdir -p /scratch/example_user/app/example_user/admin/db11g/adump
$ # Standby controlfile to all locations.
$ scp example_user@primary_host:/tmp/db11g_stby.ctl /scratch/example_
user/app/example_user/oradata/db11g/control01.ctl
$ cp /scratch/example_user/app/example_user/oradata/db11g/control01.ctl
/scratch/example_user/app/example_user/fast_recovery_area/db11g/control02.ctl
```

```
$ # Parameter file.
$ scp example_user@primary_host:/tmp/initdb11g_stby.ora /tmp/initdb11g_
stby.ora
```

```
$ # Remote login password file.
$ scp example_user@primary_host:$ORACLE_HOME/dbs/orapwdb11g $ORACLE_HOME/dbs
```

2. Edit the listener configuration file listener.ora to have the following entries:

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = db11g.example.com)
      (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
      (SID_NAME = db11g)
    )
    (SID_DESC =
      (GLOBAL_DBNAME = db11g_stby_DGMGRL.example.com)
      (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
      (SID_NAME = db11g)
```

```

)
(SID_DESC =
  (GLOBAL_DBNAME = db11g_stby_DGB.example.com)
  (ORACLE_HOME = /scratch/example_user/app/example_
user/product/11.2.0/dbhome_1)
  (SID_NAME = db11g)
)
)

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = standby_host.example.com)(PORT
= 1521))
    )
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )

ADR_BASE_LISTENER = /scratch/example_user/app/example_user
ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER=ON # line added by Agent

```

3. Verify the listener is started on the Standby Server.

```
$ lsnrctl start
```

4. Create standby Redo logs on the primary server to ensure the primary database is configured for switchover. For example:

```

ALTER DATABASE ADD STANDBY LOGFILE ('/scratch/example_user/app/example_
user/oradata/db11g/standby_redo01.log') SIZE 50M;
ALTER DATABASE ADD STANDBY LOGFILE ('/scratch/example_user/app/example_
user/oradata/db11g/standby_redo02.log') SIZE 50M;
ALTER DATABASE ADD STANDBY LOGFILE ('/scratch/example_user/app/example_
user/oradata/db11g/standby_redo03.log') SIZE 50M;
ALTER DATABASE ADD STANDBY LOGFILE ('/scratch/example_user/app/example_
user/oradata/db11g/standby_redo04.log') SIZE 50M;

```

5. Create standby using DUPLICATE command:

a. Start the auxiliary instance on the standby server, using the temporary init.ora file. For example:

```

$ export ORACLE_SID=db11g
$ sqlplus / as sysdba

SQL> STARTUP NOMOUNT PFILE='/tmp/initdb11g_stby.ora';

```

b. Connect to RMAN, specifying a full connect string for both the TARGET and AUXILIARY instances. Do not use OS authentication.

```
$ rman TARGET sys/password@db11g AUXILIARY sys/password@db11g_stby
```

c. Execute the following DUPLICATE command.

```

DUPLICATE TARGET DATABASE
FOR STANDBY
FROM ACTIVE DATABASE
DORECOVER
SPFILE
SET db_unique_name='db11g_stby' COMMENT 'Is standby'

```

```
SET LOG_ARCHIVE_DEST_2='SERVICE=db11g ASYNC VALID_FOR=(ONLINE_
LOGFILES,PRIMARY_ROLE) DB_UNIQUE_NAME=db11g'
SET FAL_SERVER='db11g' COMMENT 'Is primary'
NOFILENAMECHECK;
```

6. Restart.

```
SHUTDOWN IMMEDIATE;
STARTUP MOUNT;
ALTER DATABASE OPEN READ ONLY;
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE DISCONNECT FROM SESSION;
select status,instance_name,database_role,open_mode from
v$database,v$instance;
```

14.5.3 Test Log Transfer

Force a switchover from the Primary Server to the Standby Server in order to verify the log file transfer between the two site.

To verify the log files transfer on the two servers:

1. On Primary Server, check the latest archived redo log and force a log switch. For example:

```
ALTER SESSION SET nls_date_format='DD-MON-YYYY HH24:MI:SS';

SELECT sequence#, first_time, next_time
FROM v$archived_log
ORDER BY sequence#;

ALTER SYSTEM SWITCH LOGFILE;
```

2. On the Standby Server, verify the new archived redo log has arrived and has been applied. For example:

```
ALTER SESSION SET nls_date_format='DD-MON-YYYY HH24:MI:SS';

SELECT sequence#, first_time, next_time, applied
FROM v$archived_log
ORDER BY sequence#;
```

14.5.4 Configuring the Oracle Data Guard Broker

To configure the Oracle Data Guard broker:

1. Start DMON background process on primary and standby database.

```
connect sys/welcome1@db11g as sysdba
alter system set dg_broker_start=true;

connect sys/welcome1@db11g_stby as sysdba
alter system set dg_broker_start=true;
```

2. Call Oracle Data Guard Manager Linemode and configure. For example:

```
dgmgrl

connect sys/welcome1@db11g
create configuration myconfig as primary database is db11g connect identifier
```

```

is db11g;
add database db11g_stby as connect identifier is db11g_stby maintained as
physical;
enable configuration;
show configuration;

```

3. Change to MA protection mode.

```

edit database db11g set property LogXptMode=SYNC;
edit database db11g_stby set property LogXptMode=SYNC;
edit configuration set protection mode as maxavailability;

```

Fast-start failover allows the broker to automatically fail over to a previously chosen standby database in the event of loss of the primary database. Fast-start failover quickly and reliably fails over the target standby database to the primary database role, without requiring you to perform any manual steps to invoke the failover. Fast-start failover can be used only in a broker configuration and can be configured only through DGMGRL or Enterprise Manager.

To enable Fast Start Failover:

1. Enable Fast Start Failover.

```

EDIT DATABASE db11g SET PROPERTY FastStartFailoverTarget = db11g_stby;
EDIT DATABASE db11g_stby SET PROPERTY FastStartFailoverTarget = db11g;
EDIT CONFIGURATION SET PROPERTY FastStartFailoverThreshold = 30;

```

Note: Run the Edit command in the DGMGRL console. Run following SQL in SQL*Plus on both the primary server and standby servers.

```

SQL> select flashback_on from v$database;
SQL> alter database flashback on;

```

2. Start the Observer on another host.

```

DGMGRL> connect sys/welcome1@db11g_stby
DGMGRL> START OBSERVER;
Turn on flashback by sqlplus

```

3. Run the following command in the DGMGRL console.

```

ENABLE FAST_START FAILOVER;\

```

14.5.5 Testing Failover and Switchover

To test the manual switchover and failover:

1. Test switchover and failover as follows.

a. To test switchover:

```

dgmgrl>connect sys/welcome1@db11g

dgmgrl>switchover to db11g_stby;

```

b. To test failover:

```

dgmgrl>connect sys/oracle@db11g_stby

```

```
dgmgrl>failover to db11g_stby;
```

2. Test Fast Start Failover by simulating a failure. For example:

a. Shutdown the current primary database to simulate a failure.

```
SQL> connect sys/welcome1@db11g as sysdba
```

```
SQL> shutdown abort
```

b. Wait 20 seconds and verify the observer has initiated a failover.

After 20 seconds has lapsed, The observer has initiated a failover.

```
00:37:13.65 Thursday, May 30, 2013
```

```
Initiating Fast-Start Failover to database "db11g_stby"...
```

```
Performing failover NOW, please wait...
```

```
Failover succeeded, new primary is "db11g_stby"
```

```
00:37:20.67 Thursday, May 30, 2013
```

c. Confirm that the new Primary Server is db11g_stby

```
DGMGRL> show configuration
```

14.5.6 Configuring a Virtual Device for Oracle ASM

A virtual device is required for Oracle ASM. Use the `losetup` command to create virtual devices in place of real disk device.

Login as root to create a virtual device for Oracle ASM, for example:

```
mkdir /scratch/example_user/asmdisks
chown example_user:dba /asmdisks
```

```
dd if=/dev/zero of=/scratch/example_user/asmdisks/_file_disk1 bs=1k count=100000
dd if=/dev/zero of=/scratch/example_user/asmdisks/_file_disk2 bs=1k count=100000
dd if=/dev/zero of=/scratch/example_user/asmdisks/_file_disk3 bs=1k count=100000
dd if=/dev/zero of=/scratch/example_user/asmdisks/_file_disk4 bs=1k count=100000
```

```
"/sbin/losetup /dev/loop1 /scratch/example_user/asmdisks/_file_disk1"
"/sbin/losetup /dev/loop2 /scratch/example_user/asmdisks/_file_disk2"
"/sbin/losetup /dev/loop3 /scratch/example_user/asmdisks/_file_disk3"
"/sbin/losetup /dev/loop4 /scratch/example_user/asmdisks/_file_disk4"
```

```
"/bin/raw /dev/raw/raw1 /dev/loop1"
"/bin/raw /dev/raw/raw2 /dev/loop2"
"/bin/raw /dev/raw/raw3 /dev/loop3"
"/bin/raw /dev/raw/raw4 /dev/loop4"
```

```
"chown example_user:dba /dev/raw/raw1"
"chown example_user:dba /dev/raw/raw2"
"chown example_user:dba /dev/raw/raw3"
"chown example_user:dba /dev/raw/raw4"
```

```
"chmod 660 /dev/raw/raw1"
```

```
"chmod 660 /dev/raw/raw2"
"chmod 660 /dev/raw/raw3"
"chmod 660 /dev/raw/raw4"
```

14.5.7 Installing Oracle Grid Infrastructure for a Standalone Server

Both Oracle Restart and Oracle Automatic Storage Management (Oracle ASM) are required and must be configured. They are both included with an Oracle Grid Infrastructure for a standalone server installation.

If you do not already have Oracle Grid Infrastructure for a standalone server installed on both `primary_host` and `standby_host`, follow instructions in *Oracle Database Installation Guide*.

14.5.8 Configuring Oracle Restart

If Oracle Restart is installed after Oracle database, the database components need to be registered to Oracle Restart using `srvctl` command. Before proceeding, install Grid Infrastructure 11gR2 for the standalone server (Oracle Restart) on both `primary_host` and `standby_host`.

Note: The following applies to restarting a service:

- The `distribution.example.com` service must be explicitly started with `SRVCTL START SERVICE` and stopped with `SRVCTL STOP SERVICE` on primary database to ensure its information is propagated using redo to physical standby. For example: `srvctl start service -d db11g_stby -s distribution.example.com`
 - Whenever a role change occurs after an Oracle Data Guard automatic or manual failover, always make sure that both the manage and distribution services are started and running on both the primary and standby servers. If they are not running, start the service.
-

To register the database components if Oracle Restart is installed after the database, perform the following steps on both the primary and standby servers:

1. Add the database, ensure `ORACLE_HOME` is set to the database home. For example:

```
srvctl add database -d db11g -o $ORACLE_HOME -r PRIMARY
srvctl add database -d db11g_stby -o $ORACLE_HOME -r PHYSICAL_STANDBY -s MOUNT
```

2. If the listener is started from the database home, add the listener by ensuring the `ORACLE_HOME` is set to database home.

```
srvctl add listener -o $ORACLE_HOME
```

3. Add the Oracle notification service (ONS/eONS) for Oracle Broker, ensure `ORACLE_HOME` is set to Oracle Grid Infrastructure home. For example:

```
srvctl add ons
srvctl enable ons
srvctl start ons
srvctl status ons

srvctl add eons
srvctl enable eons
srvctl start eons
```

```
srvctl status eons
```

By default ONS listening port for local client connections is 6100 and for connections from remote hosts is 6200

4. Add database service, ensure ORACLE_HOME is set to database home. For example:

- a. On the primary database:

```
srvctl add service -d db11g -s manage.example.com -l PRIMARY -y AUTOMATIC
-q FALSE -e NONE -m NONE -w 0 -z 0
srvctl add service -d db11g -s distribution.example.com -l PHYSICAL_
STANDBY,PRIMARY -y AUTOMATIC -q FALSE -e NONE -m NONE -w 0 -z 0
```

- b. On the standby database:

```
srvctl add service -d db11g_stby -s manage.example.com -l PRIMARY -y
AUTOMATIC -q FALSE -e NONE -m NONE -w 0 -z 0
srvctl add service -d db11g_stby -s distribution.example.com -l PHYSICAL_
STANDBY,PRIMARY -y AUTOMATIC -q FALSE -e NONE -m NONE -w 0 -z 0
```

5. After adding the services, restart the Oracle database:

```
shutdown immediate;
startup;
```

14.5.9 Installing OPSS Schema

Run Oracle Fusion Middleware Repository Creation Utility (RCU) against the primary database. After it is finished, the OPSS schema can be propagated to the standby database. For more information about using RCU, see "Database Requirements" section in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

14.5.10 Installing the Primary Administration Server

For information about installing Oracle Entitlements Server Administration Server, see "Installing and Configuring Oracle Entitlements Server" chapter in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Note the following when installing:

- When running the `config.sh` script to install a Weblogic domain, choose GridLink to create data source.
- When inputting listeners for GridLink data source, add primary database as the first listener.
- When running the `configureSecurityStore.py` script ensure `-m create` option is added to parameters. For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh MW_HOME/Oracle_
IDM1/common/tools/configureSecurityStore.py
-d /scratch/example_user/Oracle/Middleware/user_projects/domains/domainname/
-t DB_ORACLE -j cn=jpsroot -m create -p welcome1
```

- Edit the JPS configuration files to support HA failover mode operation as follows:

```
$MW_HOME/user_projects/domains/domainname/config/fmwconfig/jps-config.xml
```

The Gridlink JDBC URL configured for the data source property in `opss-jdbc.xml` is used by WebLogic Server for switching. Edit the `jps-config.xml` file to comment out the following property entries under `props.db.1`:

```
jdbc.url

jdbc.driver

bootstrap.security.principal.map

bootstrap.security.principal.key
```

Edit `$MW_HOME/user_`

`projects/domains/domainname/config/fmwconfig/jps-config-jse.xml`:

```
<property name="jdbc.url" value="jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD
_BALANCE = off) (FAILOVER = on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS =
(PROTOCOL = TCP)(HOST = primary.example.com)(PORT = 1521)))(CONNECT_DATA =
(SERVICE_NAME = manage.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS
= (PROTOCOL = TCP)(HOST = standby.example.com)(PORT = 1521)))(CONNECT_DATA =
(SERVICE_NAME = manage.example.com)))/">
```

Edit `$MW_HOME/user_`

`projects/domains/domainname/config/jdbc/opss-jdbc.xml`:

```
<url>jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER =
on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
primary.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME =
manage.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
TCP)(HOST = standby.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME
= manage.example.com)))/</url>
```

14.5.11 Installing the Secondary Administration Server

Install the secondary Oracle Entitlements Server Administration Server. Note the following when installing:

- Create a GridLink data source by following the steps in [Section 14.5.10, "Installing the Primary Administration Server"](#) with the following changes: use `distribution.example.com` instead of `manage.example.com`, and the first host is a standby database.

- Export EncryptionKey from primary domain. For example:

```
exportEncryptionKey(jpsConfigFile="/scratch/example_user/Oracle/Middleware/
user_
projects/domains/domainname/config/fmwconfig/jps-config.xml",keyFilePath="/net
/
standby_host/scratch/example_user/keydir",keyFilePassword="welcome1")
```

- When running the `configureSecurityStore.py` script ensure `-m join` option is added, and the farm name is set to the one used when installing the Primary Administration Server. For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh MW_HOME/Oracle_
IDM1/common/tools/configureSecurityStore.py
-d /scratch/example_user/Oracle/Middleware/
user_projects/domains/domainname/ -t DB_ORACLE -j cn=jpsroot -m join -f
domainname -p welcome1 -k /net/standby_host/scratch/example_user/keydir -w
welcome1 --create_diagnostic_data
```

- Edit the JPS configuration file to support HA failover mode operation. For example:

```
$MW_HOME/user_projects/domains/domainname/config/fmwconfig/jps-config.xml
```

The Gridlink JDBC URL configured for the data source property in `opss-jdbc.xml` is used by WebLogic Server for switching. Edit the `jps-config.xml` file to comment out the following property entries under `props.db.1`:

```
dbc.url
```

```
jdbc.driver
```

```
bootstrap.security.principal.map
```

```
bootstrap.security.principal.key
```

Edit `$MW_HOME/user_projects/domains/domainname/config/fmwconfig/jps-config-jse.xml`:

```
property name="jdbc.url" value="jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD
_BALANCE = off) (FAILOVER = on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS =
(PROTOCOL = TCP)(HOST = standby.example.com)(PORT = 1521)))(CONNECT_DATA =
(SERVICE_NAME = distribution.example.com)))(DESCRIPTION = (ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCP)(HOST = primary.example.com)(PORT =
1521)))(CONNECT_DATA = (SERVICE_NAME = distribution.example.com)))"/>
```

Edit `$MW_HOME/user_projects/domains/domainname/config/jdbc/opss-jdbc.xml`:

```
<url>jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER =
on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
standby.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME =
distribution.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS =
(PROTOCOL = TCP)(HOST = primary.example.com)(PORT = 1521)))(CONNECT_DATA =
(SERVICE_NAME = distribution.example.com)))</url>
```

- After installation, launch WebLogic Server Console to change the GridLink data source JDBC connection's first host to be the local `standby_host`.

14.5.12 Configuring the Security Module

When operating in a multi-site environment, Security Modules must be configured to be in controlled-pull mode.

To configure a security module, edit parameters about multi-site in the `smconfig.prp` file and then run `config.sh`. To do so, proceed as follows:

1. Edit the `smconfig.prp` file for the primary site to include entries similar to the following example. Note these differences from the `smconfig.prp` file for the standby site:
 - The `jdbc.url` property references the `SERVICE_NAME` as `manage.example.com`.
 - The first host in the URL is the primary host, then followed by the standby host.

```
jdbc.url=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off)
(FAILOVER = on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
TCP)(HOST = primary-host.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE
_NAME = manage.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS =
```

```
(PROTOCOL = TCP)(HOST = standby-host.example.com)(PORT = 1521)))(CONNECT_DATA
= (SERVICE_NAME = manage.example.com)))
```

2. Edit the smconfig.prp file on the standby site to include entries similar to the following example:

```
# Policy distribution mode.
oracle.security.jps.runtime.pd.client.policyDistributionMode=controlled-pull

# Policy Store URL for DB policy store
jdbc.url=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off)
(FAILOVER = on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
TCP)(HOST = standby-host.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE
_NAME = distribution.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS =
(PROTOCOL = TCP)(HOST = primary-host.example.com)(PORT = 1521)))(CONNECT_DATA
= (SERVICE_NAME = distribution.example.com))))

# Primary Policy Store URL for Mutli-site Deployment
oracle.security.jps.runtime.pd.client.multisite.primaryJdbcUrl=jdbc:oracle:th
in:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER = on) (DESCRIPTION =
(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
primary-host.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE_NAME =
manage.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
TCP)(HOST = standby-host.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE
_NAME = manage.example.com))))

# Oracle Notification Servers for Mutli-site Deployment
oracle.security.jps.runtime.pd.client.multisite.onserver=nodes=primary-host.
example.com:6200,standby-host.example.com:6200
```

3. Configure the domain (pull mode) using config.sh command with -multisite parameter to enable the multi-site configuration.

■ For a WebLogic Server domain:

```
config.sh -smType wls -smConfigId wlsPullDomain -serverLocation
<MiddlewareHome>/wlserver10.3 -multisite
```

■ For a Tomcat domain:

```
config.sh -smType tomcat -smConfigId tomcatSmPull -serverLocation
/scratch/oesuser/tomcat7/ -multisite
```

4. When prompted for primary JdbcURL, provide information similar to the following example:

```
jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER =
on)(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
primary-host.example.com)(PORT = 1522)))(CONNECT_DATA = (SERVICE_NAME =
manage.example.com)))(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
TCP)(HOST = standby-host.example.com)(PORT = 1521)))(CONNECT_DATA = (SERVICE
_NAME = manage.example.com))))
```

5. When prompted for Onserver, provide information similar to the following example:

```
nodes=primary-host.example.com:6200,standby-host.example.com:6200
```

Configuring an Oracle RAC Disaster Recovery Solution

The Oracle Fusion Middleware Disaster Recovery solution for enterprise deployments makes use of storage replication technology using Oracle Data Guard. An Oracle Data Guard configuration can consist of any combination of single-instance and Oracle Real Application Clusters (Oracle RAC) multiple-instance databases.

This chapter describes how to set up Oracle Entitlements Server to use Oracle Data Guard with Oracle RAC databases to synchronize data for disaster recovery in a multi-site deployment.

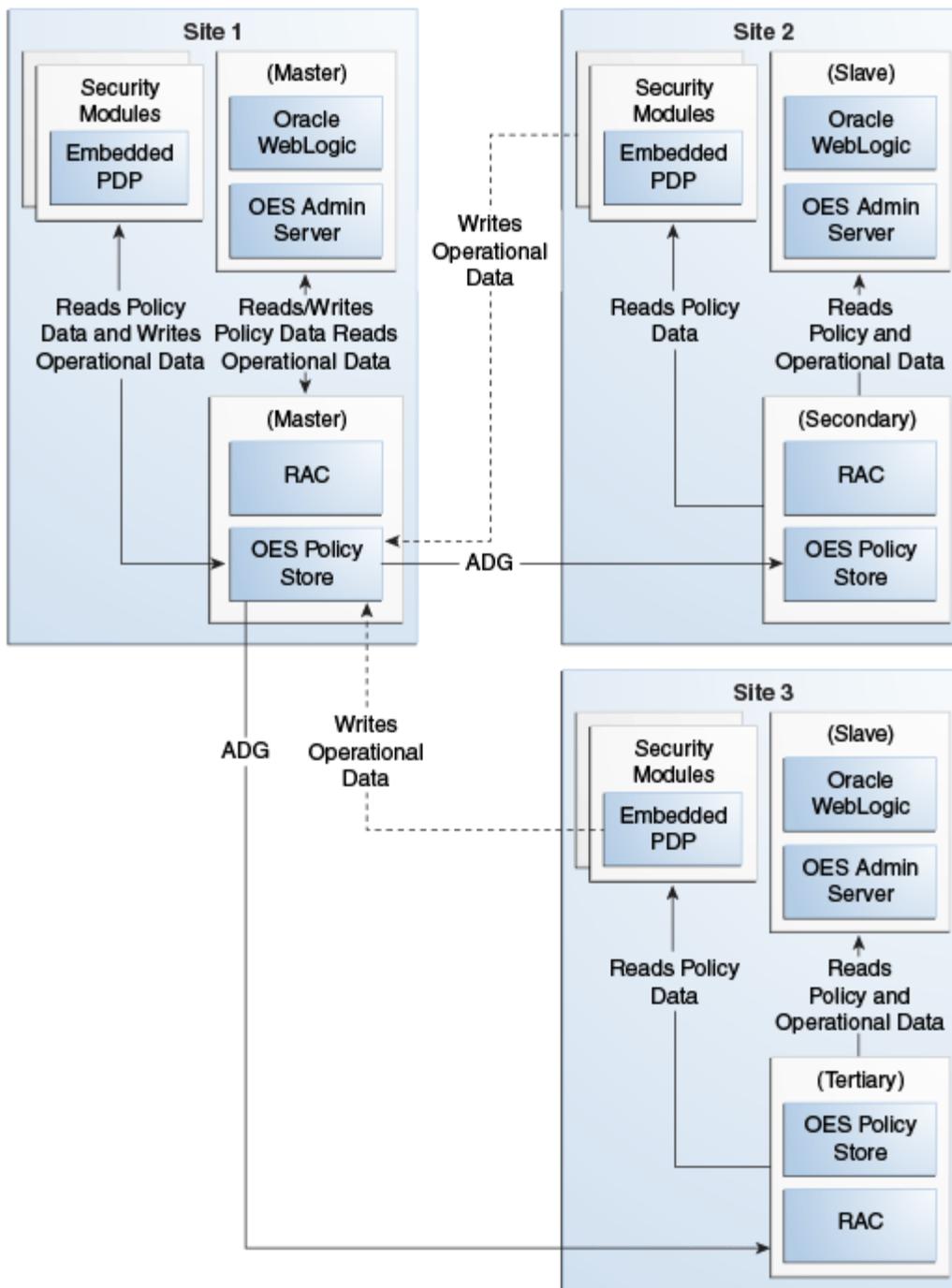
15.1 Multi-Site Oracle Data Guard with Oracle RAC Database Deployment Topology

In this release, the following configuration is required:

- One site is acting as master at any time. All the write operations are against the policy store configured for the current master site.
- All Security Modules are configured in controlled-pull mode. Non-controlled and controlled push modes are not supported.
- A policy store configured in mixed mode is not supported.
- Primary and standby databases are set up with Oracle Active Data Guard.
- Oracle Clusterware is installed and active on the primary and standby sites for Oracle RAC Databases.

Figure 15–1 illustrates the relationship between the Oracle Entitlements Server components when configured in a multi-site deployment:

Figure 15–1 Multi-Site Deployment Topology



As seen in the figure, when in a multi-site deployment the following relationships exist:

- Policy Distribution:** Security Modules are configured in controlled-pull mode on all the sites. The snapshot is generated by the Administration Server at the master site and replicated to the secondary and tertiary sites using Oracle Data Guard. The PDP on the secondary and tertiary sites retrieve the snapshot from the local policy store.

- **Configuration:** PDP are configured with multiple JDBC URL's. The primary JDBC URL is configured to the local policy store. In an event of failure to connect to the local Policy Store, a connection attempt to the secondary JDBC URL is made. This ensures that the policy store is accessible in an event of a failure.
- **SM ConfigUI:** Can be used to configure the JDBC URLs that are required to support failover functionality.

15.2 Oracle RAC Primary to Oracle RAC Standby Data Guard

In the following sections it is assumed that a primary Oracle RAC database has already been created and is up and running. The configuration is for a 2-node Oracle RAC Primary Database with a 2-node Oracle RAC Physical Standby Data Guard.

15.2.1 Installing Oracle Clusterware

To perform Oracle Clusterware and Oracle Automatic Storage Management installation and to perform the preinstallation steps for Oracle RAC, see *Oracle Grid Infrastructure Installation Guide for Linux*.

Prerequisites and steps for installing the Oracle Grid infrastructure software are as follows:

- Verifying system requirements
- Identifying and checking software requirements
- Installing the Linux operating system on all the Oracle RAC nodes and the DNS host
- Checking network requirements/configuration for Oracle RAC nodes, other servers, and DNS host
- Configuring the DNS server for SCAN VIPs, Node VIPs and Node IPs
- Enabling the Name Service Cache Daemon
- Creating Oracle Users, Groups, Permissions, and Installation Paths on all the Oracle RAC nodes
- Setting the Network Time Protocol on all Oracle RAC nodes
- Configuring shared storage for Oracle Grid infrastructure for a cluster and Oracle RAC
- Configuring the disk devices for Oracle ASM with ASMLib
- Configuring the Oracle Grid infrastructure

15.2.2 Installing Oracle Real Application Clusters

Install Oracle Real Application Clusters by following the instructions in *Oracle Real Application Clusters Installation Guide*. For information on Oracle RAC architecture, administration, and deployment, see *Oracle Real Application Clusters Administration and Deployment Guide*.

A *cluster* is a set of processes running on a single or multiple computers that share the same workload. After system components have been clustered, they are viewed functionally as a single entity from the perspective of a client for runtime processing and manageability. There is a close correlation between clustering and redundancy. A cluster provides redundancy for a system. With a load-balancing mechanism in place, the instances are redundant. If any of the instances fail, requests to the failed instance

can be sent to the surviving instances. If failover occurs during a transaction in a clustered environment, the session data is retained as long as there is at least one surviving instance available in the cluster.

See Also: "Oracle Entitlements Server High Availability Concepts" in *Oracle Fusion Middleware High Availability Guide*.

15.3 Setting Up Data Guard for Oracle RAC Databases

The primary database can be a single instance database or an Oracle Real Application Clusters (Oracle RAC) database. The standby databases can be single instance databases or Oracle RAC databases. See *Oracle Database High Availability Overview* for an overview of configuring and using Oracle Data Guard with Oracle RAC.

For information on setting up Data Guard for Oracle RAC Databases, see "Data Guard and Oracle Real Application Clusters" in *Oracle Data Guard Concepts and Administration*.

15.3.1 Preparing the Primary Database for Standby Database Creation

Before you create a standby database you must first ensure the primary database is properly configured. The tasks you must complete are listed below:

1. Place the primary database in FORCE LOGGING mode. You can do this after database creation using the following SQL statement:

```
SQL> ALTER DATABASE FORCE LOGGING;
```

2. Set the initialization parameters for the primary database.

Configure each instance of the Oracle RAC primary database to send its redo data to the Oracle RAC standby database (set up the `log_archive_dest_n` parameter on all primary instances).

For details, see "Configuring an Oracle RAC Primary Database to Send Redo Data" in *Oracle Data Guard Concepts and Administration*.

Ensure you use the correct format for archived redo log filenames as specified in "Format for Archived Redo Log Filenames" in *Oracle Data Guard Concepts and Administration*.

There are additional parameters you must add that control the receipt of the redo data and apply services when the primary database is transitioned to the standby role.

3. Put the primary database in ARCHIVELOG mode and enable automatic archiving.

See "Managing Archived Redo Logs" in *Oracle Database Administrator's Guide* for more information.

For details on preparing the primary database for standby database creation, see "Preparing the Primary Database for Standby Database Creation" in *Oracle Data Guard Concepts and Administration*.

For information on Oracle RAC-specific configuration consideration, see "Configuration Considerations in an Oracle RAC Environment" in *Oracle Data Guard Concepts and Administration*.

15.3.2 Creating a Physical Standby Database

Tasks you perform to create a physical standby database are as follows:

1. Create a backup of the primary database.
See Oracle Database Backup and Recovery User's Guide for information about how to perform a database backup operation.
2. Connect to the primary database and create a control file for the standby database.
3. Create the standby initialization parameter file and set the initialization parameters for each instance of the standby database. Depending on your configuration, you may need to set filename conversion parameters.

You must set up the appropriate parameters in the parameter file for each instance. For example, you must configure standby redo log archival on each standby database instance.
4. Copy files from the primary system to the standby system.

Copy the backup data files, standby control file, all available archived redo logs, and online redo logs from the primary site to the standby site. Copying of the online redo logs is necessary to facilitate switchover.
5. Set up the environment to support the standby database.
 - a. Create a Windows-based service if the standby database will be hosted on a Windows system.
 - b. Copy the remote login password file from the primary database system to the standby database system (all nodes).
 - c. Configure listeners for the primary and standby databases.
See Oracle Database Net Services Administrator's Guide.
 - d. Create Oracle Net service names.
See the Oracle Database Net Services Administrator's Guide and the Oracle Database Administrator's Guide.
 - e. Create a server parameter file for the standby database.
 - f. Copy the primary database encryption wallet to the standby database system.
6. Start the physical standby database.
 - a. Start the physical standby database.
 - b. Configure an Oracle RAC standby database to receive redo data from a primary database.

For details, see "Configuring an Oracle RAC Standby Database to Receive Redo Data" in *Oracle Data Guard Concepts and Administration*.
 - c. Create an online redo log on the standby database.
 - d. Start Redo Apply.

See "Starting Redo Apply" in *Oracle Data Guard Concepts and Administration*.
7. Verify the physical standby database is performing properly.
 - a. Identify the existing archived redo log files.
 - b. Force a log switch to archive the current online redo log file.
 - c. Verify the new redo data was archived on the standby database.
 - d. Verify that received redo has been applied.

For details, see "Creating a Physical Standby Database" in *Oracle Data Guard Concepts and Administration*.

For information on Oracle RAC-specific configuration consideration, see "Configuration Considerations in an Oracle RAC Environment" in *Oracle Data Guard Concepts and Administration*.

15.3.3 Configuring the Oracle Data Guard Broker

To configure the Oracle Data Guard broker, refer to "Managing Broker Configurations" in *Oracle Data Guard Broker*.

15.3.4 Performing Switchover and Failover Operations with Data Guard Broker

To test the manual switchover and failover, refer to "Switchover and Failover Operations" in *Oracle Data Guard Broker*.

15.4 Configuring Oracle Entitlements Server for High Availability Disaster Recovery

This section provides instructions to set up Oracle Entitlements Server for high availability and disaster recovery.

15.4.1 Oracle Entitlements Server High Availability Disaster Recovery Configuration Roadmap

Table 15–1 lists the configuration tasks for Oracle Entitlements Server high availability disaster recovery.

Table 15–1 Oracle Entitlements Server Disaster Recovery Configuration Flow

| No. | Task | Description |
|-----|--|--|
| 1 | Verify that all prerequisites are met. | See Section 15.4.2, "Prerequisites for Installing Oracle Entitlements Server." |
| 2 | Install OPSS Schema. | For more information, see Section 15.4.3, "Installing OPSS Schema". |
| 3 | Install Oracle Entitlements Server Administration Server Cluster on master policy store on OESHOST1. | For more information, see Section 15.4.4, "Installing Oracle Entitlements Server Administration Server Cluster on Master Policy Store on OESHOST1" |
| 4 | Install Oracle Entitlements Server Client in high availability environment. | For more information, see Section 15.4.5, "Installing Oracle Entitlements Server Client in High Availability Environment". |
| 5 | Configuring WebLogic Security Module cluster in controlled-pull distribution mode with JDBC URL with master Oracle RAC Database policy store. | For more information, see Section 15.4.6, "Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Master Oracle RAC Database Policy Store". |
| 6 | Install Oracle Entitlements Server Administration Server Cluster on secondary policy store. | For more information, see Section 15.4.7, "Installing Oracle Entitlements Server Administration Server Cluster". |
| 7 | Configuring WebLogic Security Module Cluster in controlled-pull distribution mode with JDBC URL with secondary Oracle RAC Database policy store. | For more information, see Section 15.4.8, "Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Secondary Oracle RAC Database Policy Store". |

15.4.2 Prerequisites for Installing Oracle Entitlements Server

You must have two groups of Oracle RAC Databases with

- Two instances for Active Data Guard primary Oracle RAC Database
- Two instances for Active Data Guard standby Oracle RAC Database

15.4.3 Installing OPSS Schema

Run Oracle Fusion Middleware Repository Creation Utility (RCU) against the primary database. After it is finished, the OPSS schema can be propagated to the standby database. For more information about using RCU, see "Database Requirements" section in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

15.4.4 Installing Oracle Entitlements Server Administration Server Cluster on Master Policy Store on OESHOST1

Primary Administration Server cluster must have two OES Managed Servers for MAPI Create, Update and Delete (CUD) operations.

15.4.4.1 Install Oracle Entitlements Server Administration Server with Primary Oracle RAC Database

Install the Oracle Entitlements Server Administration Server with the primary Oracle RAC Database Policy Store.

Oracle Entitlements Server is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11g Installer to install Oracle Identity and Access Management Suite.

For information about installing the Oracle Entitlements Server Administration Console, see "Installing and Configuring Oracle Entitlements Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

15.4.4.2 Create the Oracle Entitlements Server Administration Server Domain with WebLogic Server Cluster

Run the Oracle Fusion Middleware Configuration Wizard to create a domain containing the Administration Server.

1. Run the `MW_HOME/oracle_common/common/bin/config.sh` script.
2. On the Welcome screen, select **Create a new WebLogic domain** and click **Next**. The Select Extension Source screen appears.
3. On the Select Extension Source screen, select **Oracle Entitlements Server for Managed Server**. The Configuration Wizard automatically selects Oracle JRF, Oracle Platform Security Service, and Basic WebLogic Server Domain.
4. In the Specify Domain Name and Location screen, enter the domain name for the domain you are creating and the domain location.
5. Configure a user name and a password for the administrator.
6. Choose the WebLogic domain startup mode and JDK in the Configure Server Start Mode and JDK screen.
7. For data source configuration, choose **GridLink** to create the data source.

8. When inputting listeners for the GridLink data source, add the primary Oracle RAC Database as the first listener and the service name as `manage.example.com`.
9. On the Select Optional Configuration screen, select **Administration Server and Managed Servers, Clusters and Machines**.

10. In the Configure the Administration Server screen, enter the following values:

- **Name:** AdminServer
- **Listen address:** All Local Addresses
- **Listen port:** 7001
- **SSL listen port:** 7002
- **Select SSL enabled**

11. On the Configure Managed Servers screen, when you first enter the screen, one Managed Server called `oes_server1` is created automatically. You can rename `oes_server1` and update its attributes for this entry.

For example:

- **Name:** `oes_server1`
- **Listen Address:** hostname of the server on which `oes_server1` is running
- **Listen Port:** 14600
- **SSL Port:** 14601

For the second Managed Server, click Add and enter the following values:

- **Name:** `oes_server2`
- **Listen Address:** hostname of the machine on which `oes_server2` is running.
- **Listen Port:** 14600
- **SSL Port:** 14601

12. In the Configure Clusters screen, click **Add** to create a cluster.

Enter the name `oes_cluster`. Select **unicast** for the Cluster messaging mode, then enter the Cluster address in the format `listen address or DNS name of oes_server1:port,listen address or DNS name of oes_server2:port` or `managed server1:port,managed server2: port`.

13. On the Assign Servers to Clusters screen, associate the Managed Servers with the cluster:

Click on the cluster name **oes_cluster** in the right window.

Click on the Managed Server **oes_server1** then click the arrow to assign it to the cluster.

Repeat the preceding steps for the Managed Server `oes_server2`.

14. On the Configure Machines screen, create a machine for each host in the topology.

For Administration Server Host:

- **Name:** Name of your host. Use the DNS name here.
- **Node Manager Listen Address:** Oracle recommends that the machine IP address be identical to the DNS name of the machine.
- **Node Manager Listen Port:** Enter a port for Node Manager to use.

Leave all other values at the default settings.

Repeat the preceding steps for OESHOST1 and OESHOST2 and enter the following values. Leave all other values at the default settings.

- **Name:** Name of the host. A good practice is to use the DNS name.
 - **Node Manager Listen Address:** Oracle recommends that the machine IP address be identical to the DNS name of the machine.
 - **Node Manager Listen Port:** Enter a port for Node Manager to use.
15. On the Assign Servers to Machines screen, you assign the Managed Servers that will run on the machines you just created. Follow these steps:
1. Click a machine in the right hand window.
 2. Click the Managed Servers you want to run on that machine in the left window.
 3. Click the arrow to assign the Managed Servers to the machine.
 4. Repeat these steps until you assign all Managed Servers to the appropriate machine.
- ADMINHOST: AdminServer
- OESHOST1: oes_server1
- OESHOST2: oes_server2
5. On the Configuration Summary screen, click **Create**.
 6. Configure the OPSS Security Store. See "Configuring the Database Security Store for Oracle Entitlements Server Administration Server" in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.

15.4.4.3 Configuring Security Store for Oracle Entitlements Server Administration Server

1. Run `configureSecurityStore.py` to configure the database policy store. For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh MW_HOME/Oracle_
IDM1/common/tools/configureSecurityStore.py
-d /scratch/example_user/Oracle/Middleware/user_
projects/domains/oesserver2/
-t database_ORACLE
-j cn=jpsroot
-m create
-p password
```

2. Start up the Administration Server and Managed Servers.

15.4.4.4 Configuring Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP Request Distribution

To configure Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP request distribution:

1. Open the `mod_wl_ohs.conf` file, which is located in the following directory, in a text editor:

```
ORACLE_INSTANCE/config/OHS/ohs1/
```

2. Specify the details of the destination cluster within a new <location> element.

```
# OES admin console
<Location /apm>
SetHandler weblogic-handler
WebLogicCluster apmhost1:port1, apmhost2:port2
</Location>
```

3. Restart Oracle HTTP Server instance.

15.4.4.5 Access the Oracle Entitlements Server Administration Console

Access the Oracle Entitlements Server Administration Console at the master site:

```
http://ohs_host:port/apm
```

The OES folder is located under *MW_HOME/IDM_HOME*.

Access and login to Oracle Entitlements Server Administration Console at

- `http://hostname1:port/apm`
- `http://hostname2:port/apm`
- `http://ohs_host:port/apm`

15.4.5 Installing Oracle Entitlements Server Client in High Availability Environment

For instructions on how to install the Oracle Entitlements Server Client, see "Installing Oracle Entitlements Server Client" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

Verify that the installation was successful and the oessm directory was created under *OES_CLIENT_HOME*.

15.4.6 Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Master Oracle RAC Database Policy Store

The WebLogic Security Module cluster must have two WebLogic Security Module Managed Servers against the primary Oracle RAC Database.

Note: All Security Modules are configured in controlled-pull mode. Non-controlled and controlled push modes are not supported.

To configure the Oracle Entitlements Server Client, see the following sections in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*:

- Configuring Controlled Pull Distribution Mode
- Configuring WebLogic Server Security Module

Important configuration details are listed as follows:

1. Edit `smconfig.prp` to modify the properties for the following:
 - `oracle.security.jps.runtime.policyDistributionMode`
 - `jdbc.url`
 - `oracle.security.jps.runtime.pd.client.multisite.primaryJdbcUrl`
 - `oracle.security.jps.runtime.pd.client.multisite.onsserver`

For example:

- oracle.security.jps.runtime.policyDistributionMode=controlled-pull
- jdbc.url=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER = on) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = **racpri_scan_ip**) (PORT = **racpri_scan_listenerport**))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = **racstby_scan_ip**) (PORT = **racstby_scan_listenerport**))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))))
- oracle.security.jps.runtime.pd.client.multisite.primaryJdbcUrl=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER = on) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = **racpri_scan_ip**) (PORT = **racpri_scan_listenerport**))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL=TCP) (HOST = **racstby_scan_ip**) (PORT = **racstby_scan_listenerport**))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))))
- oracle.security.jps.runtime.pd.client.multisite.onsserver= nodes=**racpri_scan_ip:onsport, racstby_scan_ip: onsport**

2. Create a controlled-pull WebLogic Security Module instance and configure the WebLogic Security Module cluster domain:

```
$OES_CLIENT_HOME/oessm/bin/config.sh -multisite
```

- Note: Use the OPSS schema for the Oracle Entitlements Server Policy Store user name
 - Add a parameter -multisite to enable multi-site configuration.
 - Select **Oracle Entitlements Server WebLogic Security Module On WebLogic Managed Server** template.
 - Create the wlssm_cluster with wlssm_server1, wlssm_server2.
3. Check the WebLogic Server controlled-pull Security Module jps-config.xml file of each Managed Server in the WebLogic Security Module domain to confirm Oracle RAC Database URL to jdbc.url, for example,


```
{{jdbc:oracle:thin@(DESCRIPTION= }} (LOAD_BALANCE=on) {{ (ADDRESS=(PROTOCOL=TCP) (HOST=racnode1) (PORT=1521)) }} {{ (ADDRESS=(PROTOCOL=TCP) (HOST=racnode2) (PORT=1521)) }} (CONNECT_DATA=(SERVICE_NAME=service_name))"
```
 4. Start WebLogic Server controlled-pull Security Module Administration Server and Managed Servers
 5. Verify the following:
 - The controlled-pull WebLogic Security Module instance is created under *OES_CLIENT_HOME/oes_sm_instances*.
 - The WebLogic Security Module domain is created.
 - The controlled-pull WebLogic Security Module Cluster started successfully.
 - Log in is successful to the WebLogic Security Module Administration Console at:

```
http://WLSSM_host:port/console
```

15.4.7 Installing Oracle Entitlements Server Administration Server Cluster

The secondary Administration Server cluster must have two OES Managed Servers for MAPI query operations.

15.4.7.1 Install Oracle Entitlements Server Administration Server with Secondary Oracle RAC Database

Install Oracle Entitlements Server Administration Server with the primary Oracle RAC Database policy store.

Oracle Entitlements Server is included in the Oracle Identity and Access Management Suite. You can use the Oracle Identity and Access Management 11g Installer to install Oracle Identity and Access Management Suite.

For information about installing the Oracle Entitlements Server Administration Console, see "Installing and Configuring Oracle Entitlements Server" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

15.4.7.2 Create the Oracle Entitlements Server Administration Server Domain with WebLogic Server Cluster

Run Oracle Fusion Middleware Configuration Wizard to create a domain containing the Administration Server.

1. Run the `MW_HOME /oracle_common/common/bin/config.sh` script.
2. On the Welcome screen, select **Create a new WebLogic domain** and click **Next**. The Select Extension Source screen appears.
3. On the Select Extension Source screen, select **Oracle Entitlements Server for Managed Server**. The Configuration Wizard automatically selects Oracle JRF, Oracle Platform Security Service, and Basic WebLogic Server Domain.
4. In the Specify Domain Name and Location screen, enter the domain name for the domain you are creating and the domain location.
5. Configure a user name and a password for the administrator.
6. Choose the Weblogic domain startup mode and JDK in the Configure Server Start Mode and JDK screen.
7. For data source configuration, choose **GridLink** to create data source.
8. When inputting listeners for GridLink data source, add the primary Oracle RAC Database as the first listener and service name as `distribution.example.com`.
9. On the Select Optional Configuration screen, select **Administration Server and Managed Servers, Clusters and Machines**.
10. In the Configure the Administration Server screen, enter the following values:
 - **Name:** AdminServer
 - **Listen address:** All Local Addresses
 - **Listen port:** 7001
 - **SSL listen port:** 7002
 - **Select SSL enabled**
11. On the Configure Managed Servers screen, when you first enter the screen, one Managed Server called `oes_server1` is created automatically. You can rename `oes_server1` and update its attributes for this entry.

For example:

- **Name:** oes_server1
- **Listen Address:** host name of the machine on which oes_server1 is running.
- **Listen Port:** 14600
- **SSL Port:** 14601

For the second Managed Server, click **Add** and enter the following values:

- **Name:** oes_server2
- **Listen Address:** host name of machine on which oes_server2 is running.
- **Listen Port:** 14600
- **SSL Port:** 14601

12. In the Configure Clusters screen, click **Add** to create a cluster.

Enter the name `oes_cluster`. Select **unicast** for Cluster messaging mode, then enter the Cluster address in the format `listen address or DNS name of oes_server1:port,listen address or DNS name of oes_server2:port` or `managed server1:port,managed server2: port`.

13. On the Assign Servers to Clusters screen, associate the Managed Servers with the cluster:

Click on the cluster name **oes_cluster** in the right window.

Click on the Managed Server **oes_server1** then click the arrow to assign it to the cluster.

Repeat the preceding steps for the Managed Server **oes_server2**.

14. On the Configure Machines screen, create a machine for each host in the topology.

For Administration Server Host:

- **Name:** Name of your host. Use the DNS name here.
- **Node Manager Listen Address:** Oracle recommends that the machine IP address be identical to the DNS name of the machine.
- **Node Manager Listen Port:** Enter a port for Node Manager to use.

Leave all other values at the default settings.

Repeat the preceding steps for OESHOST1 and OESHOST2 and enter the following values. Leave all other values at the default settings.

- **Name:** Name of the host. A good practice is to use the DNS name.
- **Node Manager Listen Address:** Oracle recommends that the machine IP address be identical to the DNS name of the machine.
- **Node Manager Listen Port:** Enter a port for Node Manager to use.

15. On the Assign Servers to Machines screen, you assign the Managed Servers that will run on the machines you just created. Follow these steps:

1. Click on a machine in the right hand window.
2. Click on the Managed Servers you want to run on that machine in the left window.
3. Click on the arrow to assign the Managed Servers to the machine.

4. Repeat these steps until you assign all Managed Servers to the appropriate machine.
ADMINHOST: Administration Server
OESHOST1: oes_server1
OESHOST2: oes_server2
5. On the Configuration Summary screen, click **Create**.
6. Configure the OPSS Security Store. See "Configuring the Database Security Store for Oracle Entitlements Server Administration Server" in Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management.

15.4.7.3 Export Encryption Key from Primary Domain

Export EncryptionKey from the primary domain.

```
exportEncryptionKey(jpsConfigFile="/scratch/example_user/Oracle/Middleware/
user_
projects/domains/domainname/config/fmwconfig/jps-config.xml",keyFilePath="/net/
standby_host/scratch/example_user/keydir",keyFilePassword="welcome1")
```

15.4.7.4 Configuring Security Store for Oracle Entitlements Server Administration Server

1. Run `configureSecurityStore.py` to configure the database policy store. For example:

```
MW_HOME/oracle_common/common/bin/wlst.sh MW_HOME/Oracle_
IDM1/common/tools/configureSecurityStore.py
-d /scratch/example_user/Oracle/Middleware/user_projects/domains/oesserver2/
-t database_ORACLE
-j cn=jpsroot
-m join
-f oesserver2
-p password
-k /net/standby_host/scratch/example_user/keydir
-w password
```

2. Start up the Administration Server and Managed Servers.

15.4.7.5 Configuring Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP Request Distribution

To configure Oracle HTTP Server for Oracle Entitlements Server Administration Console HTTP request distribution:

1. Open the `mod_wl_ohs.conf` file, which is located in the following directory, in a text editor:

```
ORACLE_INSTANCE/config/OHS/ohs1/
```

2. Specify the details of the destination cluster within a new `<location>` element.

```
# OES admin console
<Location /apm>
SetHandler weblogic-handler
WebLogicCluster apmhost1:port1, apmhost2:port2
</Location>
```

- Restart Oracle HTTP Server instance.

15.4.7.6 Access the Oracle Entitlements Server Administration Console

Access the Oracle Entitlements Server Administration Console at the master site:

`http://ohs_host:port/apm`

Access and login to Oracle Entitlements Server Administration Console at

- `http://hostname1:port/apm`
- `http://hostname2:port/apm`
- `http://ohs_host:port/apm`

15.4.8 Configuring WebLogic Security Module Cluster in Controlled-Pull Distribution Mode with JDBC URL with Secondary Oracle RAC Database Policy Store

The WebLogic Security Module cluster must have two WebLogic Security Module Managed Servers against a standby Oracle RAC Database.

Note: All Security Modules are configured in controlled-pull mode. Non-controlled and controlled push modes are not supported.

To configure the Oracle Entitlements Server Client, see the following sections in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*:

- Configuring Controlled Pull Distribution Mode
- Configuring WebLogic Server Security Module

Important configuration details are listed as follows:

- Edit `smconfig.prp` to modify the properties for the following:

- `jdbc.url`
- `oracle.security.jps.runtime.pd.client.multisite.primaryJdbcUrl`
- `oracle.security.jps.runtime.pd.client.multisite.onserver`

For example:

- `jdbc.url=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER = on) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = racstby_scan_ip) (PORT = racstby_scan_listenerport))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = racpri_scan_ip) (PORT = racpri_scan_listenerport))) (CONNECT_DATA = (SERVICE_NAME = distribution.example.com))))`
- `oracle.security.jps.runtime.pd.client.multisite.primaryJdbcUrl=jdbc:oracle:thin:@(DESCRIPTION_LIST = (LOAD_BALANCE = off) (FAILOVER = on) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = racpri_scan_ip) (PORT = racpri_scan_listenerport))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))) (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL=TCP) (HOST = racstby_scan_ip) (PORT = racstby_scan_listenerport))) (CONNECT_DATA = (SERVICE_NAME = manage.example.com))))`

- oracle.security.jps.runtime.pd.client.multisite.onserver= nodes= **racpri_scan_ip:onsport, racstby_scan_ip: onsport**

NOTE: the service name for parameter jdbc.url is "distribution.example.com" instead of "manage.example.com"

2. Create a controlled-pull WebLogic Security Module instance and configure WebLogic Security Module cluster domain.

```
$OES_CLIENT_HOME/oessm/bin/config.sh -multisite
```

Note: Use the OPSS schema for the Oracle Entitlements Server Policy Store user name

Add a parameter -multisite to enable multi-site configuration.

3. Select **Oracle Entitlements Server WebLogic Security Module On WebLogic Managed Server** template.
4. Create the wlssm_cluster with wlssm_server1, wlssm_server2.
5. Check WebLogic Server controlled-pull Security Module jps-config.xml file in the WebLogic Security Module domain to confirm Oracle RAC Database URL to jdbc.url, for example, {{jdbc:oracle:thin@(DESCRIPTION= }} (LOAD_BALANCE=on) {{ (ADDRESS=(PROTOCOL=TCP)(HOST=racnode1) (PORT=1521)) }} {{ (ADDRESS=(PROTOCOL=TCP)(HOST=racnode2) (PORT=1521)) }} (CONNECT_DATA=(SERVICE_NAME=service_name))"
6. Start the WebLogic Server controlled-pull Security Module.
7. Verify the following:
 - The controlled-pull WebLogic Security Module instance is created under *OES_CLIENT_HOME/oes_sm_instances*.
 - The WebLogic Security Module domain is created.
 - The controlled-pull WebLogic Security Module Cluster started successfully.
 - Log in is successful to the WebLogic Security Module Administration Console at:

```
http://WLSSM_host:port/console
```

Tuning Performance and Monitoring Components

Monitoring and performance tuning are essential to the administration of the Oracle Entitlements Server components used by your applications. You monitor components to ensure they are running smoothly and tune the performance of Oracle Entitlements Server components to achieve optimal performance and throughput based on the current system resources and traffic load.

This chapter describes how to configure and deploy Oracle Entitlements Server to maximize performance and throughput and covers monitoring, analyzing, and tuning the components that are used by your applications. This chapter contains the following sections:

- [Section 16.2, "Oracle Entitlements Server Performance Planning"](#)
- [Section 16.3, "Performance Tuning Considerations for Oracle Entitlements Server"](#)

16.1 Understanding Key Concepts and Components in Oracle Entitlements Server Deployment

This chapter assumes that you are familiar with the key concepts and components in an Oracle Entitlements Server deployment. The following sections will provide the basis for some of the performance-related topics in this chapter:

- [Section 1.2, "Overview of Oracle Entitlements Server"](#) introduction and [Figure 1–1, "Components of Oracle Entitlements Server"](#)
- [Section 1.3.1, "The Policy Administration Point"](#)
- [Section 1.3.2, "The Policy Decision Point and the Policy Enforcement Point"](#)
- [Section 1.3.3, "The Policy Information Point"](#)
- [Section 1.4, "How Oracle Entitlements Server Processes Authorization Policies"](#)

16.2 Oracle Entitlements Server Performance Planning

Performance tuning usually involves a series of trade-offs. If you experience bottlenecks and determine what the causes are, you may need to modify performance in some other areas to achieve the expected results. If you have a clearly defined plan for achieving your performance objectives, the decision on what to trade for higher performance is easier because you have identified the most important areas.

To maximize the performance capabilities of your applications, you must build performance and scalability into your design. The performance plan addresses the

current performance requirements, the existing issues (such as bottlenecks or insufficient hardware resources), and any anticipated variances in load, users or processes. The performance plan also addresses how the components scale during peak usage without impacting performance.

The following sections of this chapter discuss the steps to create a plan to tune your application environment and optimize performance:

Step 1: [Define Your Performance Objectives and Requirements](#)

Step 2: [Design Authorization for Applications](#)

16.2.1 Define Your Performance Objectives and Requirements

Before you can begin performance tuning your applications, you must first identify the performance objectives you want to achieve.

To understand what your performance objectives are, complete the following steps:

- [Define Operational Requirements](#)
- [Identify Performance Goals](#)
- [Conduct Performance Evaluations](#)

16.2.1.1 Understand Performance Constraints

Understanding performance constraints and their impacts ensures that you set realistic performance objectives for your application environment, such as response times, throughput, and load on specific hardware. Performance objectives are limited by constraints, such as:

- The configuration of hardware and software such as CPU type, disk size, disk speed, and sufficient memory.
- The type of hardware and software configuration that is required to meet application needs adequately. The process of determining the needs is called capacity planning, and there is no single formula for determining your hardware requirements.
- The system performance goals. Capacity planning requires an assessment of your system performance goals and an understanding of your application. Capacity planning for server hardware focuses on maximum performance requirements.

For more information on capacity planning, see the "Capacity Planning and Using Clusters and High Availability Features" chapter in *Oracle Fusion Middleware Performance and Tuning Guide*.

- The configuration of high availability architecture to address peak usage and response times.

For more information on implementing high availability features in Oracle Entitlements Server see the "Configuring High Availability for Oracle Entitlements Server" chapter in *Oracle Fusion Middleware High Availability Guide for Oracle Identity and Access Management*.

- The ability to interoperate between domains, use legacy systems, support legacy data.
- The development, implementation, and maintenance costs.

16.2.1.2 Define Operational Requirements

Before you begin to deploy and tune your application for high availability (HA) and disaster recovery (DR), it is important to clearly define the operational environment. The operational environment is determined by high-level constraints and requirements such as:

- Deployment architecture
- End-to-end deployment and operational security requirements
- Hardware resources
- High availability (HA) and disaster recovery (DR) requirements

16.2.1.3 Identify Performance Goals

Whether you are designing a new system or maintaining an existing system, set specific performance goals so that you know how and what to optimize. To determine your performance objectives, you must understand the application deployed and the environmental constraints placed on the system.

Gather information about the levels of authorization activity that application are expected to meet, such as:

- Anticipated number of users per business application (total and concurrent)
- Number of concurrent user authorization requests per application
- Total number of applications being managed
- Amount of authorization data (organized by application)
- High availability and disaster recovery choices and possible impact on authorization system performance
- Capacity planning based on target CPU utilization

16.2.1.4 Conduct Performance Evaluations

With clearly defined performance goals and performance expectations and based on sizing guidelines and performance data, you can readily conduct and determine if performance tuning has been successful. Success depends on the functional objectives you have established with the user community, your ability to measure whether the criteria are being met, and your ability to take corrective action to overcome any exceptions.

16.2.2 Design Authorization for Applications

This section contains the following topics:

- [Policy Design](#)
- [Best Practices for Designing Application Authorization](#)

16.2.2.1 Policy Design

Oracle Entitlements Server strives to provide a policy model which closely represents common business, application and service flows.

A simple one to one mapping of individual business roles and privileges often leads to policy bloat and more importantly does not capture the underlying process and object relationships. Oracle Entitlements Server uses hierarchy as basis for policy modeling. This facilitates grouping of objects based on their relationships. Furthermore it allows

attribute and privilege inheritance. The Oracle Entitlements Server hierarchical resource, role, policy, and policy domain hierarchies structures allow for exponential reduction in size and complexity of policies. Oracle Entitlements Server supports Attribute-Based Access Control (ABAC), Role-based Access Control (NIST RBAC), ERBAC (Enterprise RBAC) and Java Authentication and Authorization Service (JAAS) policy models. Based on business needs either of the policy models can be used or several of them can be used in combination.

Business process and objects often tend to be hierarchical. For example, a loan approval process consists of multiple subprocesses and some of these subprocess might constitute additional finer grained processes. In a similar way a web application can consist of multiple web pages, each page has different sections and each section has different pieces of information.

16.2.2.1.1 Building Role-based Access Control (RBAC) Models Using Oracle Entitlements

Server Role-based Access Control (RBAC) models use roles to model enterprise security. For RBAC, permission (or privilege) is a trivial extension of role. Roles can be divided into three categories:

- **Enterprise Wide Static Roles:** Users are granted these roles irrespective of what they are trying to do. For example, an Employee role can be a static assignment because it is common across enterprise. These roles are best stored in an LDAP or some other enterprise wide identity store. These roles are normally assigned at the time of authentication and are generally valid until session expiration.
- **Application Specific Static Roles:** These are static role assignments which are specific to a subset of enterprise applications. A user or an enterprise role is granted different roles based on the applications they are trying to access. Typically, it is recommended to grant the application role to the enterprise role as best practice. The user number normally is extremely large in the enterprise. It is hardly managed and might affect performance.
- **Application Specific Dynamic Roles:** These are dynamically or conditionally assigned application roles. They are assigned on an as-needed basis depending on the action initiated by the user. For example, the Fund Manager role should be granted to a person only on certain funds. They come into existence when an authorization request is made and they are destroyed once a decision is computed. As discussed previously Oracle Entitlements Server provides sophisticated facilities to accurately control role assignments based on the context.

As seen above, enterprise wide static roles are easy to compute, but they are rigid. Dynamic roles need to be computed for every authorization request but they are very flexible and dynamic. However due to locality of reference, these roles can often be fetched from the cache and do not require full computation. The static/dynamic nature and scope of roles are deciding factors in choosing the correct role type. Depending on changing requirements, an enterprise wide role can be converted to an Application specific dynamic role or vice versa.

This type of interoperability is possible because Oracle Entitlements Server is based on the NIST RBAC and ABAC standards.

16.2.2.1.2 Building Attribute Based Access Control (ABAC) Models Using Oracle Entitlements

Server Attributes are the basis for the ABAC (Attribute Based Access Control) model. Oracle Entitlements Server supports a variety of attributes (for example user, enterprise role attributes are supported by OES via PIP; resource attributes are supported by OES directly; application role attributes are not supported); in addition, custom attributes can be defined for special needs. ABAC has heavy reliance of conditions, essentially all authorization decisions are made by evaluating expressions

based on these attributes. As an authorization model ABAC offers more flexibility than RBAC because it heavily relies on dynamic computation. However, this comes at the cost of being able to perform audits based on static policy data. Also, the added complexity means that ABAC models are more computation-intensive than their RBAC counterparts.

Oracle Entitlements Server lays out a policy structure to help map business security requirements into raw ABAC models. Subjects (Users and Enterprise Role), Resources, and attributes are the most commonly used elements in ABAC policies. The Oracle Entitlements Server UI creates an easy to use abstraction around these objects to simplify the construction of policies. Oracle Entitlements Server also supports Resource, Attribute and Policy inheritance which allow policies to be placed strategically so that they will be able to control large number of Users and Resources.

For more information on the recommended design techniques for the different Oracle Entitlements Server components, see *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

16.2.2.2 Best Practices for Designing Application Authorization

The previous section presented various standard authorization models like RBAC, Java2 ABAC, and so on that are supported by Oracle Entitlements Server for designing the application authorization. The following are the key areas to consider to design a highly scalable authorization subsystem.

The first one is to choose the right authorization model that is inherently suited for the application usage pattern. For example, if you want to build a hospital information application where the application usage pattern is well defined through functional entities like nurse, doctor, and so on, then it is natural that this application can readily benefit by uptaking the RBAC based authorization design pattern.

The second one is that the aspect of the design is to decide the growth factor of the various elements of the authorization subsystem. Typically an authorization system can be thought of as a 3-dimensional space where the application consumer (identified as End User, Group or an application role), the application resources and the operations that are protected and the authorization policy that binds the application user & (allowed resource + operations) with additional rules become the 3 dimensions. In a good scalable and performant authorization subsystem, it is very important to keep effect of the growth in the dimensions of the authorization space as much constant as possible on authorization subsystem. For example:

- If in an application the total number of protected resources is continuously growing like the growth in total number expense report database records along with the total number users for data security
- If the total number of application roles are growing as there are new kinds, end-user groupings need to be handled for functional security

In these scenarios it is very important the design of the authorization subsystem be tolerant to handle the growth through some intelligent authorization patterns like inheritable policies on hierarchical resources, attribute based policies and the application roles policies with attribute based conditions to handle types of user populations. The important point is the growth in the authorization subsystem is based on the application business requirements for dealing with a new kind's authorization requirements rather than dealing with the growth of the dimension of the authorization scope.

The third item is dealing with the new challenges of the modern cloud based applications that needs to make authorization decisions not only on the conventional static information about the application user but also needs to use the user's dynamic

contextual information. This requires adaptation of application authorization modeling and design to combine multiple authorization standards to deal with new requirements like using RBAC and ABAC together, and so on.

The fourth item is designing SAAS applications that are deployed on Cloud and provide services to multiple customers. This requires designing applications to support multitenancy and data isolation not only in the business data but also the security data. This will bring much more stringent requirements and restrictions on the authorization subsystem to be more compact, efficient and resilient with the growth number of tenants.

16.3 Performance Tuning Considerations for Oracle Entitlements Server

Once you have installed and configured Oracle Entitlement Server, you want the best possible performance. This section provides guidelines for Oracle Entitlement Server administrators on optimizing Oracle Entitlement Server performance. This section includes the following topics:

- [Tuning the OES Policy Store](#)
- [Tuning of OES Administration Server](#)
- [Tuning OES Security Modules](#)
- [Tuning OES Distribution Service](#)
- [Tuning OES Attribute Retrievers](#)
- [Tuning OES Cache](#)
- [Tuning Resource Intensive Operations](#)
- [Enabling Logging](#)

The tuning optimizations for these Oracle Entitlements Server components are described in the following sections.

16.3.1 Tuning the OES Policy Store

The first component that needs to be tuned from the overall performance tuning is the OES policy store. Tuning the policy store involves the tuning of the underlying database and the TopLink Java Persistence API (JPA) provider. The Java Persistence API is a specification for persistence in Java EE and Java SE applications. The following sections provides information about specific tuning aspects as a part of policy store tuning.

16.3.1.1 Oracle Database System Parameters Tuning

[Table 16–1](#) explains the various Oracle Database system parameters that need to be tuned with their optimal values and provides example values. You may adjust the values based on your application needs.

Table 16–1 Oracle Database System Parameters Tuning

| Parameter Name | Description | Default value | Recommended value |
|-----------------------|---|--|--------------------------|
| processes | PROCESSES specifies the maximum number of operating system the user processes that can simultaneously connect to Oracle | 40 | 1500 |
| sga_target | SGA_TARGET specifies the total size of all SGA components. | 0 (SGA autotuning is disabled for DEFERRED mode and autotuning requests, but allowed for IMMEDIATE mode autotuning requests) | 3221225472 (3GB) |
| audit_trail | AUDIT_TRAIL enables or disables database auditing. | None | None |
| open_cursors | OPEN_CURSORS specifies the maximum number of open cursors (handles to private SQL areas) a session can have at once | 50 | 500 |
| pga_aggregate_target | PGA_AGGREGATE_TARGET specifies the target aggregate PGA memory available to all server processes attached to the instance | 10 MB or 20% of the size of the SGA, whichever is greater | 1610612736 (1.5GB) |

Table 16–1 (Cont.) Oracle Database System Parameters Tuning

| Parameter Name | Description | Default value | Recommended value |
|------------------------|---|---------------|-------------------|
| nls_sort | NLS_SORT specifies the collating sequence for ORDER BY queries. If the value is BINARY, then the collating sequence for ORDER BY queries is based on the numeric value of characters (a binary sort that requires less system overhead). If the value is a named linguistic sort, sorting is based on the order of the defined linguistic sort. Most (but not all) languages supported by the NLS_LANGUAGE parameter also support a linguistic sort with the same name. | | BINARY |
| filesystemio_options | FILESYSTEMIO_OPTIONS specifies I/O operations for file system files. | | SETALL |
| fast_start_mttr_target | FAST_START_MTTR_TARGET enables you to specify the number of seconds the database takes to perform crash recovery of a single instance | 0 | 3600 |
| db_securefile | DB_SECUREFILE specifies whether or not to treat LOB files as Secure Files. | PERMITTED | ALWAYS |
| session_cached_cursors | SESSION_CACHED_CURSORS specifies the number of session cursors to cache | 0 | 500 |
| plsql_code_type | PLSQL_CODE_TYPE specifies the compilation mode for PL/SQL library units. | INTERPRETED | NATIVE |
| "_b_tree_bitmap_plans" | | | False |

Table 16–1 (Cont.) Oracle Database System Parameters Tuning

| Parameter Name | Description | Default value | Recommended value |
|----------------|---|---------------|-------------------|
| Memory_target | MEMORY_TARGET is a database initialization parameter (introduced in Oracle 11g) that can be used for automatic PGA and SGA memory sizing. | 0 | 0 |

For more information about the Oracle Database redo logs, see *Oracle Database Reference*.

The following SQL script could be used for setting the system parameters. The SQL script needs to be run as a DB user with the SYSDBA role.

```
ALTER SYSTEM SET processes = 1500 SCOPE = spfile;
ALTER SYSTEM SET sga_target = 3221225472 SCOPE = spfile;
ALTER SYSTEM SET audit_trail = NONE SCOPE = spfile;
ALTER SYSTEM SET open_cursors = 500 SCOPE = spfile;
ALTER SYSTEM SET pga_aggregate_target = 1610612736 SCOPE = spfile;
ALTER SYSTEM SET nls_sort = BINARY SCOPE = spfile;
ALTER SYSTEM SET filesystemio_options = SETALL SCOPE = spfile;
ALTER SYSTEM SET fast_start_mttr_target = 3600 SCOPE = spfile;
ALTER SYSTEM SET db_securefile = ALWAYS SCOPE = spfile;
ALTER SYSTEM SET session_cached_cursors = 500 SCOPE = spfile;
ALTER SYSTEM SET plsql_code_type = NATIVE SCOPE = spfile;
ALTER SYSTEM SET "_b_tree_bitmap_plans" = FALSE scope=spfile
ALTER SYSTEM SET memory_target=0 SCOPE = SPPFILE;
```

Also make sure the kernel.shmall, kernel.shmmax, kernel.sem, and fs.file-max are set at optimal values (all kernel level parameter can be tuned and obtained from /etc/sysctl.conf).

16.3.1.2 Oracle Database REDO Log and UNDO Tablespace Tuning

All of the following operations for managing REDO logs and UNDO change logs need to be performed as a DB user with the SYSDBA role.

Increase Allocated Disk Space for Redo Log Files

It is recommended that you use three redo log files where each file is at least 4 GB in size. After creating the new REDO log files, the existing or old REDO log files (groups) need to be removed.

Run the following SQL command to add new redo log groups. Make sure the proper file path is set according to your environment.

```
alter database add logfile ('<oradata directory>/orcl/redo04.log') SIZE 4G;
alter database add logfile ('<oradata directory>/orcl/redo05.log') SIZE 4G;
alter database add logfile ('<oradata directory>/orcl/redo06.log') SIZE 4G;
```

Run the following SQL command to drop old redo log files (groups). Please follow the instructions below.

```
Exec SQL: SELECT group#, member FROM V$LOGFILE;
```

For the group# not for the members you added, you could drop them by:

```
ALTER DATABASE DROP LOGFILE GROUP <group#>;
```

If you are dropping an active Log group, you need to force a log switch as below:

```
ALTER SYSTEM SWITCH LOGFILE;
```

For more information about the Oracle Database redo log, refer to the "Managing the Redo Log" chapter of the *Oracle Database Administrator's Guide*.

Increase Disk Space Allocated for UNDO Tablespace

It is recommended that the UNDO tablespace be 20 GB in size.

Run the following SQL command to resize UNDO tablespace. Make sure the proper file path is set according to your environment.

```
ALTER DATABASE DATAFILE '<oradata directory>/orcl/undotbs01.dbf' RESIZE 20G;
```

For more information about Oracle Database UNDO, refer to the "Managing Undo" chapter of the *Oracle Database Administrator's Guide*.

16.3.1.3 Tablespaces Tuning

Tune Tablespaces During Repository Creation

The OES DB schema is created via RCU (Repository Creation Utility). While creating a database schema using RCU:

- Allocate sufficient large initial disk spaces for OES tablespaces for optimal performances. Allocate 6 GB files for IAS_OPSS and IAS_TEMP tablespaces.
- If many large applications will be managed in policy store, allocate a large tablespace size, 40 GB for IAS_OPSS tablespace, 15 GB for IAS_TEMP tablespace
- If many large applications will be added to policy store, it is recommended that you mark the tablespace increment as 1 GB, instead of 100 MB, to avoid continuous extending tablespace when it is full.

Steps using RCU to tune tablespaces during schema creation are provided below.

1. In the Map Tablespaces screen of RCU, click the **Manage Tablespaces** button to modify existing tablespaces.
2. Select the IAS_OPSS or IAS_TEMP tablespace on the left-hand portion of the screen, and edit the fields as described in [Table 16–2](#).

Table 16–2 Specifying the Tablespace to Edit

| Field | Description |
|-----------------|--|
| Name | The name of the tablespace. |
| Type | Permanent tablespace |
| Block Size (KB) | Default |
| Storage Type | Select Use Automatic Segment Space Management to use bitmaps to manage the free space within segments. |

3. To modify or edit a datafile, select the icon next to the datafile you want to edit, then click the icon with the pencil.
The Edit Datafile screen appears.
4. Provide the information described in the following table:

Table 16–3 Specifying the Size of a Datafile

| Field | Description |
|--|--|
| Size | Allocate sufficient large initial disk spaces for OES tablespaces for optimal performances. Allocate 6 GB files for IAS_OPSS and IAS_TEMP tablespaces. If many large applications will be managed in policy store, allocate a large tablespace size, 40 GB for IAS_OPSS tablespace and 15 GB for IAS_TEMP tablespace. Use the drop-down list to specify the size in gigabytes (GB). |
| Automatically extend datafile when full (AUTOEXTEND) | Select Automatically extend datafile when full (AUTOEXTEND) to automatically extend the size of your datafile when it becomes full. In the Increment field, specify 1 GB by which your datafile should be increased each time it becomes full. Use the drop-down list to specify gigabytes (GB). If many large applications will be added to the policy store, it is recommended that you mark the tablespace increment as 1 GB instead of 100 MB to avoid continuous extending tablespace when it is full. |
| Maximum Size | Unlimited |

Tune Tablespaces If DB Instance Already Exists

If the DB instance already exists, add more disk space by running the ALTER TABLESPACE command as a DB user with the SYSDBA role. For example:

```
alter tablespace R2_IAS_OPSS ADD DATAFILE '<oradata directory>/orcl/R2_ias_
opss2.dbf' SIZE 20 G AUTOEXTEND ON;
alter tablespace R2_IAS_TEMP ADD TEMPFILE '<oradata directory>/orcl/R2_
iastemp2.dbf' SIZE 10 G AUTOEXTEND ON;
```

16.3.1.4 Schema Statistics Gathering

The above steps take care of all of the required OES DB schema tuning. The only ongoing tuning that needs to be performed from time to time, as the policy data has been stored in the database, is gathering the database statistics as the OES DB scheme user.

The schema statistics should not be gathered for the column JPS_DN.PARENTDN. Gathering a histogram on this column will impact query performance. To disable histogram, run the following SQL script:

```
EXECUTE dbms_stats.delete_column_stats(ownname=><SCHEMA_NAME>, tabname=>'JPS_
DN', colname=>'PARENTDN', col_stat_type=>'HISTOGRAM');
EXECUTE dbms_stats.set_table_prefs(<SCHEMA_NAME>, 'JPS_DN', 'METHOD_OPT', 'FOR
ALL COLUMNS SIZE AUTO, FOR COLUMNS SIZE 1 PARENTDN');
```

Using your schema name, run the DBMS_STATS procedure to gather the latest statistics as follows:

```
Execute DBMS_STATS.gather_schema_stats(<SCHEMA_NAME>, DBMS_STATS.AUTO_SAMPLE_
SIZE, no_invalidate=>FALSE)
```

You can automate this by defining a database job to run the procedure with required frequency. This collection needs to be performed after a large policy data migration into store.

The following SQL example creates a database job called OPSS_AUTO_STATISTICS, which will be executed at 0:00 every Sunday morning. The database job needs to be added by a user with SYSDBA privileges.

```

BEGIN
  SYS.DBMS_SCHEDULER.CREATE_JOB (
    job_name => '"SYS"."OPSS_AUTO_STATISTICS"',
    job_type => 'PLSQL_BLOCK',
    job_action => 'Execute
DBMS_STATS.gather_schema_stats(''<SCHEMA>'', DBMS_STATS.AUTO_SAMPLE_SIZE, no_
invalidate=>FALSE);',
    number_of_arguments => 0,
    start_date => NULL,
    repeat_interval =>
'FREQ=WEEKLY;BYDAY=SUN;BYHOUR=0;BYMINUTE=0;BYSECOND=0',
    end_date => NULL,
    job_class => '"SYS"."DEFAULT_JOB_CLASS"',
    enabled => FALSE,
    auto_drop => FALSE,
    comments => '',
    credential_name => NULL,
    destination_name => NULL);

  SYS.DBMS_SCHEDULER.SET_ATTRIBUTE(
    name => '"SYS"."OPSS_AUTO_STATISTICS"',
    attribute => 'logging_level', value => DBMS_SCHEDULER.LOGGING_OFF);

  SYS.DBMS_SCHEDULER.enable(
    name => '"SYS"."OPSS_AUTO_STATISTICS"');
END;
/

```

Refer to Section 13.3.2 "When to Gather Statistics" in the *Oracle Database Performance Tuning Guide*.

16.3.1.5 EclipseLink Tuning

Oracle Entitlements Server uses EclipseLink as the JPA (Java Persistence API) implementation for database operations. Some EclipseLink tuning parameters (Table 16–4) could be set into the `jps-config.xml` file.

Table 16–4 EclipseLink Tuning

| Property | Description | Default |
|---|---|---------|
| <code>eclipselink.jdbc.connection_pool.default.max</code> | The maximum number of read connection in the internal connection pool | 32 |
| <code>eclipselink.jdbc.connection_pool.default.min</code> | The minimum number of read connection in the internal connection pool | 32 |

The properties could be overwritten by setting the DB policy store service instance for Oracle Entitlements Server Admin, or a PDP service in controlled-pull mode, as shown below.

```

<propertySet name="props.db.1">
  <property name="jdbc.url"
    value="jdbc:oracle:thin:@<HOST>:<PORT>/<SID>" />

```

```

<property name="oracle.security.jps.farm.name" value="cn=my_domain"/>
<property name="server.type" value="DB_ORACLE"/>
... ..
<property name=" eclipselink.jdbc.connection_pool.default.min" value="16"/>
<property name=" eclipselink.jdbc.connection_pool.default.min" value="64"/>
</propertySet>
... ..

<serviceInstance name="policystore.db" provider="policystore.provider">
  <property name="policystore.type" value="DB_ORACLE"/>
  <propertySetRef ref="props.db.1"/>
</serviceInstance>

```

For more EclipseLink properties, see the `PersistenceUnitProperties` class in the *EclipseLink API Reference*.

16.3.2 Tuning of OES Administration Server

To have better performance of large data operations, like migration and distribution, tune the JVM parameters as described in this section.

16.3.2.1 WLST Tuning

WLST (WebLogic Scripting Tool) is an Oracle Middleware command-line scripting interface. It is used for Oracle Entitlements Server for some management work, including migration of security store. For migrating large applications, you need to tune JVM parameters for the WLST tool for the Java memory size, as shown below:

Edit file `MIDDLEWARE_HOME/wlserver_10.3/common/bin/wlst.sh`.

Specify `JAVA_HOME` to JDK with version **1.6.0_31 or higher** and add `MEM_ARGS` as below:

```
MEM_ARGS="-Xms6144m -Xmx6144m -Xmn1900m -XX:+UseParallelGC -XX:PermSize=128m
-XX:MaxPermSize=1024m"
```

Note that the required heap size parameter (ms, mx, mn) could be based on the size of the application you will migrate.

16.3.2.2 OES Administration Server Tuning

The OES Administration Server needs to be tuned for optimized performance for the snapshot generation of application during policy distribution and also for all of the OES management UI CRUD operations as given below.

1. Use JDK version 1.6.0_31 or higher.
2. JDK memory size tuning. Large memory is required on the Administration Server to generate the application policy snapshot, especially for a large application policy. The JDK could be chosen while configuring the WebLogic domain for OES Administration. On the Configure Server Start Mode and JDK screen, choose from available JDKs if you have version is 1.6.0_31 or higher, or click "Other JDK" to choose one.

If you need to manually edit file the `DOMAIN_HOME/bin/startWeblogic.sh` script to set the `JAVA_HOME` property. Edit file the `DOMAIN_HOME/bin/startWeblogic.sh` script as shown below:

```
JAVA_HOME="/home/user/jdk1.6.0_31"
MEM_ARGS="-Xms6144m -Xmx6144m -Xmn1900m -XX:PermSize=128m -XX:MaxPermSize=1024m"
before the line "${JAVA_HOME}/bin/java ${JAVA_VM} -version"
```

16.3.3 Tuning OES Security Modules

When the OES Security Module is configured for controlled pull mode, it has two main functionalities

- It acts as a PDP and/or PEP; it receives an authorization request, makes a decision and enforces the decision.
- It calls the Policy Distribution component periodically to make configured policies and policy data available for evaluation.

So tuning the OES Security Module will focus on two parts, one is to ensure high throughput of authorization request processing and another is to distribute policy efficiently.

Policy data affects performance of the security module. The number of functions, attributes, roles, resources, and policies have a great influence on the authorization throughput, distribution time and memory size needed for Security Module.

In this section, the following policy data sample will be used in the examples. Your applications may vary in size and modeling.

```
Application Name: myapp
oracle.security.jps.ldap.root.name: cn=jpsroot
oracle.security.jps.farm.name: cn=base_domain
```

The policy data shown below is only an example. Policy artifacts numbers should be from your policy modeling.

The information shown below cannot be tuned on the SM side. The data could be used to estimate required memory on the SM.

Table 16–5 Security Module Tuning Attributes

| Item | Number | Comment | Query SQL |
|----------------------|--------|--|--|
| Resource Type | 1 | | |
| Attribute definition | 17 | | |
| Function definition | 269 | | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%cn=functions,;' |
| Application Role | 0 | No application role is created. WebLogic Server's roles and principals are used. | |
| Grantee | 5351 | The principals of the policy are stored as grantee. It seems one policy for one principal for both 2 applications. | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,cn=jaas policy,cn=grantees,;' |
| Permission | 1772 | The resource actions pairs used in policies | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,cn=jaas policy,cn=permissions,;' |
| Resource | 3173 | | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%cn=resources,;' |

Table 16-5 (Cont.) Security Module Tuning Attributes

| Item | Number | Comment | Query SQL |
|---------------------|-----------|----------------------------------|---|
| Entitlement | 1806 | | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%cn=permissions sets;' |
| Policy | 5351 | | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%cn=policies;' |
| Rule | 5351 | | select count(*) from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%cn=rules;' |
| Attributes | 1,484,356 | Attributes of above entries | select count(*) from jps_attrs where jps_dn_entryid in (select entryid from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,%'); |
| assignee attributes | 1,220,877 | Attribute for policy assignments | select count(*) from ct_9_1 where jps_dn_entryid in (select entryid from jps_dn where parentdn like 'cn=jpsroot,cn=jpscontext,cn=base_domain,cn=myapp,cn=jaas policy,cn=permissions,'); |

Policy distribution is the process to obtain policy data from a database policy store, write policy data to a local encrypted XML policy file, and switch between two copies of the runtime policy cache.

16.3.3.1 OES Security Module Memory Sizing

OES Security Module uses memory in following aspects:

- **To hold policy data in memory as cache.** Refer to "Final Formula" for more information. The policy cache data will always be in memory after Security Module startup. The size is statically predictable based on policy data. There could be multiple application policies bound to single Security Module, so the memory size need to multiply bound application number.
- **For authorization process memory usage.** This part is dynamic, and affected by request frequency. The memory could be GCed after authorization process is done. There is no analysis on this part. The given buffer = 1.5 * runtime cache.
- **For policy distribution.** Policy distribution is the process to get policy data from a database policy store, write policy data to a local encrypted XML policy file, and switch between two copies of the runtime policy cache.
 - Flush distribution will occur for the first time, or there will be too many changes that are not picked by the Security Module
 - Incremental distribution will occur when PDP already had the policy distributed, and small size changes occurred in the policy store

Regular authorization memory requirement is computed as (1) + (2) = **2.5* runtime cache.**

Initialization time to get flush policy distribution is computed as $[[\text{Runtime Cache}] * (2 + 3.67 * \text{App Count}) * 1.2 * 1.33] + 256 \text{ MB}$

As flush distribution requires more memory, use the $[[\text{Runtime Cache}] * (2 + 3.67 * \text{App Count}) * 1.2 * 1.33] + 256 \text{ MB}$ formula to calculate the recommended memory size for the PDP.

App Count is the applications count bound to the Security Module instance.

Runtime Policy Cache Memory Sizing Based on Policy Artifacts

Create OES authorization policy artifacts based on business security requirements. The policy artifacts will be stored in the database security store (1), migrated between different type of security stores (XML file-based or RDBMS based) (2), managed and distributed by you via an Administration Server (3), and loaded in memory as a policy cache consumed by an OES Security Module (4).

Policy artifacts are listed below.

Table 16–6 Policy Artifacts

| Policy Artifact | Description |
|-------------------------|---|
| Resource Type | A Resource Type represents the type of a secured object. Metadata in small size. |
| Resource | A Resource is a protected component or object to which access is granted or denied. The number could be large. |
| Resource attributes | Attribute values assigned to resource. |
| Function Definition | Metadata for built-in functions, and custom plugin function. Small size data. |
| Attribute Definition | Metadata for attribute declaration. Small size data. |
| Application Role | |
| Application Role member | |
| Role Mapping Policy | A policy to assign application role(s) to user, group, on given resource(s), and given condition |
| Entitlement | A small set of resources and the associated actions needed to perform a task. |
| Principal | User, group, or application role used in a policy. The number is large and could vary with different applications. It is subset of total user/group in ID store. |
| Permission | Resource and associated actions used in a policy. The number is large, and could vary with different applications. |
| Assignment | Total number of resource * principals of all of the policy. |
| Authorization Policy | Authorization policy The number is large. The size of each policy could vary, as it might have complex condition, and multiple obligations. For complex policy, a factor is needed for sizing. |

Runtime Policy Cache is a memory representation of OES authorization policy. The size is made based on policy artifacts numbers.

Final Formula:

0.54K * Assignment Number +
 0.41K * Permission Number +
 0.72K * Grantee Number +
 0.044K * Resource Number * **Resource Attribute Factor** +
 0.85K * Policy Number * **Policy Factor**
 0.122K * Total application role memberships

Resource Attribute Factor defaults to 1 for the case without resource attribute.

Policy Factor defaults to 1 for the case policy without condition and obligations

Table 16–5 provides more information on the Security Module tuning attributes.

16.3.3.2 WebLogic Security Module

Edit the `DOMAIN_HOME/bin/startWeblogic.sh` script with all the JVM parameters as shown below. Note that the lines are before the line "`{JAVA_HOME}/bin/java {JAVA_VM} -version`":

```

JAVA_HOME="/scratch/example_user/tools/jdk1.6.0_31"
/home/user/jdk1.6.0_31
MEM_ARGS="-Xms6144m -Xmx6144m -Xmn1900m -XX:PermSize=128m -XX:MaxPermSize=1024m
-XX:+UseParallelGC "

```

Where:

-Xms6144m -Xmx6144m: Selects the initial and maximum memory sizes available to the JVM, respectively. These values are used for the JVM heap, which reserves memory for the runtime cache and transient policy data during distribution.

Properly tuning this parameter reduces the overhead of garbage collection, improving authorization response time and throughput. If its value is too low, it may result in an out of memory error or a lot of minor/full garbage collections.

-XX:PermSize: Selects the initial memory size available for the permanent generation data. Specifying 128 Mbytes eliminates the overhead of increasing this part of the heap for most of the scenarios.

-XX:MaxPermSize: Selects the maximum size of Permanent Generation. Specifying 1024 Mbytes eliminates possible out of memory error in case there are large custom permissions.

-XX:+UseParallelGC: Uses parallel garbage collection for scavenges. This collection algorithm is designed to maximize throughput while minimizing pauses and a suitable GC algorithm for the Security Module.

16.3.3.3 Java Security Module

Edit the `OES_CLIENT_HOME/oes_sm_instances/SM_NAME/run-j2se.sh` script by adding all the JVM parameters shown below into the last line:

```

${JAVA_HOME}/bin/java -Xms6144m -Xmx6144m -Xmn1900m -XX:PermSize=128m
-XX:MaxPermSize=1024m -XX:+UseParallelGC
-Doracle.security.jps.config=./config/jps-config.xml
-classpath ./: ./sm-config-tool.jar oracle.security.oes.tools.OESJ2SESampleApp PD

```

16.3.3.4 Web Service Security Module

Edit the `OES_CLIENT_HOME/oes_sm_instances/SM_NAME/startWSServer.sh` script, by adding all the JVM parameters as shown below. Note that the properties are added after the last `JAVA_OPT` line:

```
JAVA_OPT="$JAVA_OPT -Xms6144m -Xmx6144m -Xmn1900m -XX:PermSize=128m
-XX:MaxPermSize=1024m -XX:+UseParallelGC"
```

For PDP service configurations, refer to [Table 16–7](#) which lists available parameter for the Web Service Security Module.

Table 16–7 Web Service Security Module Parameters

| Web Service Security Module Parameters | Description |
|---|---|
| <code>oracle.security.jps.pdp.sm.IdentityCacheEnabled</code> | Flag to set if using identity cache. If not set, identity cache enabled by default |
| <code>oracle.security.jps.pdp.sm.IdentityMaxCacheSize</code> | Specify the maximum cache size. Its default value is 20000. Tuning this parameter according to number of all subjects. |
| <code>oracle.security.jps.pdp.sm.IdentityCacheEvictionPercentage</code> | Specifies percentage of identities that must be evicted when cache has reached the maximum size Its default value is 20 percentages. |
| <code>oracle.security.jps.pdp.sm.IdentityCachedEntryTTL</code> | Specifies time-to-live in seconds for a identity record in the cache. Its default value is 3600 seconds. |
| <code>oracle.security.jps.pdp.wssm.WSLoggingSoapHandlerEnabled</code> | Flag to set if enable <code>EnvelopLoggingSOAPHandler</code> of Web Service Security Module. Its default value is false. |

16.3.3.5 Tomcat Security Module

Edit the `TOMCAT_HOME/bin/catalina.sh` script by adding all the following JVM parameters after the last `JAVA_OPTS` line:

```
JAVA_OPTS="$JAVA_OPTS -Xms6144m -Xmx6144m -Xmn1900m -XX:PermSize=128m
-XX:MaxPermSize=1024m -XX:+UseParallelGC"
```

16.3.4 Tuning OES Distribution Service

For PDP service configuration, add the following property

```
oracle.security.jps.pd.client.PollingTimerInterval:
```

This property specifies the PD periodic check interval. Its default value is 600 seconds. Depending on how often policy data is changed, it can be set to a smaller or larger value.

16.3.5 Tuning OES Attribute Retrievers

Out-of-the-box Attribute retrievers could be tuned for caching.

For information, refer to [Section B.3, "Configuring the Predefined Attribute Retrievers Manually."](#) For the instructions in [Section B.3.2, "Configuring Individual Attribute Values"](#), use the properties "ttl" (Time-to-live "ttl" in seconds of any cached attribute values when cached is enabled) and "cached" (enables the caching of attribute values).

16.3.6 Tuning OES Cache

Authorization decision caching allows Oracle Entitlements Server to cache the result of an authorization call and use that decision in the future, if an identical call is made.

For the Decision Cache in the Security Module, set the following properties in the `jps-config.xml` file of the PDP:

```
<property name="oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled"
value="true"/>
<property
name="oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionCapacity"
value="1500"/>
<property
name="oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage"
value="10"/>
<property name="oracle.security.jps.pdp.AuthorizationPerUserDecisionCacheSize"
value="1500"/>
<property name="oracle.security.jps.pdp.AuthorizationDecisionCacheTTL"
value="300"/>
```

Table 16–8 describes details of the above configurations.

Table 16–8 Tuning OES Cache Example Configuration

| Property | Description | Default | Recommended |
|--|---|---------|--|
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionCapacity | This is the number that is used to evict the decision cache if the decision cache size reaches this size. | 500 | Tuning this parameter according to number of concurrent users making authorization requests. |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage | The percentage of authorization decisions to drop when the decision cache has reached the maximum capacity. | 10 | |
| oracle.security.jps.pdp.AuthorizationPerUserDecisionCacheSize | This is the number that is used to evict the decision cache of each user (Subject) if the second level decision cache size reaches this size. Tuning this parameter according to number of all subjects. | 1000 | How many authorization results to be cached for single user |

Table 16–8 (Cont.) Tuning OES Cache Example Configuration

| Property | Description | Default | Recommended |
|---|--|------------|-------------|
| oracle.security.jps.pdp.AuthorizationDecisionCacheTTL | This is the TTL for the Decision Cache in seconds. | 60 seconds | |

16.3.7 Tuning Resource Intensive Operations

Use `PepRequestFactory.newQueryPepRequest().decide()` to query access on extremely large number of child resources (for example, > 100) for Security Module instances in the controlled distribution mode.

This feature is disabled by default, but you can enable it for Security Module instances in the controlled distribution mode.

To enable it, update the `jps-config.xml` file of the Security Module instances to add the following property for the PDP service instance:

```
<serviceInstance name="pdp.service" provider="pdp.service.provider">
    ... ..
    <property name="oracle.security.jps.runtime.enableResourcePermissionCache"
value="true"/>
```

16.3.8 Enabling Logging

This section contains the following topics:

- [Enable Logging for Performance Measurement](#)
- [Enable Logging for Snapshot Generation Measurement](#)
- [Enable Logging for Migration Performance Measurement](#)

16.3.8.1 Enable Logging for Performance Measurement

Logs are required for performance measurement for some key operations, including migration, snapshot generation, and distribution.

There is a log at the INFO level for migration via WLST. You could see logs with the timestamp printed to the WLST console directly. Refer to the example below:

```
Apr 19, 2013 3:07:00 AM
oracle.security.jps.internal.tools.utility.JpsUtilMigrationPolicyImpl
migrateAppPolicyData
INFO: Migration of Application Policies in progress....
... ..
Apr 19, 2013 3:07:39 AM
oracle.security.jps.internal.tools.utility.util.JpsMigrateUtil cloneResourceType
INFO: Migration of Resources started
Apr 19, 2013 3:08:12 AM
oracle.security.jps.internal.tools.utility.util.JpsMigrateUtil cloneResourceType
INFO: Migration of Resources completed in 00:00:33
... ..
Apr 19, 2013 3:08:44 AM
oracle.security.jps.internal.tools.utility.util.JpsMigrateUtil clonePermissionSet
INFO: Migration of Permission Sets completed in 00:00:31
... ..
Apr 19, 2013 3:11:35 AM
oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstPolicy clone
INFO: Completed Migrating 5,351 policies in [170,914] ms.
... ..
```

```

Apr 19, 2013 3:20:57 AM
oracle.security.jps.internal.tools.utility.destination.apibased.JpsDstPolicy clone
INFO: Migration of Grants completed in 00:09:22
... ..
Apr 19, 2013 3:20:57 AM
oracle.security.jps.internal.tools.utility.JpsUtilMigrationPolicyImpl
migrateAppPolicyData
INFO: Migration of Application Policies completed, Time taken for migration is
00:13:57

```

16.3.8.2 Enable Logging for Snapshot Generation Measurement

Create a Java logging.properties file with the log level setting shown below:

```

handlers= java.util.logging.FileHandler
.level= INFO
#####
# Handler specific properties.
# Describes specific configuration info for Handlers.
##### default file output
is in user's home directory.
java.util.logging.FileHandler.pattern =<Log_home>/performance.log
java.util.logging.FileHandler.limit = 10000000
java.util.logging.FileHandler.count = 200
java.util.logging.FileHandler.formatter =java.util.logging.SimpleFormatter
java.util.logging.FileHandler.level = FINE
java.util.logging.ConsoleHandler.level = INFO
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter
#####
# Facility specific properties.
#####
# Provides extra control for each logger.
#####
# For example, set the com.xyz.foo logger to only log SEVERE
# messages:
oracle.security.jps.internal.policystore.SnapshotWorker.level=FINEST

```

To enable the log, edit the *DOMAIN_HOME/bin/startWeblogic.sh* script as follows:

```

${JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS}
-Djava.util.logging.config.file=./logging.properties
-Dweblogic.Name=${SERVER_NAME}
-Djava.security.policy=${WL_HOME}/server/lib/weblogic.policy ${JAVA_OPTIONS}
${PROXY_SETTINGS} ${SERVER_CLASS}

```

From the log file, the following log message is shown when the snapshot is generated for the application policy:

```

Jan 31, 2013 1:07:49 AM oracle.security.jps.internal.policystore.SnapshotWorker
run
FINE: SnapshotWorker begin.
.....
Jan 31, 2013 1:12:43 AM oracle.security.jps.internal.policystore.SnapshotWorker
run
FINE: SnapshotWorker end.

```

16.3.8.3 Enable Logging for Migration Performance Measurement

Create logging.properties file like above section, and add following line:

```

oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet.level=FINEST

```

You will need to update a different script for different Security Module types.

Java Security Module

Edit the java Security Module start scripts to add the log properties. Refer to *OES_CLIENT_HOME/oes_sm_instances/SM_NAME/run-j2se.sh* as an example:

```
{JAVA_HOME}/bin/java -Doracle.security.jps.config=${OES_INSTANCE_
HOME}/config/jps-config.xml
${MEM_ARGS} -Djava.util.logging.config.file=./config/logging.properties
oracle.security.oes.tools.OESJ2SESampleApp PD
```

and enable the following in the log property file:

```
oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet.level=FINEST
```

Web Service Security Module

In the *OESCLIENT/oes_sm_instances/wssm/startWSServer.sh* script, add the following line:

```
JAVA_OPT="$JAVA_OPT -Djava.util.logging.config.file=./config/logging.properties".
```

WebLogic Security Module

Edit the *DOMAIN_HOME/bin/startWeblogic.sh* script at the end with the following:

```
{JAVA_HOME}/bin/java ${JAVA_VM} ${MEM_ARGS}
-Djava.util.logging.config.file=./config/logging.properties
```

Tomcat Security Module

Edit the *TOMCAT_HOME/bin/catalina.sh* script by adding the following line after the last *JAVA_OPTS* line:

```
JAVA_OPTS="$JAVA_OPTS
-Djava.util.logging.config.file=./config/logging.properties".
```

Log Messages

You can use the log messages with time stamp to obtain the time spent on policy distribution, from "starting" to "afterCommit finished". The following is an example message:

```
Jan 31, 2013 10:11:19 PM
oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet commit
FINE: Starting ...
.....
Jan 31, 2013 10:20:06 PM
oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet commit
FINE: completed. Active Apps: [[]], Bounded Apps [[FinanceApp]]
Jan 31, 2013 10:20:07 PM
oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet commit
FINE: afterCommit is finished
Jan 31, 2013 10:20:07 PM
oracle.security.jps.az.internal.runtime.pd.receiver.UpdatePolicySet
finishFirstDist
```

Installation and Configuration Parameters

This appendix lists the parameters and accepted values that may be defined for Oracle Entitlements Server services using `jps-config.xml`, the configuration file used by Java EE containers. It is located in the `$DOMAIN_HOME/config/fmwconfig` directory. This appendix is comprised of the following sections.

- Section A.1, "Policy Distribution Configuration"
- Section A.2, "Security Module Configuration"
- Section A.3, "PDP Proxy Client Configuration"
- Section A.4, "Policy Store Service Configuration"

A.1 Policy Distribution Configuration

The Policy Distribution Component is responsible for distributing policy objects and policies from the policy store to one or more Security Modules. It can distribute in a controlled-push mode, a controlled-pull mode, a non-controlled mode, or a mixed mode. Each mode entails different configurations.

- Section A.1.1, "Policy Distribution Component Server Configuration"
- Section A.1.2, "Policy Distribution Component Client Configuration"

A.1.1 Policy Distribution Component Server Configuration

Typically, configuration for the Policy Distribution Component to fetch policies and policy objects (in a scenario when it runs within Oracle Entitlements Server) is associated with the Policy Store configuration in the `jps-config.xml` file. Only in cases when data is pulled in a controlled manner (*controlled-pull mode*) is the Policy Distribution Component associated with the PDP Service configuration on the Security Module side. Table A-1 contains the configuration parameters.

Table A-1 Policy Distribution Server Configuration

| Parameter Name | Information | Console Name |
|--|--|--------------|
| oracle.security.jps.pd.server.transactionalScope | <p>Defines the scope of the policy distribution as either to one Security Module or to all Security Modules. If distribution fails when it involves only one Security Module, it does not affect distributions to other Security Modules.</p> <p>Optional</p> <p>Accepted Values: All (default), One</p> | none |

Table A–1 (Cont.) Policy Distribution Server Configuration

| Parameter Name | Information | Console Name |
|---|---|--------------|
| oracle.security.jps.register.waiting.interval | <p>Defines the amount of time to delay policy distribution after a request for registration is received.</p> <p>Optional</p> <p>Accepted Values: time in seconds (default value is 0)</p> | none |

A.1.2 Policy Distribution Component Client Configuration

The Policy Distribution Component client is responsible for making policies available to the Security Module. Thus, the Policy Distribution Client configuration is always associated with the PDP Service configuration portion of the `jps-config.xml` file on the Security Module side. Configuration is different depending on the mode of distribution and the environment in which the Security Module is running. The following sections contain descriptions of the applicable configuration parameters.

- [Section A.1.2.1, "Policy Distribution Component Client Java Standard Edition Configuration \(Controlled Push Mode\)"](#)
- [Section A.1.2.2, "Policy Distribution Component Client Java Enterprise Edition Container Configuration \(Controlled Push Mode\)"](#)
- [Section A.1.2.3, "Policy Distribution Client Configuration \(Controlled-Pull Mode\)"](#)
- [Section A.1.2.4, "Policy Distribution Client Configuration \(Non-controlled Mode\)"](#)
- [Section A.1.2.5, "Policy Distribution Client Configuration \(Mixed Mode\)"](#)

A.1.2.1 Policy Distribution Component Client Java Standard Edition Configuration (Controlled Push Mode)

[Table A–2](#) compiles the parameters for the Policy Distribution Component client configuration when the Oracle Entitlements Server is running in a Java Standard Edition (JSE) environment and is configured to distribute data in the controlled-push mode.

Table A–2 Policy Distribution Client Configuration, JSE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|--|---|--------------------------|
| oracle.security.jps.runtime.pd.client.policyDistributionMode | <p>Specifies the mode of policy distribution. <i>Controlled distribution</i> is initiated by the Policy Distribution Component, ensuring that the Security Module receives policy data that has been created or modified since the last distribution.</p> <p>Mandatory</p> <p>Accepted Value: controlled-push</p> | Policy Distribution Mode |
| oracle.security.jps.runtime.pd.client.sm_name | <p>Defines the name of the Security Module.</p> <p>Mandatory</p> <p>Accepted Value: Name of the Security Module</p> | SM Name |

Table A–2 (Cont.) Policy Distribution Client Configuration, JSE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|--|-----------------------------|
| oracle.security.jps.runtime.pd.client.localpolicy.work_folder | <p>Defines the name of any directory in which local cache files are stored. If a value is not defined, a work directory will be created in the directory where <code>jps-config.xml</code> is kept. If the applicable Security Module is created in a JRF domain, the server name will be used to create a sub directory under the specified or default work folder which will be used as the actual work folder.</p> <p>Optional</p> <p>Accepted Value: The name of any directory in which local cache files will be stored. This directory must have read and write privileges.</p> | Local Policy Work Folder |
| oracle.security.jps.runtime.pd.client.incrementalDistribution | <p>Defines whether the distribution is incremental or flush. <i>Incremental distribution</i> is when only new and modified data is distributed. <i>Flush distribution</i> is when the Policy Distribution Component notifies the Security Module to cleanup locally stored policies in preparation for a complete re-distribution of all policy objects in the policy store.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false (policy distribution is flush for this Security Module) ▪ true (default value; policy distribution is incremental for this Security Module if the required change logs are kept in the policy store) | Incremental Distribution |
| oracle.security.jps.runtime.pd.client.registrationRetryInterval | <p>When a Security Module starts, it registers itself with the Policy Distribution Component to ensure the local policy cache is up to date. If registration fails, it will retry each time this interval of time passes until successful.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 5)</p> | Registration Retry Interval |

Table A–2 (Cont.) Policy Distribution Client Configuration, JSE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|--|----------------------------------|
| oracle.security.jps.runtime.policyDistributionWaitTime | <p>If this value is defined and not equal to zero, it specifies the amount of time that a Security Module will wait for initial policy distribution to happen. During this wait period, authorization requests are blocked until either the initial policy distribution completes or the configured period expires.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 60)</p> | Wait Distribution Time (seconds) |
| oracle.security.jps.runtime.pd.client.RegistrationServerURL | <p>Defines the URL of the Oracle Entitlements Server Administration Server. Used by the Security Module to register itself with Oracle Entitlements Server when it starts.</p> <p>Mandatory</p> <p>Accepted Value: URL</p> | Registration Server URL |
| oracle.security.jps.runtime.pd.client.backupRegistrationServerURL | <p>Defines a backup URL for the Oracle Entitlements Server Administration Server. Used by the Security Module to register itself with Oracle Entitlements Server when it starts if the primary URL (parameter above) is unavailable.</p> <p>Optional (although if not configured Oracle Entitlements Server failover will not work)</p> <p>Accepted Value: URL</p> | Backup Registration Server URL |
| oracle.security.jps.runtime.pd.client.DistributionServicePort | <p>Defines the port to which a remote Policy Distributor will push policy updates.</p> <p>Mandatory</p> <p>Accepted Value: port number</p> | Distribution Service Port |
| oracle.security.jps.pd.client.sslMode | <p>Defines whether communication between the Policy Distribution Component server and client will use the Secure Sockets Layer (SSL) protocol or not.</p> <p>Mandatory</p> <p>Accepted Values: none, two-way (default value)</p> | SSL Mode |
| oracle.security.jps.pd.client.ssl.identityKeyStoreFileName | <p>Defines the name of the Identity Key Store file in which client certificates are stored. Used for SSL communication between the Security Module and the Policy Distribution Component.</p> <p>Mandatory</p> <p>Accepted Value: the name of the keystore file</p> | SSL Identity Key Store File Name |

Table A–2 (Cont.) Policy Distribution Client Configuration, JSE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|--|---|
| oracle.security.jps.pd.client.ssl.trustKeyStoreFileName | <p>Defines the name of the Trust Key Store file where Certificate Authority (CA) certificates are stored. Used for SSL communication between the Security Module and the Policy Distribution Component.</p> <p>Mandatory</p> <p>Accepted Value: the name of the identity key store file</p> | SSL Trust Key Store File Name |
| oracle.security.jps.pd.client.ssl.identityKeyStoreKeyAlias | <p>Defines an Identity Key alias to identify the client certificate used for SSL communication between the Security Module and the Policy Distribution Component.</p> <p>Optional (if only one alias exists in the identity keystore there is no need to specify this value)</p> <p>Accepted Value: the identity key alias</p> | SSL Identity Key Store Key Alias |
| oracle.security.jps.runtime.pd.client.SMinstanceType | <p>Defines the type of Security Module to which the Policy Distribution Component client is connecting.</p> <p>Mandatory</p> <p>Accepted Value: java (Other accepted values include wls, RMI and ws. Because this table covers the Java Security Module only, the value must be java.)</p> | Configured during OES Client installation only. |
| oracle.security.jps.runtime.pd.client.localpolicy.JCEProviderName | <p>Defines which JCE provider will be used.</p> <p>Optional</p> <p>Accepted Values: SunJCE, JsafeJCE; no default value is defined. The value is case-sensitive. If no value is provided, the default JDK provider is used.</p> | |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherKeyLength | <p>Defines the key length used for the Cipher class available from the specified JCE provider.</p> <p>Optional</p> <p>Accepted Values: 128, 192, 256; default value is 128.</p> | |

Table A–2 (Cont.) Policy Distribution Client Configuration, JSE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|---|--------------|
| oracle.security.jps.runtime.pd.client.localpolicy.CipherModePadding | <p>Defines a cipher algorithm name, mode and padding schema used for the Cipher class available from the specified JCE provider. It is not case-sensitive. The format should be:</p> <p><i>algorithm name/mode/padding</i></p> <p>Optional</p> <p>Accepted Values: default value is AES/CBC/PKCS5Padding; others include AES/CBC/PKCS5Padding or AES/GCM/NoPadding.</p> | |

A.1.2.2 Policy Distribution Component Client Java Enterprise Edition Container Configuration (Controlled Push Mode)

Table A–3 compiles the parameters for the Policy Distribution Component client configuration when the Oracle Entitlements Server is running in a Java Enterprise Edition (JEE) environment and is configured to distribute data in the controlled-push mode.

Table A–3 Policy Distribution Client Configuration, JEE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|--|---|--------------------------|
| oracle.security.jps.runtime.pd.client.policyDistributionMode | <p>Specifies the mode of policy distribution. <i>Controlled distribution</i> is initiated by the Policy Distribution Component, ensuring that the Security Module receives policy data that has been created or modified since the last distribution.</p> <p>Mandatory</p> <p>Accepted Value: controlled-push</p> | Policy Distribution Mode |
| oracle.security.jps.runtime.pd.client.sm_name | <p>Defines the name of the Security Module.</p> <p>Mandatory</p> <p>Accepted Value: Name of the Security Module</p> | SM Name |

Table A-3 (Cont.) Policy Distribution Client Configuration, JEE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|---|---------------------------------------|
| oracle.security.jps.runtime.pd.client.localpolicy.work_folder | <p>Defines the name of any directory in which local cache files are stored. If a value is not defined, a work directory will be created in the directory where <code>jps-config.xml</code> is kept. If the applicable Security Module is created in a JRF domain, the server name will be used to create a sub directory under the specified or default work folder which will be used as the actual work folder.</p> <p>Optional</p> <p>Accepted Value: The name of any directory in which local cache files will be stored. This directory must have read and write privileges.</p> | Local Policy Work Folder |
| oracle.security.jps.runtime.pd.client.incrementalDistribution | <p>Defines whether the distribution is incremental or flush. <i>Incremental distribution</i> is when new and modified data is distributed. <i>Flush distribution</i> is when the Policy Distribution Component notifies the Security Module to cleanup locally stored policies in preparation for a complete re-distribution of all policy objects in the policy store.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false (policy distribution is flush for this Security Module) ▪ true (default value; policy distribution is incremental for this Security Module if the required change logs are kept in the policy store) | Incremental Distribution |
| oracle.security.jps.runtime.pd.client.registrationRetryInterval | <p>When a Security Module starts, it registers itself with the Policy Distribution Component to ensure the local policy cache is up to date. If registration fails, it will retry each time this interval of time passes until successful.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 5)</p> | Registration Retry Interval (seconds) |

Table A-3 (Cont.) Policy Distribution Client Configuration, JEE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|--|---|
| oracle.security.jps.runtime.policyDistributionWaitTime | <p>If this value is defined and not equal to zero, it specifies the amount of time that a Security Module will wait for initial policy distribution to happen. During this wait period, authorization requests are blocked until either the initial policy distribution completes or the configured period expires.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 60)</p> | Wait Distribution Time (seconds) |
| oracle.security.jps.runtime.pd.client.RegistrationServerURL | <p>Defines the URL of the Oracle Entitlements Server Administration Server. Used by the Security Module to register itself with Oracle Entitlements Server when it starts.</p> <p>Mandatory</p> <p>Accepted Value: URL</p> | Registration Server URL |
| oracle.security.jps.runtime.pd.client.backupRegistrationServerURL | <p>Defines a backup URL for the Oracle Entitlements Server Administration Server. Used by the Security Module to register itself with Oracle Entitlements Server when it starts if the primary URL (parameter above) is unavailable.</p> <p>Optional (although if not configured Oracle Entitlements Server failover will not work)</p> <p>Accepted Value: URL</p> | Backup Registration Server URL |
| oracle.security.jps.runtime.pd.client.SMInstanceType | <p>Defines the type of Security Module to which the Policy Distribution Component client is connecting.</p> <p>Mandatory</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ■ was ■ wls | Configured during OES Client installation only. |
| oracle.security.jps.runtime.pd.client.DistributionServiceURL | <p>Defines the URL to which the remote Policy Distributor will push policy updates.</p> <p>Mandatory</p> <p>Accepted Values: URL</p> | |

Table A–3 (Cont.) Policy Distribution Client Configuration, JEE, Controlled Push Mode

| Parameter Name | Information | Console Name |
|---|--|--------------|
| oracle.security.jps.runtime.pd.client.localpolicy.JCEProviderName | Defines which JCE provider will be used. It is optional and case sensitive. Optional Accepted Values: SunJCE, JsafeJCE; no default value is defined. If no value is provided, the default JDK provider is used. | |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherKeyLength | Defines the key length used for the Cipher class available from the specified JCE provider. Optional Accepted Values: 128, 192, 256; default value is 128. | |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherModePadding | Defines a cipher algorithm name, mode and padding schema used for the Cipher class available from the specified JCE provider. It is not case-sensitive. The format should be: <i>algorithm name/mode/padding</i> Optional Accepted Values: default value is AES/CBC/PKCS5Padding; others include AES/CBC/PKCS5Padding or AES/GCM/NoPadding. | |

A.1.2.3 Policy Distribution Client Configuration (Controlled-Pull Mode)

Table A–4 compiles the parameters for the Policy Distribution Component client configuration when the Oracle Entitlements Server is running in either a JEE or a JSE environment and is configured to distribute data in the controlled-pull mode.

Table A–4 Policy Distribution Client Configuration, Controlled-Pull Mode

| Parameter Name | Information | Console Name |
|--|--|--------------------------|
| oracle.security.jps.runtime.pd.client.policyDistributionMode | Specifies the mode of policy distribution. <i>Controlled distribution</i> is initiated by the Policy Distribution Component, ensuring that the Security Module receives policy data that has been created or modified since the last distribution. Mandatory Accepted Value: controlled-pull | Policy Distribution Mode |
| oracle.security.jps.runtime.pd.client.sm_name | Defines the name of the Security Module. Mandatory Accepted Value: the name of the Security Module | SM Name |

Table A–4 (Cont.) Policy Distribution Client Configuration, Controlled-Pull Mode

| Parameter Name | Information | Console Name |
|---|--|----------------------------------|
| oracle.security.jps.runtime.pd.client.localpolicy.work_folder | <p>Defines the name of any directory in which local cache files are stored. If a value is not defined, a work directory will be created in the directory where <code>jps-config.xml</code> is kept. If the applicable Security Module is created in a JRF domain, the server name will be used to create a sub directory under the specified or default work folder which will be used as the actual work folder.</p> <p>Optional</p> <p>Accepted Value: The name of any directory in which local cache files will be stored. This directory must have read and write privileges.</p> | Local Policy Work Folder |
| oracle.security.jps.runtime.pd.client.incrementalDistribution | <p>Defines whether the distribution is incremental or flush. <i>Incremental distribution</i> is when new and modified data is distributed. <i>Flush distribution</i> is when the Policy Distribution Component notifies the Security Module to cleanup locally stored policies in preparation for a complete re-distribution of all policy objects in the policy store.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false (policy distribution is flush for the Security Module) ▪ true (default value; policy distribution is incremental for this Security Module if the required change logs are kept in the policy store) | Incremental Distribution |
| oracle.security.jps.runtime.policyDistributionWaitTime | <p>If this value is defined and not equal to zero, it specifies the amount of time that a Security Module will wait for initial policy distribution to happen. During this wait period, authorization requests are blocked until either the initial policy distribution completes or the configured period expires.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 60)</p> | Wait Distribution Time (seconds) |

Table A–4 (Cont.) Policy Distribution Client Configuration, Controlled-Pull Mode

| Parameter Name | Information | Console Name |
|--|---|----------------------|
| oracle.security.jps.pd.client.PollingTimerEnabled | <p>Enables a periodic check for policy updates in the Policy Store. Can be set to false to disable polling for environment when policies are not expected to be modified.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false ▪ true (default value) | |
| oracle.security.jps.pd.client.PollingTimerInterval | <p>Defines the interval of time in which the Policy Distribution Component will check for policy data changes.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value of 600)</p> | |
| oracle.security.jps.ldap.root.name | <p>Defines the top (root) entry of the LDAP policy store directory information tree (DIT).</p> <p>Mandatory</p> <p>Accepted Value: the top (root) entry of the LDAP policy store directory information tree (DIT)</p> | LDAP Root Name |
| oracle.security.jps.farm.name | <p>Defines the RDN format of the domain node in the LDAP policy store.</p> <p>Mandatory</p> <p>Accepted Value: name of the domain</p> | Farm Name |
| jdbc.url | <p>Takes a URL that points to the database.</p> <p>Mandatory (if using Java Database Connectivity API to connect to policy store)</p> <p>Accepted Value: URL</p> | JDBC URL |
| jdbc.driver | <p>Location of the driver if using Java Database Connectivity API to connect to an Apache Derby database.</p> <p>Mandatory</p> <p>Accepted Value: driver</p> | JDBC Driver |
| datasource.jndi.name | <p>The JNDI name of the JDBC data source instance. The instance may correspond to a single source or multi-source datasource. Valid in only JEE applications. Applies only to database stores.</p> <p>Mandatory</p> <p>Accepted Value: name of JNDI data source; for example, jdbc/APMDBDS.</p> | Datasource JNDI Name |

Table A-4 (Cont.) Policy Distribution Client Configuration, Controlled-Pull Mode

| Parameter Name | Information | Console Name |
|---|--|----------------------------------|
| security.principal | The name of the user with access rights to the database. Mandatory Accepted Value: Database user name | |
| security.credential | The password of the user with access rights to the database. Optional Accepted Value: Password associated with the database user in clear text; instead of storing the password in clear text, use <code>bootstrap.security.principal.map</code> . | |
| bootstrap.security.principal.key | The key for the password credentials to access the policy store. Credentials are stored in the Credential Store Framework (CSF) store. Mandatory Accepted Value: CSF credential key | Bootstrap Security Principal Key |
| bootstrap.security.principal.map | The map for the password credentials to access the policy store. Credentials are stored in the CSF store. Mandatory Accepted Value: name of the CSF credential map | Bootstrap Security Principal Map |
| oracle.security.jps.runtime.pd.client.localpolicy.JCEProviderName | Defines which JCE provider will be used. It is optional and case sensitive. Optional Accepted Values: SunJCE, JsafeJCE; no default value is defined. If no value is provided, the default JDK provider is used. | |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherKeyLength | Defines the key length used for the Cipher class available from the specified JCE provider. Optional Accepted Values: 128, 192, 256; default value is 128. | |

Table A–4 (Cont.) Policy Distribution Client Configuration, Controlled-Pull Mode

| Parameter Name | Information | Console Name |
|---|---|--------------|
| oracle.security.jps.runtime.pd.client.localpolicy.CipherModePadding | <p>Defines a cipher algorithm name, mode and padding schema used for the Cipher class available from the specified JCE provider. It is not case-sensitive. The format should be:</p> <p><i>algorithm name/mode/padding</i></p> <p>Optional</p> <p>Accepted Values: default value is AES/CBC/PKCS5Padding; others include AES/CBC/PKCS5Padding or AES/GCM/NoPadding.</p> | |

A.1.2.4 Policy Distribution Client Configuration (Non-controlled Mode)

Table A–5 compiles the parameters for Policy Distribution Component client configuration when the Oracle Entitlements Server is running in either a JEE or a JSE environment and is configured to distribute data in the non-controlled mode.

Table A–5 Policy Distribution Client Configuration, Non-controlled Mode

| Parameter Name | Information | Console Name |
|--|---|--------------------------|
| oracle.security.jps.runtime.pd.client.policyDistributionMode | <p>Specifies the mode of policy distribution. <i>Non-controlled distribution</i> is when the Security Module periodically retrieves policy data from a policy store (or from a component that serves as an intermediary between the two).</p> <p>Optional</p> <p>Accepted Value: non-controlled (default value)</p> | Policy Distribution Mode |

A.1.2.5 Policy Distribution Client Configuration (Mixed Mode)

Table A–4 compiles the parameters for the Policy Distribution Component client configuration when the PDP is running in either a JEE or a JSE environment and is configured to distribute data in mixed mode. Mixed mode is a distribution combination of controlled-pull and uncontrolled mode.

Table A–6 Policy Distribution Client Configuration, Mixed Mode

| Parameter Name | Information | Console Name |
|--|---|--------------------------|
| oracle.security.jps.runtime.pd.client.policyDistributionMode | <p>Specifies the mode of policy distribution. <i>Controlled distribution</i> is initiated by the Policy Distribution Component, ensuring that the Security Module receives policy data that has been created or modified since the last distribution.</p> <p>Mandatory</p> <p>Accepted Value: mixed</p> | Policy Distribution Mode |

Table A–6 (Cont.) Policy Distribution Client Configuration, Mixed Mode

| Parameter Name | Information | Console Name |
|---|--|----------------------------------|
| oracle.security.jps.runtime.pd.client.sm_name | <p>Defines the name of the Security Module.</p> <p>Mandatory</p> <p>Accepted Value: the name of the Security Module</p> | SM Name |
| oracle.security.jps.runtime.pd.client.localpolicy.work_folder | <p>Defines the name of any directory in which local cache files are stored. If a value is not defined, a work directory will be created in the directory where <code>jps-config.xml</code> is kept. If the applicable Security Module is created in a JRF domain, the server name will be used to create a sub directory under the specified or default work folder which will be used as the actual work folder.</p> <p>Optional</p> <p>Accepted Value: The name of any directory in which local cache files will be stored. This directory must have read and write privileges.</p> | Local Policy Work Folder |
| oracle.security.jps.runtime.pd.client.incrementalDistribution | <p>Defines whether the distribution is incremental or flush. <i>Incremental distribution</i> is when new and modified data is distributed. <i>Flush distribution</i> is when the Policy Distribution Component notifies the Security Module to cleanup locally stored policies in preparation for a complete re-distribution of all policy objects in the policy store.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false (policy distribution is flush for the Security Module) ▪ true (default value; policy distribution is incremental for this Security Module if the required change logs are kept in the policy store) | Incremental Distribution |
| oracle.security.jps.runtime.policyDistributionWaitTime | <p>If this value is defined and not equal to zero, it specifies the amount of time that a Security Module will wait for initial policy distribution to happen. During this wait period, authorization requests are blocked until either the initial policy distribution completes or the configured period expires.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 60)</p> | Wait Distribution Time (seconds) |

Table A–6 (Cont.) Policy Distribution Client Configuration, Mixed Mode

| Parameter Name | Information | Console Name |
|---|---|------------------------|
| oracle.security.jps.pd.client.PollingTimerEnabled | <p>Enables a periodic check for policy updates in the Policy Store. Can be set to false to disable polling for environment when policies are not expected to be modified.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ■ false ■ true (default value) | Polling Timer |
| oracle.security.jps.pd.client.PollingTimerInterval | <p>Defines the interval of time in which the Policy Distribution Component will check for policy data changes.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value of 600)</p> | Polling Timer Interval |
| oracle.security.jps.runtime.pd.client.localpolicy.JCEProviderName | <p>Defines which JCE provider will be used. It is optional and case sensitive.</p> <p>Optional</p> <p>Accepted Values: SunJCE, JsafeJCE; no default value is defined. If no value is provided, the default JDK provider is used.</p> | N/A |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherKeyLength | <p>Defines the key length used for the Cipher class available from the specified JCE provider.</p> <p>Optional</p> <p>Accepted Values: 128, 192, 256; default value is 128.</p> | N/A |
| oracle.security.jps.runtime.pd.client.localpolicy.CipherModePadding | <p>Defines a cipher algorithm name, mode and padding schema used for the Cipher class available from the specified JCE provider. It is not case-sensitive. The format should be:</p> <p><i>algorithm name/mode/padding</i></p> <p>Optional</p> <p>Accepted Values: default value is AES/CBC/PKCS5Padding; others include AES/CBC/PKCS5Padding or AES/GCM/NoPadding.</p> | N/A |
| <p>In Mixed Mode, the following nine properties should be configured for the Policy Store and not the Security Module. See Section A.4, "Policy Store Service Configuration."</p> | | |
| oracle.security.jps.ldap.root.name | <p>Defines the top (root) entry of the LDAP policy store directory information tree (DIT).</p> <p>Mandatory</p> <p>Accepted Value: the top (root) entry of the LDAP policy store directory information tree (DIT)</p> | LDAP Root Name |

Table A–6 (Cont.) Policy Distribution Client Configuration, Mixed Mode

| Parameter Name | Information | Console Name |
|----------------------------------|---|----------------------------------|
| oracle.security.jps.farm.name | <p>Defines the RDN format of the domain node in the LDAP policy store.</p> <p>Mandatory</p> <p>Accepted Value: name of the domain</p> | Farm Name |
| jdbc.url | <p>Takes a URL that points to the database.</p> <p>Mandatory (if using Java Database Connectivity API to connect to policy store)</p> <p>Accepted Value: URL</p> | JDBC URL |
| jdbc.driver | <p>Location of the driver if using Java Database Connectivity API to connect to an Apache Derby database.</p> <p>Mandatory</p> <p>Accepted Value: driver</p> | JDBC Driver |
| datasource.jndi.name | <p>The JNDI name of the JDBC data source instance. The instance may correspond to a single source or multi-source datasource. Valid in only JEE applications. Applies only to database stores.</p> <p>Mandatory</p> <p>Accepted Value: name of JNDI data source; for example, jdbc/APMDBDS.</p> | Datasource JNDI Name |
| security.principal | <p>The name of the user with access rights to the database.</p> <p>Mandatory</p> <p>Accepted Value: Database user name</p> | Username |
| security.credential | <p>The password of the user with access rights to the database.</p> <p>Mandatory</p> <p>Accepted Value: Password associated with the database user</p> | Password |
| bootstrap.security.principal.key | <p>The key for the password credentials to access the policy store. Credentials are stored in the Credential Store Framework (CSF) store.</p> <p>Mandatory</p> <p>Accepted Value: CSF credential key</p> | Bootstrap Security Principal Key |

Table A–6 (Cont.) Policy Distribution Client Configuration, Mixed Mode

| Parameter Name | Information | Console Name |
|----------------------------------|--|----------------------------------|
| bootstrap.security.principal.map | The map for the password credentials to access the policy store. Credentials are stored in the CSF store. Mandatory Accepted Value: name of the CSF credential map | Bootstrap Security Principal Map |

A.2 Security Module Configuration

This section covers the configurations for the various types of Security Modules and their proxy clients.

- [Section A.2.1, "Java Security Module"](#)
- [Section A.2.2, "Web Services Security Module"](#)
- [Section A.2.3, "Web Services Security Module on WebLogic Server"](#)
- [Section A.2.4, "RMI Security Module"](#)
- [Section A.2.5, "WebLogic Server Security Module"](#)
- [Section A.2.6, "WebLogic Server Security Module Discovery Mode"](#)

A.2.1 Java Security Module

[Table A–7](#) compiles the parameters to configure the Java Security Module embedded in either a JSE or a JEE container.

Table A–7 Java Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|-----------------------|
| oracle.security.jps.policy.store.rolemember.cache.type | Defines the role member cache type. Valid in J2EE and J2SE applications. Applies to LDAP and database stores. Optional Accepted Values <ul style="list-style-type: none"> ■ SOFT (cleaning of a cache of this type relies on the garbage collector when there is a memory crunch) ■ WEAK (behavior of a cache of this type is similar to a cache of type SOFT but the garbage collector cleans it more frequently) ■ STATIC (default value; cache objects are statically cached and can be cleaned explicitly only according to the applied cache strategy, such as FIFO; the garbage collector does not clean a cache of this type) | Rolemember Cache Type |

Table A-7 (Cont.) Java Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|---|---|--------------------------------|
| oracle.security.jps.policy.store.rolemember.cache.strategy | <p>Defines the type of strategy used in the role member cache. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ NONE (all entries in the cache grow until a refresh or reboot occurs; there is no control over the size of the cache; not recommended but typically efficient when the policy footprint is very small) ▪ FIFO (default value; the cache implements the first-in-first-out strategy) | Rolemember Cache Strategy |
| oracle.security.jps.policy.store.rolemember.cache.size | <p>Defines the number of roles kept in the role member cache. Valid in J2EE and J2SE application. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Value: number (default value is 1000)</p> | Rolemember Cache Size |
| oracle.security.jps.policy.store.rolemember.cache.warmup.enable | <p>Controls the way the Application Role membership cache is created. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ true (the cache is created at server startup; use when the number of users and groups is significantly higher than the number of Application Roles) ▪ false (default value; the cache is created on demand - lazy loading; use when the number of Application Roles is very high) | Rolemember Cache Warmup Enable |
| oracle.security.jps.policy.store.policy.lazy.load.enable | <p>Enables or disables the policy lazy load. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ false ▪ true (default value) | Policy Lazy Load Enable |

Table A-7 (Cont.) Java Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|--------------------------------------|
| oracle.security.jps.policy.store.policy.cache.strategy | <p>Defines the type of strategy used in the permission cache. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ NONE (all entries in the cache grow until a refresh or reboot occurs; there is no control over the size of the cache; not recommended but typically efficient when the policy footprint is very small.) ▪ PERMISSION_FIFO (default value; the cache implements the first-in-first-out strategy) | Policy Cache Strategy |
| oracle.security.jps.policy.store.policy.cache.size | <p>Defines the number of permissions kept in the permission cache. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Value: number (default value is 1000)</p> | Policy Cache Size |
| oracle.security.jps.policy.store.cache.updateable | <p>Defines whether the policy cache is incrementally updated for management operations on policy data.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ false ▪ true (default value) | Policy Cache Updatable |
| oracle.security.jps.policy.store.refresh.enable | <p>Enables or disables the policy store refresh. If this property is set, <code>oracle.security.jps.ldap.cache.enable</code> cannot be set. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values:</p> <ul style="list-style-type: none"> ▪ false ▪ true (default value) | Refresh Enable |
| oracle.security.jps.policy.store.refresh.purge.timeout | <p>Defines the time in milliseconds after which the policy store cache is purged. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Value: time in milliseconds; default value is 43200000 which equals 12 hours</p> | Refresh Purge Timeout (milliseconds) |

Table A-7 (Cont.) Java Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|---------------------------------------|
| oracle.security.jps.ldap.policystore.refresh.interval | <p>Defines the interval of time in which the policy store is polled for changes. Valid in J2EE and J2SE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Value: time in milliseconds; default value is 600000 which equals 10 minutes</p> | Refresh Purge Interval (milliseconds) |
| oracle.security.jps.pdp.missingAppPolicyQueryTTL | <p>Defines the interval of time to avoid frequently querying a non-existent Application (<code>ApplicationPolicy</code>) object.</p> <p>Optional</p> <p>Accepted Value: time to live in milliseconds (default value is 60000)</p> | Missing App Policy Query TTL |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEnabled | <p>Specifies whether the authorization cache should be enabled. Valid in J2EE and J2SE applications. Applies to XML, LDAP, and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ■ false ■ true (default value) | Decision Cache Enabled |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionCapacity | <p>Defines the maximum number of authorization and role mapping sessions to maintain. When the maximum is reached, old sessions are dropped and reestablished when needed. Valid in J2EE and J2SE applications. Applies to XML, LDAP, and database stores.</p> <p>Optional</p> <p>Accepted Value: number (default value is 500)</p> | Decision Cache Eviction Capacity |
| oracle.security.jps.pdp.AuthorizationDecisionCacheEvictionPercentage | <p>Defines the percentage of sessions to drop when the eviction capacity is reached. Valid in J2EE and J2SE applications. Applies to XML, LDAP, and database stores.</p> <p>Optional</p> <p>Accepted Value: number (default value is 10)</p> | Decision Cache Eviction Percentage |
| oracle.security.jps.pdp.AuthorizationDecisionCacheTTL | <p>Defines the number of seconds during which session data is cached. Valid in J2EE and J2SE applications. Applies to XML, LDAP, and database stores.</p> <p>Optional</p> <p>Accepted Value: time in seconds (default value is 60)</p> | Decision Cache TTL (seconds) |

Table A–7 (Cont.) Java Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|---|---|---------------------------|
| oracle.security.jps.pdp.anonymousrole.enable | Specifies whether anonymous role has to be added to anonymous subject for policy matching. Optional Accepted Values <ul style="list-style-type: none"> ▪ false ▪ true (default value) | Anonymous Role Enable |
| oracle.security.jps.pdp.authenticatedrole.enable | Specifies whether authenticated role has to be added to authenticated subject for policy matching. Optional Accepted Values <ul style="list-style-type: none"> ▪ false ▪ true (default value) | Authenticated Role Enable |
| oracle.security.jps.pdp.ComputeAppRolesOnceOnBulkAtz | Specifies whether Application Roles should be computed only once within a single bulk authorization call. For example, if a client calls the <code>checkBulkAuthorization()</code> method and passes ten resources to it, the roles will be calculated once if the value is <i>true</i> or once for every individual resource (ten times) if the parameter is <i>false</i> . Optional Accepted Values <ul style="list-style-type: none"> ▪ false ▪ true (default value) | |
| oracle.security.jps.pdp.AuthorizationPerUserDecisionCacheSize | Specifies the maximum number of authorization decisions cached for each Subject; if the second level decision cache size reaches this size, decisions are evicted from the cache. Optional Accepted Value: number of decisions (default value is 1000) | |

A.2.2 Web Services Security Module

Table A–8 compiles the parameters to configure the Web Services Security Module embedded in either a JSE or a JEE container.

Table A–8 Web Services Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|--------------|
| oracle.security.jps.pdp.wssm.WSServiceRegistryPortNumber | Defines the port on which the Web Services Security Module listens. Mandatory Accepted Value: port number | |

Table A–8 (Cont.) Web Services Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|---|--|--------------|
| oracle.security.jps.pdp.wssm.WSServiceRegistryHost | <p>Defines the name of the server on which the Web Services Security Module is running.</p> <p>Optional</p> <p>Accepted Value: server name (default value is localhost)</p> | |
| oracle.security.jps.pdp.wssm.Protocol | <p>Defines the transport protocol used between the Policy Distribution Component client and server.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ https ▪ http (default value) | |
| oracle.security.jps.pdp.smm.IdentityCacheEnabled | <p>Specifies whether the identity cache is being used. The default value is true. If not set, identity cache is used by default.</p> <p>Optional</p> <p>Accepted Value: true/false</p> | |
| oracle.security.jps.pdp.smm.IdentityMaxCacheSize | <p>Specifies the maximum number of users for which information is cached. When the maximum is reached, old records are dropped and reestablished when needed.</p> <p>Optional</p> <p>Accepted Value: number</p> | |
| oracle.security.jps.pdp.smm.IdentityCacheEvictionPercentage | <p>Specifies percentage of identities that must be evicted when cache has reached the maximum size.</p> <p>Optional</p> <p>Accepted Value: number indicating percentage</p> | |
| oracle.security.jps.pdp.smm.IdentityCachedEntryTTL | <p>Specifies time-to-live of an identity cache record.</p> <p>Optional</p> <p>Accepted Value: time in seconds</p> | |
| oracle.security.jps.pdp.wssm.responseContext | <p>Specifies whether to merge data from many AppContext responses into a single AppContext response.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ Merged ▪ Unmerged (default value) | |

Table A–8 (Cont.) Web Services Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|---|---|--------------|
| oracle.security.jps.pdp.wssm.ssl.identityKeyStoreFileName | <p>Defines the name of the Identity Key Store file where client certificates are stored for the Web Services Security Module. Used for SSL communications between the remote client and the Web Services Security Module.</p> <p>Optional</p> <p>Accepted Value: name of the Identity Key Store file</p> | |
| oracle.security.jps.pdp.wssm.ssl.trustKeyStoreFileName | <p>Defines the name of the Trust Key Store file in which CA certificates are stored. Used for SSL communications between the remote client and the Web Services Security Module.</p> <p>Optional</p> <p>Accepted Value: name of the Trust Key Store file</p> | |
| oracle.security.jps.pdp.wssm.ssl.identityKeyStoreKeyAlias | <p>Specifies the Identity Key alias used to identify the Web Services Security Module client certificate used for SSL communication between the Web Services Security Module and the remote client.</p> <p>Accepted value: Identity key alias</p> <p>Optional</p> <p>Accepted Value: Identity Key alias</p> | |
| oracle.security.jps.pdp.wssm.WSLoggingSoapHandlerEnabled | <p>Enables the Web Services Security Module's EnvelopLoggingSOAPHandler, the web service SOAP message handler for logging.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ true ▪ false (default value) | |

A.2.3 Web Services Security Module on WebLogic Server

Table A–9 compiles the parameters to configure the Web Services Security Module on a WebLogic Server.

Table A–9 Web Services Security Module on WebLogic Configuration Parameters

| Parameter Name | Information | Console Name |
|--|--|--------------|
| oracle.security.jps.pdp.wssm.WSServiceRegistryPortNumber | <p>Defines the port on which the Web Services Security Module listens.</p> <p>Mandatory</p> <p>Accepted Value: port number</p> | |

Table A–9 (Cont.) Web Services Security Module on WebLogic Configuration

| Parameter Name | Information | Console Name |
|---|--|--------------|
| oracle.security.jps.pdp.wssm.WSServiceRegistryHost | <p>Defines the name of the server on which the Web Services Security Module is running.</p> <p>Optional</p> <p>Accepted Value: server name (default value is localhost)</p> | |
| oracle.security.jps.pdp.wssm.Protocol | <p>Defines the transport protocol used between the Policy Distribution Component client and server.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ https ▪ http (default value) | |
| oracle.security.jps.pdp.wssm.WSServiceRegistryContextName | <p>Specifies the context name for the Web service deployed on the WebLogic Server cache is being used. If not set, no identity cache is used by default.</p> <p>Mandatory</p> <p>Accepted Value: Ssmws</p> | |
| oracle.security.jps.pdp.ssm.IdentityCacheEnabled | <p>Specifies whether the identity cache is enabled. Enabled by default.</p> <p>Optional</p> <p>Accepted Value: true (default)/false</p> | |
| oracle.security.jps.pdp.ssm.IdentityMaxCacheSize | <p>Specifies the maximum size of the identity cache.</p> <p>Optional</p> <p>Accepted Value: number indicating size; default value is 20000</p> | |
| oracle.security.jps.pdp.ssm.IdentityCacheEvictionPercentage | <p>Specifies the percentage of identities that will be removed when the identity cache has reached its maximum size.</p> <p>Optional</p> <p>Accepted Value: 20 percent</p> | |
| oracle.security.jps.pdp.ssm.IdentityCachedEntryTTL | <p>Specifies the time-to-live (TTL) in seconds for an identity record in the identity cache.</p> <p>Optional</p> <p>Accepted Value: 3600 seconds (default)</p> | |
| oracle.security.jps.pdp.wssm.responseContext | <p>Specifies whether the AppContext is returned as a single response or a merged set of data from all the AppContext responses.</p> <p>Optional</p> <p>Accepted Value: Merged/Unmerged (default)</p> | |

Table A–9 (Cont.) Web Services Security Module on WebLogic Configuration

| Parameter Name | Information | Console Name |
|--|--|--------------|
| oracle.security.jps.pdp.wssm.WSLoggingSoapHandlerEnabled | Enables the Web Services Security Module's EnvelopLoggingSOAPHandler, the web service SOAP message handler for logging. Optional Accepted Values <ul style="list-style-type: none"> ▪ true ▪ false (default value) | |

A.2.4 RMI Security Module

Table A–10 compiles the parameters to configure the RMI Security Module embedded in either a JSE or a JEE container.

Note: This configuration is for a standalone deployment.

Table A–10 RMI Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|--|--------------|
| oracle.security.jps.pdp.rism.RMIRegistryPortNumber | Defines the port on which the RMI Security Module listens to the RMI server. Mandatory Accepted Value: port number. | |
| oracle.security.jps.pdp.rism.UseSSL | Defines whether the SSL protocol is used for secure communication between the RMI Security Module and RMI server. Optional Accepted Values <ul style="list-style-type: none"> ▪ true ▪ false (default) | |
| oracle.security.jps.pdp.sm.IdentityCacheEnabled | Specifies whether the identity cache is being used. If not set, no identity cache is used by default. Optional Accepted Value: true/false | |
| oracle.security.jps.pdp.sm.IdentityMaxCacheSize | Specifies the maximum number of users for which information is cached. When the maximum is reached, old records are dropped and reestablished when needed. Optional Accepted Value: number | |

Table A–10 (Cont.) RMI Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|--|--|--------------|
| oracle.security.jps.pdp.sm.IdentityCacheEvictionPercentage | Specifies percentage of identities that must be evicted when cache has reached the maximum size. Optional Accepted Value: number representing percentage | |
| oracle.security.jps.pdp.sm.IdentityCachedEntryTTL | Specifies the time-to-live of an identity cache record. Optional Accepted Value: time in seconds | |

A.2.5 WebLogic Server Security Module

Table A–11 compiles the parameters to configure the WebLogic Server (WLS) Security Module embedded in a JEE container. These parameters are used only when the WLS Security Module is configured to be used as a PEP.

- See Section 1.3.2, "The Policy Decision Point and the Policy Enforcement Point" for contextual information.
- See Section 9.4, "Securing WebLogic Server Resources" to enable the WebLogic Server Security Module.

Table A–11 WebLogic Server Security Module Configuration Parameters

| Parameter Name | Information | Console Name |
|----------------------------|---|--|
| UndefinedApplicationEffect | Specifies the effect (GRANT, DENY) that the provider must return if an application is not defined in the policy store. Optional Accepted Values <ul style="list-style-type: none"> ■ permit (default) ■ abstain ■ deny | Set in the WebLogic Server Administration Console; values are saved to config.xml in the WebLogic domain |
| NoApplicablePolicyEffect | Specifies the effect that the provider has to return if no applicable policies have been found. Optional Accepted Values <ul style="list-style-type: none"> ■ deny (default value represents a closed system) ■ abstain ■ permit (represents an open system) | Set in the WebLogic Server Administration Console; values are saved to config.xml in the WebLogic domain |

A.2.6 WebLogic Server Security Module Discovery Mode

Table A–12 compiles the parameters to enable Discovery Mode. See Section 9.4.2, "Discovering WebLogic Server Resources" for more information.

Table A–12 WebLogic Server Discovery Mode Parameters

| Parameter Name | Information | Console Name |
|--|---|------------------------|
| oracle.security.jps.discoveryMode | By default, Discovery Mode is off. Optional Accepted Values <ul style="list-style-type: none"> ■ true ■ false | Only in jps-config.xml |
| oracle.security.jps.discoverydPolicyDir | Specifies the absolute path to the directory in which discovery results are defined. Optional (Mandatory when Discovery Mode is enabled) Accepted Value: absolute path to directory | Only in jps-config.xml |
| oracle.security.jps.discoverydResourceIsHierarchical | Specifies whether the resource is hierarchical. Optional Accepted Values <ul style="list-style-type: none"> ■ true ■ false | Only in jps-config.xml |
| oracle.security.jps.discoverydResourceNameDelimiter | Specifies the delimiter to separate the resource name. Optional (Mandatory when resource is defined as Hierarchical) Accepted Value: any valid resource name delimiter; when used with WLS SM and OSB SM, the value should be "/" | Only in jps-config.xml |

A.3 PDP Proxy Client Configuration

This section contains information regarding configuration for the PDP Proxy Client available for the RMI and Web Services Security Module.

- [Section A.3.1, "Web Services Security Module PDP Proxy Client"](#)
- [Section A.3.2, "RMI Security Module PDP Proxy Client"](#)

A.3.1 Web Services Security Module PDP Proxy Client

[Table A–13](#) compiles the parameters to configure the Web Services Security Module PDP Proxy Client.

Table A–13 Web Services Proxy Client Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|--------------|
| oracle.security.jps.pdp.PDPTransport | <p>Specifies the underlying protocol to be used by Multi-protocol Security Module to communicate with Oracle Entitlements Server.</p> <p>Mandatory</p> <p>Accepted Values: no default value; XACML is always available in the Web Services Security Module.</p> <ul style="list-style-type: none"> ■ WS ■ RMI | |
| oracle.security.jps.pdp.proxy.PDPAddress | <p>Specifies the host and port number of either the Web Services Security Module. For example, <code>http://dadvm10134:9015</code></p> <p>Optional</p> <p>Accepted Value: a comma separated list of URIs (if more than one address is specified the first is considered the primary, and the rest as backups)</p> | |
| oracle.security.jps.pdp.proxy.RequestTimeoutMilliSecs | <p>Defines the interval of time in which an authorization request times out when the remote PDP (RMI or Web Services Security Module) is not responding.</p> <p>Optional</p> <p>Accepted Value: time in milliseconds (default value is 10000)</p> | |
| oracle.security.jps.pdp.proxy.FailureRetryCount | <p>Specifies the number of attempts to make before attempting the alternate failover server.</p> <p>Optional</p> <p>Accepted Value: number (default value is 3)</p> | |
| oracle.security.jps.pdp.proxy.FailbackTimeoutMilliSecs | <p>Specifies the interval of time after which a failed primary server is tried again for failover.</p> <p>Optional</p> <p>Accepted Value: time in milliseconds (default value is 180000)</p> | |
| oracle.security.jps.pdp.proxy.SynchronizationIntervalMilliSecs | <p>Defines how often the PDP Proxy polls the PDP server in order to synchronize its state. For example, the interval is used to periodically check whether the authorization cache has to be flushed.</p> <p>Optional</p> <p>Accepted Value: time in milliseconds (default value is 60)</p> | |

Table A–13 (Cont.) Web Services Proxy Client Configuration Parameters

| Parameter Name | Information | Console Name |
|---|--|--------------|
| oracle.security.jps.pdp.proxy.wssm.ssl.identityKeyStoreFileName | <p>Defines the name of the Identity Key Store file where client certificates for the Web Services Security Module are stored. Used for SSL communication between a client and the Web Services Security Module.</p> <p>Optional</p> <p>Accepted Value: name of the Identity Key Store file</p> | |
| oracle.security.jps.pdp.proxy.wssm.ssl.trustKeyStoreFileName | <p>Defines the name of the Trust Key Store file where CA certificates for Web Services Security Module are stored. Used for SSL communication between a client and the Web Services Security Module.</p> <p>Optional</p> <p>Accepted Value: the name of the Trust Key Store file.</p> | |
| oracle.security.jps.pdp.proxy.wssm.ssl.identityKeyStoreKeyAlias | <p>Specifies the alias name of the Web Services client certificate. Used for SSL communication between a client and the Web Services Security Module.</p> <p>Optional</p> <p>Accepted Value: alias of the identity key store (if only one alias exists in the identity key store, no need to specify this value)</p> | |
| oracle.security.jps.pdp.proxy.wssm.protocol | <p>Defines the transport protocol used between the Policy Distribution Component client and server.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ▪ https ▪ http (default value) | |

A.3.2 RMI Security Module PDP Proxy Client

Table A–14 compiles the parameters to configure the RMI Security Module PDP Proxy Client.

Table A–14 PDP RMI Proxy Client Configuration Parameters

| Parameter Name | Information | Console Name |
|--------------------------------------|--|--------------|
| oracle.security.jps.pdp.PDPTransport | <p>Specifies the underlying protocol to be used by Multi-protocol Security Module to communicate with Oracle Entitlements Server.</p> <p>Mandatory</p> <p>Accepted Values: no default value; XACML is always available in the RMI Security Module.</p> <ul style="list-style-type: none"> ▪ WS ▪ RMI | |

Table A–14 (Cont.) PDP RMI Proxy Client Configuration Parameters

| Parameter Name | Information | Console Name |
|--|---|--------------|
| oracle.security.jps.pdp.proxy.PDPAddress | Specifies the host and port number of the RMI Security Module. For example, <code>rmi://localhost:9400</code> Mandatory Accepted Value: a comma separated list of URIs (if more than one address is specified the first is considered the primary, and the rest as backups) | |
| oracle.security.jps.pdp.proxy.RequestTimeoutMilliSecs | Defines the interval of time in which an authorization request times out when the remote PDP (RMI or Web Services Security Module) is not responding. Optional Accepted Value: time in milliseconds (default value is 10000) | |
| oracle.security.jps.pdp.proxy.FailureRetryCount | Specifies the number of attempts to make before attempting the alternate failover server. Optional Accepted Value: number (default value is 3) | |
| oracle.security.jps.pdp.proxy.FailbackTimeoutMilliSecs | Specifies the interval of time after which a failed primary server is tried again for failover. Optional Accepted Value: time in milliseconds (default value is 180000) | |
| oracle.security.jps.pdp.proxy.SynchronizationIntervalMilliSecs | Defines how often the PDP Proxy polls the PDP server in order to synchronize its state. For example, the interval is used to periodically check whether the authorization cache has to be flushed. Optional Accepted Value: time in milliseconds (default value is 60) | |

A.4 Policy Store Service Configuration

Table A–15 compiles the configuration parameters for the Policy Store Service.

Table A–15 Policy Store Service Configuration Parameters

| Parameter Name | Information | Console Name |
|----------------|---|--------------|
| ldap.url | Defines the URL of the LDAP policy store. Valid in JEE and JSE applications and only applies to LDAP stores. Mandatory Accepted Value: URI of the LDAP policy store in the format <code>ldap://host:port</code> . | |

Table A–15 (Cont.) Policy Store Service Configuration Parameters

| Parameter Name | Information | Console Name |
|---|---|--------------|
| max.search.filter.length | <p>Defines the maximum length of a search filter.</p> <p>Mandatory</p> <p>Accepted Value: integer defining the maximum length of a search filter; for example, 1024</p> | |
| oracle.security.jps.ldap.root.name | <p>Defines the RDN format of the root node in the LDAP policy store. Valid in JEE and JSE applications. Applies to LDAP and database stores.</p> <p>Mandatory</p> <p>Accepted Value: root name of jps context; for example, cn=jpsroot.</p> | |
| oracle.security.jps.farm.name | <p>Defines the RDN format of the root node in the LDAP policy store. Valid in JEE and JSE applications. Applies to LDAP and database stores.</p> <p>Mandatory</p> <p>Accepted Value: farm name of the domain; for example, cn=base_domain.</p> | |
| oracle.security.jps.policy.store.resource.type.enforcement.mode | <p>Controls the throwing of exceptions if any of the following checks fail:</p> <ul style="list-style-type: none"> ■ Verify that if two resource types share the same permission class, that permission must be either ResourcePermission or extend AbstractTypedPermission, and this last resource type cannot be created. ■ Verify that all permissions have resource types defined, and that the resource matcher permission class and the permission being granted match. <p>Valid in JEE and JSE applications. Applies to LDAP and database stores.</p> <p>Optional</p> <p>Accepted Values</p> <ul style="list-style-type: none"> ■ strict (when any of the above checks fail, the system throws an exception and the operation is aborted) ■ lenient (default value; when any of the above checks fail, the system does not throw any exceptions, the operation continues without disruption, and any discrepancies encountered are logged) | |

Table A–15 (Cont.) Policy Store Service Configuration Parameters

| Parameter Name | Information | Console Name |
|----------------------------------|---|--------------|
| bootstrap.security.principal.key | <p>Defines the key for the password credentials to access the LDAP policy store, stored in the CSF store. Valid in JEE and JSE applications. Applies to LDAP and database stores.</p> <p>Mandatory</p> <p>Accepted Value: the key name of the credential; for example, <code>oes_sm_key</code>. The out-of-the-box value is <code>bootstrap</code>.</p> | |
| bootstrap.security.principal.map | <p>Defines the map for the password credentials to access the LDAP policy store, stored in the CSF store. Valid in JEE and JSE applications. Applies to LDAP and database stores.</p> <p>Mandatory</p> <p>Accepted Value: map name of the credential; for example, <code>oes_sm_map</code>. The default value is <code>BOOTSTRAP_JPS</code>.</p> | |
| jdbc.driver | <p>Defines the name of the JDBC driver.</p> <p>Mandatory</p> <p>Accepted Value: name of the JDBC driver.</p> | |
| jdbc.url | <p>Defines the JDBC driver connection URL.</p> <p>Mandatory</p> <p>Accepted Value: the JDBC driver connection URL.</p> | |

Configuring Attribute Retrievers

As discussed in [Section 1.3, "Overview of the Oracle Entitlements Server Architecture,"](#) the Policy Information Point (PIP) is a system entity that acts as a source for attribute values. Oracle Entitlements Server relies on an attribute retriever plug-in to get attribute values from one or more of these information stores. These attribute retrievers allow policies to be data-driven in that the value of the attribute can impact the access decision. For example, if access to transfer money from a bank account is based on how much money is currently in the account, an attribute retriever can be used to get a value for the current balance.

Predefined attribute retrievers are shipped with Oracle Entitlements Server. This chapter documents these predefined attribute retrievers and related configuration requirements and the configuration of custom attribute retrievers. It contains the following sections.

- [Section B.1, "Understanding Predefined Attribute Retrievers"](#)
- [Section B.2, "Configuring the Attribute Retrievers Using SMConfig UI"](#)
- [Section B.3, "Configuring the Predefined Attribute Retrievers Manually"](#)
- [Section B.4, "Configuring the Custom Attribute Retrievers Manually"](#)

Note: For more information, see "Working With Attribute Retrievers" in *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

B.1 Understanding Predefined Attribute Retrievers

Oracle Entitlements Server contains predefined attribute retrievers that are used to connect to, and retrieve attribute values from, Lightweight Directory Access Protocol (LDAP) data stores and relational database management systems (RDBMS). These predefined attribute retrievers can handle one or more attributes defined in the system without additional programming. They also contain a caching feature and failover.

B.2 Configuring the Attribute Retrievers Using SMConfig UI

The SMConfig UI enables you to create the following attribute retrievers:

- LDAP attribute retriever
- RDBMS attribute retriever
- Custom attribute retriever

B.2.1 Prerequisites

Prerequisites for configuring an attribute retriever using the SMConfig UI are:

- the OES Client is installed
- a Security Module is installed or a `jps-config.xml` file exists

B.2.2 Running the SMConfig UI to Edit the `jps-config.xml` File

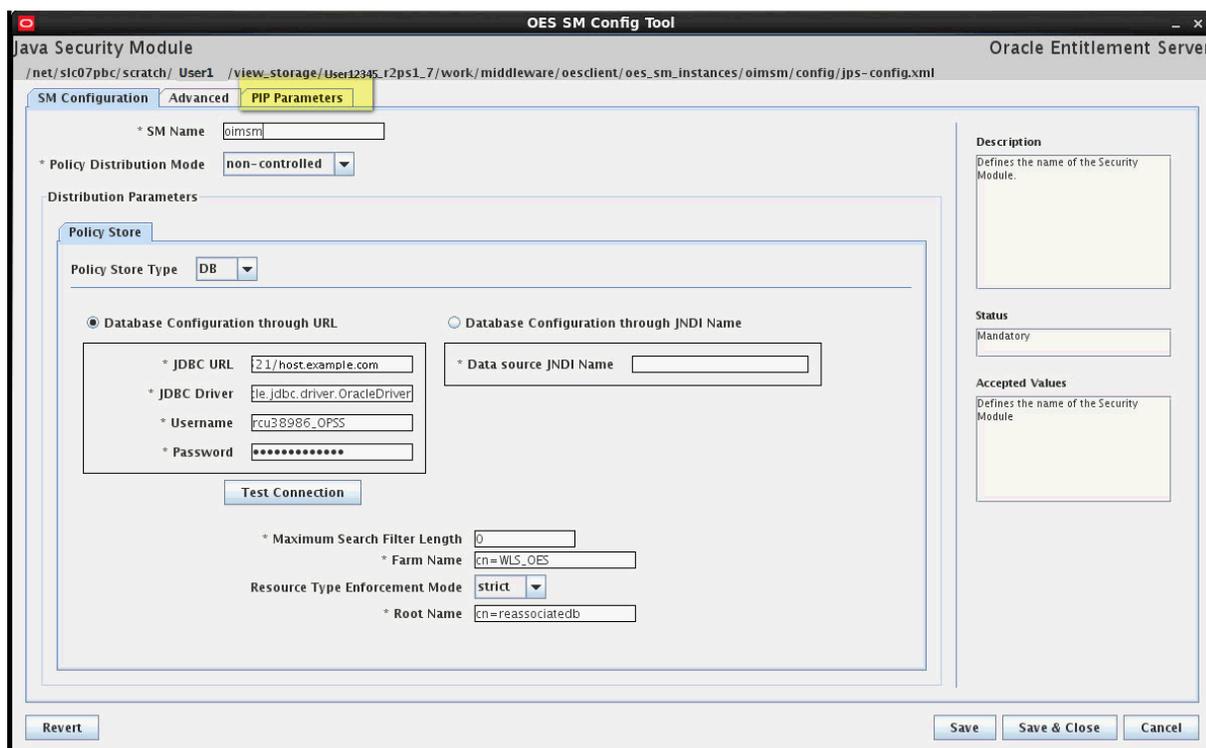
To edit the `jps-config.xml` file:

1. Navigate to the `oesclient/oesm/enroll/bin` directory.
2. Run the command: `./oesmconfig.sh -jpsconfig [path]/jps-config.xml`.

To edit the SM instance `jps-config.xml` file:

1. Navigate to the `oesclient/oes_sm_instances/[SM Name]/bin` directory.
2. Run the command `./oesmconfig.sh`.

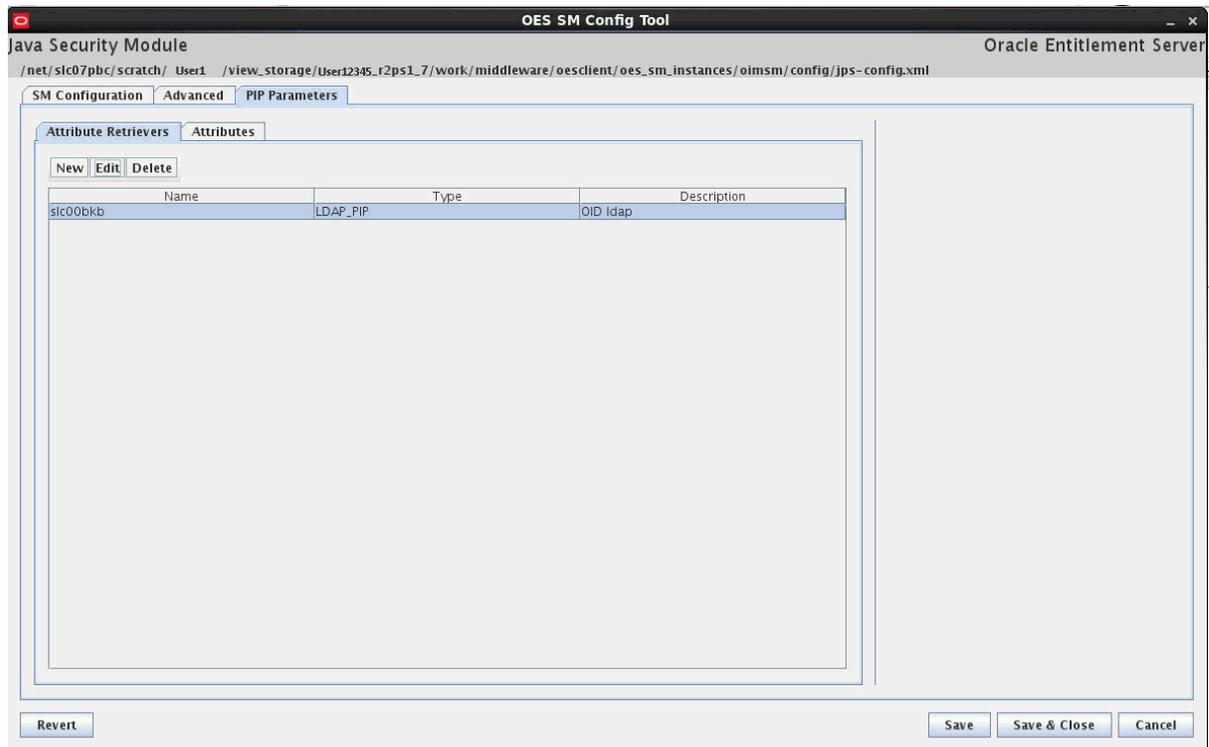
A screen similar to the following appears.



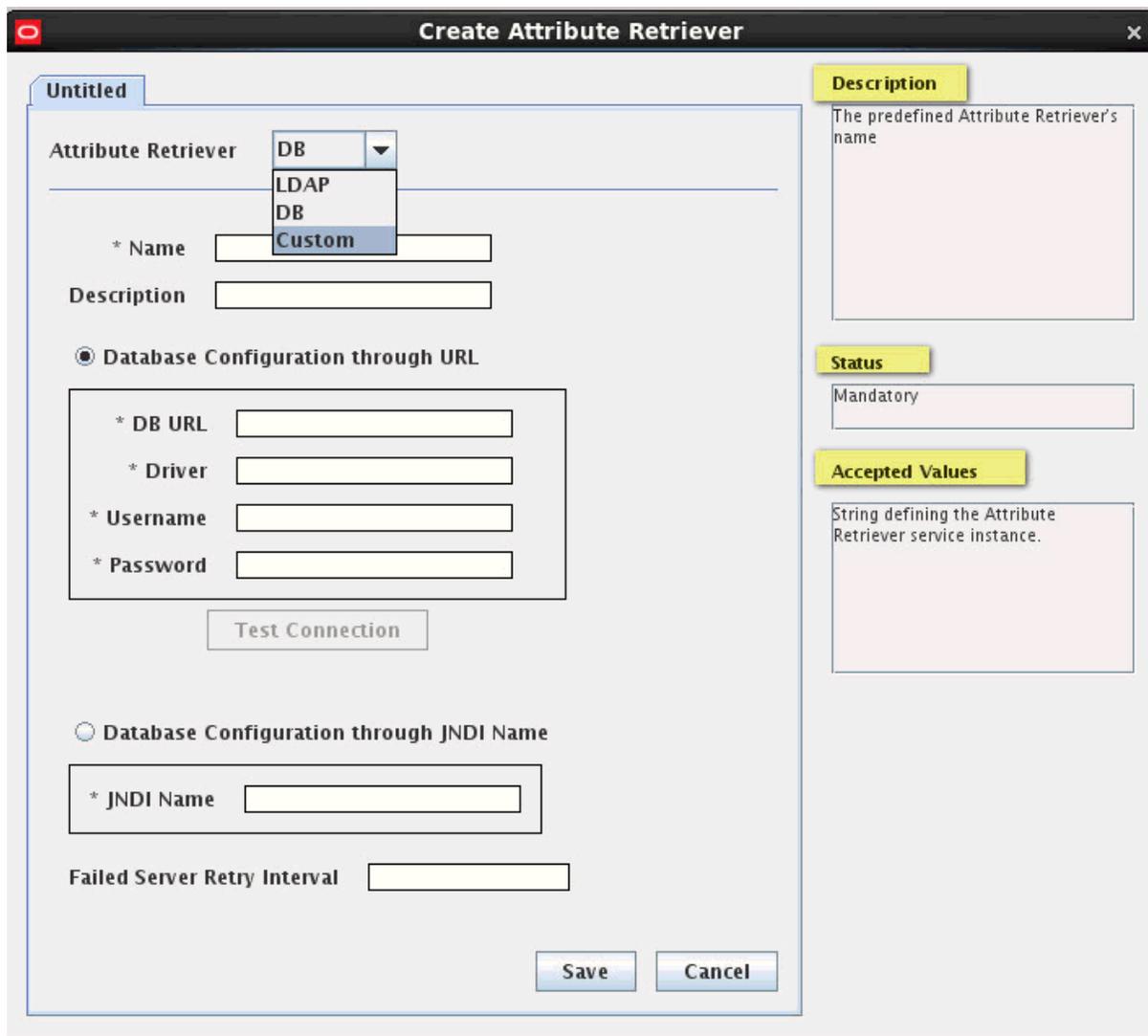
B.2.3 Adding, Editing, or Deleting Attribute Retrievers

To add, edit, delete an attribute retriever:

1. In the SMConfig UI, click the **PIP Parameters** tab.
The PIP configuration screen is displayed.



2. Click the **Attribute Retrievers** tab.
3. To create a new attribute retriever:
 - a. Click the **New** button to add a new attribute retriever.
The Create New Attribute Retriever screen is displayed.



- b. In the Create Attribute Retriever screen, provide information as documented in Table 8–6, "Java Security Module PIP Parameters (Attribute Retrievers)" in Chapter 8, "Managing Security Module Configurations."
- c. Click **Save** to save the new attribute retriever.

Note: The screen displays the field description, status, and accepted values.

4. To edit an attribute retriever:
 - a. Select an existing attribute retriever that is listed in the Attribute Retrievers tab.
 - b. Click the **Edit** button to edit the attribute retriever.
 - c. In the attribute retriever dialog that appears, update the value.
 - d. Click the **Save** button to save the changes.
5. To delete an attribute retriever:

- a. Select an existing attribute retriever that is listed in the Attribute Retrievers tab.
- b. Click the **Delete** button to delete the attribute retriever.
- c. Click **Yes** in the confirmation dialog.

B.2.4 Adding, Editing, or Deleting Attributes in Attribute Retriever Configuration

To add, edit, or delete an attribute in the attribute retriever:

Note: There must be 1 attribute retriever at least to perform any of the following tasks.

1. In the SMConfig UI, click the **PIP Parameters** tab.
2. Click the **Attributes** tab.
3. To create a new attribute in the attribute retriever:
 - a. Click the **New** button.

The Create Attribute screen appears.

- b. In the Create Attribute dialog, fill in the fields.
- c. Click **Save** to Save the Attribute.
4. To edit an attribute in the attribute retriever:
 - a. Select an existing attribute listed in the Attributes tab.
 - b. Click the **Edit** button.
 - c. In the Attributes dialog, updated the attribute information.

- d. Click **Save** to Save the Attribute changes.
5. To delete an attribute in the attribute retriever:
 - a. Select an existing Attribute in the Attributes tab.
 - b. Click the **Delete** button.
 - c. In the confirmation dialog, click **Yes** to delete the Attribute.

B.3 Configuring the Predefined Attribute Retrievers Manually

Configuration information for attribute retrievers is defined in the `jps-config.xml` configuration file (used by Java EE containers) located in the `$DOMAIN_HOME/config/fmwconfig` directory. To set up a predefined Attribute Retrieve manually, you must:

- Configure individual attribute values including attribute name, name of attribute retriever used, search query to retrieve the value (for example, SQL query if the PIP is a relational database or LDAP query if it's a directory), and any attribute value caching information.
- Configure information regarding the name of the class implementing the attribute retriever.
- Configure information needed to connect to the data store as well as credential information.
- Declare the attribute retriever reference

The following sections contain information on the configuration parameters for each type of attribute retriever.

- [Section B.3.2, "Configuring Individual Attribute Values"](#)
- [Section B.3.3, "Declaring the PIP Service Provider"](#)
- [Section B.3.4, "Configuring Repository Connection"](#)
- [Section B.3.5, "Declaring the Predefined Attribute Retriever Reference in jpsContexts Section"](#)
- [Section B.3.6, "Configuring Cache and Failover"](#)

B.3.1 Roadmap

The types of predefined attribute retriever are:

- the LDAP attribute retriever
LDAP attribute retrievers retrieve attribute values from a LDAP database.
- the RDBMS attribute retriever
RDBMS attribute retrievers retrieve attribute values from an RDBMS database.

[Table B-1](#) contains a roadmap for configuring attribute retrievers.

Table B-1 Configuration Roadmap

| No. | Task | Information |
|-----|--|---|
| 1. | Configure individual attribute values by updating the <code>propertySets</code> section in the <code>jps-config.xml</code> file. | For more information, see Section B.3.2, "Configuring Individual Attribute Values." |

Table B–1 (Cont.) Configuration Roadmap

| No. | Task | Information |
|-----|--|--|
| 2. | Declare the PIP service provider by updating the <code>serviceProviders</code> section in the <code>jps-config.xml</code> file. | For more information, see Section B.3.3, "Declaring the PIP Service Provider." |
| 3. | Configure information needed to connect to the repository by updating the <code>serviceInstances</code> section in the <code>jps-config.xml</code> file. | For more information, see Section B.3.4, "Configuring Repository Connection." |
| 4. | Declare the attribute retriever reference by updating the <code>jpsContexts</code> section in the <code>jps-config.xml</code> file. | For more information, see Section B.3.5, "Declaring the Predefined Attribute Retriever Reference in <code>jpsContexts</code> Section." |

B.3.2 Configuring Individual Attribute Values

Attribute query information is related to a particular attribute and includes its name, the name of the predefined attribute retriever used, the search query for retrieval (for example, a SQL query if the store is a relational database or an LDAP query if it is a directory), and any attribute caching information. Attribute query information is defined in the `<propertySets>` section of `jps-config.xml`.

[Table B–2](#) documents the parameters to be defined for each attribute retrieved by the configured attribute retriever.

Table B–2 Configure Attributes to be Retrieved

| Name | Usage |
|--------|---|
| name | <p>Description: The name of the attribute as defined in the policy store. When using the LDAP predefined attribute retriever, the attribute name defined for Oracle Entitlements Server must be the same as the attribute name defined in the LDAP store. Currently, there is no name mapping functionality.</p> <p>Mandatory</p> <p>Accepted Value: Attribute name</p> |
| query | <p>Description: The database SQL command or LDAP filter used for the query. Users can use a built-in and custom attributes in the query string. For example, the built-in attribute <code>sys_user</code> can be used to define a query such as <code>select age from customers where name=%sys_user%;</code>. The token is automatically replaced by its value before sending the query to the data store. Bi-directional dependency (where, for example, AttributeA's query string contains AttributeB and AttributeB's query string contains AttributeA) can also be detected and, in such cases, an exception is thrown.</p> <p>Mandatory</p> <p>Accepted Value: SQL command or LDAP filter.</p> |
| ttl | <p>Description: The time-to-live in seconds of any cached attribute values when cached is enabled.</p> <p>Optional</p> <p>Accepted Value: Any integer; default value is 60 seconds if cache is enabled.</p> |
| cached | <p>Description: Enables the caching of attribute values.</p> <p>Optional</p> <p>Accepted Value: Default value is false.</p> |

Table B–2 (Cont.) Configure Attributes to be Retrieved

| Name | Usage |
|--------------------|---|
| ootb.pip.attr.type | Description: Should be set to OOTB_PIP_ATTRIBUTE. Mandatory Accepted Value: OOTB_PIP_ATTRIBUTE. |
| ootb.pip.ref | Description: Should be set to an OOTB PIP instance. Mandatory Accepted Value: The PIP service instance name defined in the <serviceInstance> section of jps-config.xml |

Example B–1 shows an attribute defined for a LDAP retriever.

Example B–1 Attribute Query Information Defined for LDAP Attribute Retriever

```
<propertySet name="ootb.pip.attribute.age.based.on.myattr.ldap">
  <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
  <property name="ootb.pip.ref" value="pip.service.ootb.ldap"/>
  <property name="name" value="oespipage_myattr"/>
  <property name="query" value="(cn=%MyAttr%)" />
  <property name="cached" value="true"/>
  <property name="ttl" value="60"/>
</propertySet>
```

Example B–2 shows an attribute defined for a RDBMS retriever.

Example B–2 Attribute Query Information Defined for the RDBMS Attribute Retriever

```
<propertySet name="ootb.pip.attribute.age.based.on.myattr.rdbms">
  <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
  <property name="ootb.pip.ref" value="pip.service.ootb.db"/>
  <property name="name" value="oespipage_myattr"/>
  <property name="query" value="select oespipage
  as oespipage_myattr from pip_info_store where username=%MyAttr%"/>
  <property name="cached" value="true"/>
  <property name="ttl" value="60"/>
</propertySet>
```

B.3.3 Declaring the PIP Service Provider

Example B–3 illustrates how the serviceProvider element defines the use of a predefined attribute retriever by defining the internal Oracle Entitlements Server class.

Example B–3 Declaring the Predefined Attribute Retriever

```
<serviceProvider
  class="oracle.security.jps.az.internal.runtime.provider.PIPServiceProvider"
  name="pip.service.provider" type="PIP"/>
```

B.3.4 Configuring Repository Connection

Repository connection information is used to connect to the data store and may include its location, JDBC driver and URL or LDAP URL (whichever is applicable) and the user/credential information. This connection information is related to a particular

retriever instance. Repository connection information is defined in the <serviceInstances> section of jps-config.xml.

Note: The instance must also be defined in the default <jpsContexts> section. See [Example B.3.5, "Declaring the Predefined Attribute Retriever Reference in jpsContexts Section"](#).

Section B.3.4.1, "Configuring the LDAP Repository Attribute Retriever Parameters," Section B.3.4.2, "Configuring the Database Repository Attribute Retriever Parameters," and Section B.3.7, "Sample jps-config.xml File" contain information regarding a repository connection configuration.

Note: These predefined attribute retrievers can be configured with Oracle Database 11gR1, Oracle Internet Directory 11gR1, and Oracle Virtual Directory 11gR1.

B.3.4.1 Configuring the LDAP Repository Attribute Retriever Parameters

Table B-3 documents the parameters that must be defined when using the LDAP attribute retriever. See [Example B-4, "Using the Predefined LDAP Attribute Retriever"](#) and [Example B-9, "Configuring LDAP Failover"](#) for sample configuration code.

Table B-3 LDAP Attribute Retriever Parameters

| Name | Usage |
|------------------------------|--|
| name | <p>Description: The predefined attribute retriever's name (PIP instance name)</p> <p>Mandatory</p> <p>Accepted Value: String defining the attribute retriever service instance.</p> |
| description | <p>Description: A description of the predefined attribute retriever (PIP instance description)</p> <p>Optional</p> <p>Accepted Value: string</p> |
| type | <p>Description: The predefined attribute retriever's type (The type of this PIP instance)</p> <p>Mandatory</p> <p>Accepted Value: LDAP_PIP</p> |
| failed.server.retry.interval | <p>Description: After communication with a primary repository has failed, this attribute defines the interval of time during which the backup repository is used before switching back to the primary repository.</p> <p>Optional</p> <p>Accepted Value: Takes a value equal to the number of seconds. Default value is 15.</p> |

Table B–3 (Cont.) LDAP Attribute Retriever Parameters

| Name | Usage |
|----------------------------------|--|
| bootstrap.security.principal.key | <p>Description: Defines the principal key for the password credentials to access the LDAP policy store, stored in the CSF store. Valid in JEE and JSE applications. Applies to LDAP and database stores. See Section B.3.4.3, "Setting Up PIP Connection Credentials."</p> <p>Mandatory</p> <p>Accepted Value: key name of the credential; for example, oes_sm_key.</p> |
| bootstrap.security.principal.map | <p>Description: Defines the principal map for the password credentials to access the LDAP policy store, stored in the CSF store. Valid in JEE and JSE applications. Applies to LDAP and database stores. See Section B.3.4.3, "Setting Up PIP Connection Credentials."</p> <p>Mandatory</p> <p>Accepted Value: map name of the credential; for example, oes_sm_map.</p> |
| ldap.url | <p>Description: Defines the URL of the LDAP policy store. Valid in JEE and JSE applications and only applies to LDAP stores.</p> <p>Mandatory</p> <p>Accepted Value: URI of the LDAP policy store in the format ldap://host:port.</p> |
| search.base | <p>Description: The LDAP search base.</p> <p>Mandatory: For LDAP only.</p> <p>Accepted Value: The DN of the search base object.</p> |

[Example B–4](#) illustrates how to modify the `serviceInstance` element when using the predefined LDAP attribute retriever.

Example B–4 Using the Predefined LDAP Attribute Retriever

```
<serviceInstance name="pip.service.ootb.ldap" provider="pip.service.provider">
  <property name="type" value="LDAP_PIP"/>
  <property name="ldap.url" value="ldap://dadvmg0065.domainexample.com:3080"/>
  <property name="bootstrap.security.principal.key" value="keyname"/>
  <property name="bootstrap.security.principal.map" value="mapname"/>
  <property name="failed.server.retry.interval" value="10"/>
</serviceInstance>
```

B.3.4.2 Configuring the Database Repository Attribute Retriever Parameters

[Table B–4](#) documents the parameters that must be defined when using the RDBMS attribute retriever. See [Example B–5, "Using the Predefined RDBMS Attribute Retriever with JDBC"](#) and [Example B–6, "Using the Predefined RDBMS Attribute Retriever with Data Source"](#) for sample configuration code.

Table B-4 RDBMS Attribute Retriever Parameters

| Name | Usage |
|----------------------------------|--|
| name | <p>Description: The predefined attribute retriever's name (PIP instance name)</p> <p>Mandatory</p> <p>Accepted Value: String defining the attribute retriever service instance.</p> |
| description | <p>Description: A description of the predefined attribute retriever (PIP instance description)</p> <p>Optional</p> <p>Accepted Value: string</p> |
| type | <p>Description: The predefined attribute retriever's type (The type of this PIP instance)</p> <p>Mandatory</p> <p>Accepted Value: RDBMS_PIP</p> |
| failed.server.retry.interval | <p>Description: After the primary repository has failed, this attribute identifies the interval of time during which the backup repository is used before switching back to the primary repository.</p> <p>Optional</p> <p>Accepted Value: Takes a value equal to the number of seconds. Default value is 15.</p> |
| bootstrap.security.principal.key | <p>Description: Defines the principal key for the password credentials to access the database, stored in the CSF store. Valid in JEE and JSE applications. See Section B.3.4.3, "Setting Up PIP Connection Credentials."</p> <p>Mandatory</p> <p>Accepted Value: key name of the credential; for example, oes_sm_key.</p> |
| bootstrap.security.principal.map | <p>Description: Defines the principal map for the password credentials to access the database, stored in the CSF store. Valid in JEE and JSE applications. See Section B.3.4.3, "Setting Up PIP Connection Credentials."</p> <p>Mandatory</p> <p>Accepted Value: map name of the credential; for example, oes_sm_map.</p> |
| jdbc.driver | <p>Description: Location of the driver when using Java Database Connectivity (JDBC) API to connect to a database.</p> <p>Mandatory: When using JDBC API to connect to database.</p> <p>Accepted Value: oracle.jdbc.driver.OracleDriver, for example</p> |
| jdbc.url | <p>Description: Takes a URL that points to the database.</p> <p>Mandatory: When using JDBC API to connect to database.</p> <p>Accepted Value: A list of comma-delimited URLs. The first is treated as primary and so on. For example, jdbc:oracle:thin:@sc158116.domainexample.com:1521:orcl</p> |

Table B–4 (Cont.) RDBMS Attribute Retriever Parameters

| Name | Usage |
|----------------------|---|
| datasource.jndi.name | <p>Description: Data source JNDI name if you want the PIP instance working through data source rather than directly through JDBC. The data source scenario is supported on WebLogic Server and WebSphere Application Server only.</p> <p>Mandatory: If you want the PIP instance working through data source rather than directly through JDBC.</p> <p>Accepted Value: JNDI name of pre-defined data source object</p> |

The following two examples illustrate how to modify the `serviceInstance` element when using the predefined RDBMS attribute retriever.

[Example B–5](#) is an example of when you want the RDBMS attribute retriever working via the Java Database Connectivity (JDBC) API.

Example B–5 Using the Predefined RDBMS Attribute Retriever with JDBC

```
<serviceInstance name="pip.service.ootb.db" provider="pip.service.provider">
  <property name="type" value="RDBMS_PIP" />
  <property name="jdbc.url"
    value="jdbc:oracle:thin:@scl58116.domainexample.com:1521:orcl" />
  <property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver" />
  <property name="bootstrap.security.principal.map" value="mapname" />
  <property name="bootstrap.security.principal.key" value="keyname" />
  <property name="failed.server.retry.interval" value="10" />
</serviceInstance>
```

[Example B–6](#) is an example of when you want the RDBMS attribute retriever working via a data source rather than directly with JDBC

Example B–6 Using the Predefined RDBMS Attribute Retriever with Data Source

```
<serviceInstance name="pip.service.ootb.db" provider="pip.service.provider">
  <property name="type" value="RDBMS_PIP" />
  <property name="datasource.jndi.name" value="DB_RAC" />
  <property name="failed.server.retry.interval" value="10" />
</serviceInstance>
```

B.3.4.3 Setting Up PIP Connection Credentials

As documented in [Table B–3, "LDAP Attribute Retriever Parameters"](#) and [Table B–4, "RDBMS Attribute Retriever Parameters"](#), the `bootstrap.security.principal.key` and `bootstrap.security.principal.map` parameters define the key and the map (respectively) to access the data store. Oracle Entitlements Server ships with `oesPassword.sh` which sets these LDAP and database connection credentials in the bootstrap credential store. The tool is located in the `$OES_SM_INSTANCE_DIRECTORY/bin/` directory.

Note: Set the following classes to the CLASSPATH before running `oesPassword.sh`:

- `OES_ORACLE_HOME/modules/javax.security.jacc_1.0.0.0_1-1.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wseeclient.jar`
 - `OES_ORACLE_HOME/wlserver_10.3/server/lib/wlthint3client.jar`
-

To run the tool:

1. Add `Oracle_Home/wlserver_10.3/server/lib/*` to the `OES_CLASSPATH` in the `setOesEnv.sh` file.

2. Enter the following command:

```
./oesPassword.sh -setpass
```

It prompts for the security principal key name, the security principal map name, the username and associated password.

B.3.4.4 Updating the Database Password

For security reasons, the passwords configured for databases are periodically changed; thus, the Oracle Entitlements Server components (Administration Server and Security Modules) will need to be updated with the new password. The following information documents how this can be done.

- The Administration Server uses a WebLogic Server data source to provide database access and database connection management. To change the password, update the data source configuration with the new password using the WebLogic Server console. Items must be restarted for the changes to take effect. Run the `WLST modifyBootStrapCredential` command and then restart the server.
- Security Modules may connect to a particular database in either of the following ways:
 - The Security Module will connect to the database used as a Policy Store when distributing policies in either the controlled-pull, non-controlled or mixed distribution modes.
 - The Security Module can connect to any relational database management system (RDBMS) when retrieving attributes from an attribute repository using attribute retrievers. (This connection is not limited to the default Policy Store.)

Both cases can use either the WebLogic Server data source configuration or JDBC properties directly. In cases when connecting via the WLS data source configuration, update the data source configuration with the new password using the WebLogic Server console. No additional steps are required. In cases when connecting via the JDBC properties directly, use the `oesPassword` utility as discussed in [Section B.3.4.3, "Setting Up PIP Connection Credentials."](#) The map and key for the credential is defined in `jps-config.xml`.

B.3.5 Declaring the Predefined Attribute Retriever Reference in `jpsContexts` Section

[Example B-7](#) illustrates how to declare the predefined attribute retriever reference in the `jpsContext` element. This sample defines a predefined RDBMS attribute retriever.

Example B-7 Declaring the Predefined Attribute Retriever in jpsContext

```

<jpsContext name="default">
  <serviceInstanceRef ref="policystore.db" />
  <serviceInstanceRef ref="pdp.service" />
  <serviceInstanceRef ref="audit" />
  <serviceInstanceRef ref="idstore.xml" />
  <serviceInstanceRef ref="idstore.loginmodule" />
  <serviceInstanceRef ref="pip.service.ootb.db" />
</jpsContext>

```

B.3.6 Configuring Cache and Failover

An in-memory cache mechanism is used to improve performance by reducing communications between Oracle Entitlements Server and the external repository. The cache holds up to 1000 entries and can be enabled for each individual attribute. The cache size is not configurable. If the limit is reached, cache items are removed randomly. [Example B-1](#) illustrates the definition of an individual attribute with the `cached` and `ttl` properties.

[Example B-8](#) illustrates how to configure the caching of a specific attribute value. Caching is enabled per attribute. In this example, the cache record is deleted after 60 seconds.

Example B-8 Enabling an Attribute's Cache

```

<propertySet name="ootb.pip.attribute.gender.ldap">
  <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE" />
  <property name="ootb.pip.ref" value="pip.service.ootb.ldap" />
  <property name="name" value="oespipgender" />
  <property name="query" value="(oespipage=%oespipage%)" />
  <property name="cached" value="true" />
  <property name="ttl" value="60" />
</propertySet>

```

Repository failover can also be configured. When a call for an attribute is received, Oracle Entitlements Server checks whether the primary repository is active. If it is active, the value is retrieved. If the primary repository is not active, it has failed previously and the backup repository is active. In the latter case, Oracle Entitlements Server checks to see if it is time to switch back to the active repository (based on configuration). If it is time to switch back, the switch is made and the value is retrieved from the primary repository. If the configured time has not yet passed, the value is retrieved from the active backup repository.

Note: If errors occur when retrieving values from the primary repository, Oracle Entitlements Server searches the backup repositories, trying them one by one until an active one is found.

[Example B-9](#) illustrates how to configure the failover behavior. In this example, the primary connection is `ldap://dadvmg0065:3080` and the backup connection is `ldap://sc158123:3060`. The failed server retry interval is 10 seconds.

Example B-9 Configuring LDAP Failover

```

<serviceInstance name="pip.service.ootb.ldap" provider="pip.service.provider">
  <property name="type" value="LDAP_PIP" />
  <property name="ldap.url"

```

```

        value="ldap://dadvmg0065:3080,ldap://sc158123:3060"/>
    <property name="bootstrap.security.principal.key" value="keyname"/>
    <property name="bootstrap.security.principal.map" value="mapname"/>
    <property name="failed.server.retry.interval" value="10"/>
</serviceInstance>

```

B.3.7 Sample jps-config.xml File

To configure the predefined attribute retriever in `jps-config.xml`, modify the elements as described in each example in this section. [Example B-10](#) is a sample `jps-config.xml` file. The examples following it illustrate the modifications that can be made.

Example B-10 Sample `jps-config.xml` File

```

<?xml version="1.0"?>

<jpsConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="
http://xmlns.oracle.com/oracleas/schema/jps-config-11_0.xsd">

    <property name="oracle.security.jps.jaas.mode" value="off"/>
    <property name="oracle.security.jps.enterprise.user.class"
        value="weblogic.security.principal.WLSUserImpl"/>
    <property name="oracle.security.jps.enterprise.role.class"
        value="weblogic.security.principal.WLSGroupImpl"/>

<propertySets>
<!-- These are the global authenticated role properties -->
    <propertySet name="authenticated.role.properties">
        <property name="authenticated.role.name" value="authenticated-role"/>
        <property name="authenticated.role.uniquename" value="authenticated-role"/>
        <property name="authenticated.role.description"
            value="This is the authenticated role used by identity store
            service instance."/>
    </propertySet>

<!-- attribute defined for ldap retriever -->
    <propertySet name="ootb.pip.attribute.age.ldap">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
        <property name="ootb.pip.ref" value="pip.service.ootb.ldap"/>
        <property name="name" value="oespipage"/>
        <property name="query" value="(cn=%SYS_USER%)" />
        <property name="cached" value="true"/>
        <property name="ttl" value="60"/>
    </propertySet>

    <propertySet name="ootb.pip.attribute.age.based.on.myattr.ldap">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
        <property name="ootb.pip.ref" value="pip.service.ootb.ldap"/>
        <property name="name" value="oespipage_myattr"/>
        <property name="query" value="(cn=%MyAttr%)" />
        <property name="cached" value="true"/>
        <property name="ttl" value="60"/>
    </propertySet>

    <propertySet name="ootb.pip.attribute.gender.ldap">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE"/>
        <property name="ootb.pip.ref" value="pip.service.ootb.ldap"/>

```

```

        <property name="name" value="oespipgender" />
        <property name="query" value="(oespipage=%oespipage%)" />
        <property name="cached" value="true" />
        <property name="ttl" value="60" />
    </propertySet>

<!-- attribute defined for rdbms retriever -->
    <propertySet name="ootb.pip.attribute.age.rdbms">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE" />
        <property name="ootb.pip.ref" value="pip.service.ootb.db" />
        <property name="name" value="oespipage" />
        <property name="query" value="select oespipage
            from pip_info_store where username=%SYS_USER%" />
        <property name="cached" value="true" />
        <property name="ttl" value="60" />
    </propertySet>

    <propertySet name="ootb.pip.attribute.age.based.on.myattr.rdbms">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE" />
        <property name="ootb.pip.ref" value="pip.service.ootb.db" />
        <property name="name" value="oespipage_myattr" />
        <property name="query" value="select oespipage
            as oespipage_myattr from pip_info_store where username=%MyAttr%" />
        <property name="cached" value="true" />
        <property name="ttl" value="60" />
    </propertySet>

    <propertySet name="ootb.pip.attribute.gender.rdbms">
        <property name="ootb.pip.attr.type" value="OOTB_PIP_ATTRIBUTE" />
        <property name="ootb.pip.ref" value="pip.service.ootb.db" />
        <property name="name" value="oespipgender" />
        <property name="query" value="select oespipgender
            from pip_info_store where oespipage=%oespipage%" />
        <property name="cached" value="true" />
        <property name="ttl" value="60" />
    </propertySet>
</propertySets>

<serviceProviders>

    <serviceProvider type="CREDENTIAL_STORE" name="credstoressp"
        class="oracle.security.jps.internal.credstore.ssp.
            SspCredentialStoreProvider">
        <description>SecretStore-based CSF Provider</description>
    </serviceProvider>

    <serviceProvider class="oracle.security.jps.az.
        internal.runtime.provider.PIPServiceProvider"
        name="pip.service.provider" type="PIP" />

    <serviceProvider type="POLICY_STORE" name="policy.rdbms"
        class="oracle.security.jps.internal.policystore.
            OPSSPolicyStoreProvider">
        <property name="policystore.type" value="DB_ORACLE" />
        <description>DBMS based PolicyStore</description>
    </serviceProvider>

    <serviceProvider name="pdp.service.provider" type="PDP"
        class="oracle.security.jps.az.internal.
            runtime.provider.PDPServiceProvider">

```

```

        <description>OPSS Runtime PDP Service Provider</description>
    </serviceProvider>

    <serviceProvider name="idstore.xml.provider" type="IDENTITY_STORE"
        class="oracle.security.jps.internal.idstore.
            xml.XmlIdentityStoreProvider">
        <description>XML-based IdStore Provider</description>
    </serviceProvider>

    <serviceProvider name="jaas.login.provider" type="LOGIN"
        class="oracle.security.jps.internal.
            login.jaas.JaasLoginServiceProvider">
        <description>This is Jaas Login Service Provider and is used
            to configure login module service instances</description>
    </serviceProvider>

    <serviceProvider name="policy.xml" type="POLICY_STORE"
        class="oracle.security.jps.internal.
            polycystore.xml.XmlPolicyStoreProvider">
        <description>XML-based PolicyStore</description>
    </serviceProvider>

    <serviceProvider type="POLICY_STORE" name="policy.oid"
        class="oracle.security.jps.internal.
            polycystore.ldap.LdapPolicyStoreProvider">
        <description>LDAP-based PolicyStore</description>
        <property name="polycystore.type" value="OID"/>
        <property name="connection.pool.maxsize" value="30"/>
        <property name="connection.pool.provider.type" value="idmpool"/>
    </serviceProvider>

    <serviceProvider type="AUDIT" name="audit.provider"
        class="oracle.security.jps.internal.audit.AuditProvider">
        <description>Audit Service</description>
    </serviceProvider>
</serviceProviders>

<serviceInstances>

    <serviceInstance name="credstore" provider="credstoressp" location="."/>
        <description>File Based Credential Store Service Instance</description>
    </serviceInstance>

    <serviceInstance name="idstore.xml" provider="idstore.xml.provider">
    <!-- Subscriber name must be defined for XML Identity Store -->
        <property name="subscriber.name" value="jazz.com"/>
    <!-- This is the location of XML Identity Store -->
        <property name="location" value="./user-data.xml"/>
    <!-- This property set defines the authenticated role -->
        <propertySetRef ref="authenticated.role.properties"/>
    </serviceInstance>
    <serviceInstance name="idstore.loginmodule"
        provider="jaas.login.provider">
        <description>Identity Store Login Module</description>
        <property name="loginModuleClassName" value="oracle.security.jps.internal.
            jaas.module.idstore.IdStoreLoginModule"/>
        <property name="jaas.login.controlFlag" value="REQUIRED"/>
        <property name="debug" value="true"/>
        <property name="addAllRoles" value="true"/>
    </serviceInstance>

```

```

<serviceInstance name="policystore.rdbms" provider="policy.rdbms">
  <property name="jdbc.url"
    value="jdbc:oracle:thin:@sc158116.domainexample.com:1521:orcl"/>
  <property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver"/>
  <property name="bootstrap.security.principal.key" value="keyname"/>
  <property name="bootstrap.security.principal.map" value="mapname"/>
  <property name="oracle.security.jps.ldap.root.name"
    value="cn=jpsTestNode"/>
  <property name="oracle.security.jps.farm.name"
    value="cn=wcai_view_jing.atzsrg"/>
</serviceInstance>

<serviceInstance name="policystore.rdbms.ds" provider="policy.rdbms">
  <property name="oracle.security.jps.ldap.root.name"
    value="cn=jpsTestNode"/>
  <property name="oracle.security.jps.farm.name"
    value="cn=wcai_view_jing.atzsrg"/>
  <property value="atzsrgds" name="datasource.jndi.name"/>
</serviceInstance>

<serviceInstance name="pdp.service" provider="pdp.service.provider">
  <property name="oracle.security.jps.runtime.pd.client.sm_name"
    value="{@atsrg.pdp.configuration_id}"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheEnabled" value="true"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheEvictionCapacity" value="500"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheEvictionPercentage" value="10"/>
  <property name="oracle.security.jps.pdp.
    AuthorizationDecisionCacheTTL" value="60"/>
  <property name="oracle.security.jps.ldap.
    policystore.refresh.interval" value="30000"/>
  <property name="oracle.security.jps.policystore.
    refresh.purge.timeout" value="600000"/> <!-- 10 minutes -->
  <property name="loading_attribute_backward_compatible" value="false"/>
<!-- Properties for controlled mode PD -->
  <property name="oracle.security.jps.runtime.
    pd.client.policyDistributionMode" value="non-controlled"/>
  <property name="oracle.security.jps.runtime.
    instance.name" value="{@atsrg.pdp.instance_name}"/>
</serviceInstance>

<serviceInstance name="policystore.oid" provider="policy.oid">
  <property name="max.search.filter.length" value="4096"/>
  <property name="bootstrap.security.principal.key" value="keyname"/>
  <property name="bootstrap.security.principal.map" value="mapname"/>
  <property name="ldap.url" value="ldap://sc158126.domainexample.com:3060"/>
  <property name="oracle.security.jps.ldap.root.name"
    value="cn=jpsTestNode"/>
  <property name="oracle.security.jps.farm.name"
    value="cn=wcai_view_jing.atzsrg"/>
  <property name="oracle.security.jps.policystore.resourcetypeenforcementmode"
    value="Lenient"/>
</serviceInstance>

<serviceInstance name="policystore.xml" provider="policy.xml"
  location="./system-jazn-data.xml"/>

```

```

<serviceInstance name="user.authentication.loginmodule"
  provider="jaas.login.provider">
  <description>User Authentication Login Module</description>
  <property name="loginModuleClassName"
    value="oracle.security.jps.internal.
      jaas.module.authentication.JpsUserAuthenticationLoginModule" />
  <property name="jaas.login.controlFlag" value="REQUIRED" />
</serviceInstance>

<serviceInstance name="user.assertion.loginmodule"
  provider="jaas.login.provider">
  <description>User Assertion Login Module</description>
  <property name="loginModuleClassName"
    value="oracle.security.jps.internal.
      jaas.module.assertion.JpsUserAssertionLoginModule" />
  <property name="jaas.login.controlFlag" value="REQUIRED" />
</serviceInstance>

<serviceInstance name="pip.service.ootb.ldap" provider="pip.service.provider">
  <property name="type" value="LDAP_PIP" />
  <property name="ldap.url"
    value="ldap://scl58126.domainexample.com:3060" />
  <property name="bootstrap.security.principal.key" value="keyname" />
  <property name="bootstrap.security.principal.map" value="mapname" />
  <property name="search.base" value="cn=pip_info_store,
    cn=wcai_view_jing.atzsrcg, cn=JPSContext, cn=jpsTestNode" />
  <property name="failed.server.retry.interval" value="10" />
</serviceInstance>
<!-- JPS Audit Service Instance-->
<serviceInstance name="audit" provider="audit.provider">
  <property name="audit.filterPreset" value="None" />
  <property name="audit.maxDirSize" value="0" />
  <property name="audit.maxFileSize" value="104857600" />
  <property name="audit.loader.jndi" value="jdbc/AuditDB" />
  <property name="audit.loader.interval" value="15" />
  <property name="audit.loader.repositoryType" value="File" />
</serviceInstance>

<serviceInstance name="pip.service.ootb.db" provider="pip.service.provider">
  <property name="type" value="RDBMS_PIP" />
  <property name="jdbc.url"
    value="jdbc:oracle:thin:@scl58116.domainexample.com:1521:orcl" />
  <property name="jdbc.driver" value="oracle.jdbc.driver.OracleDriver" />
  <property name="bootstrap.security.principal.key" value="keyname" />
  <property name="bootstrap.security.principal.map" value="mapname" />
  <property name="failed.server.retry.interval" value="10" />
</serviceInstance>

<serviceInstance name="pip.service.ootb.db.ds" provider="pip.service.provider">
  <property name="type" value="RDBMS_PIP" />
  <property value="atzsrcgds" name="datasource.jndi.name" />
  <property name="failed.server.retry.interval" value="10" />
</serviceInstance>
</serviceInstances>

<jpsContexts default="default">
  <jpsContext name="default">
    <serviceInstanceRef ref="policystore.oid" />
    <serviceInstanceRef ref="pdp.service" />
  </jpsContext>
</jpsContexts>

```

```

        <serviceInstanceRef ref="audit" />
        <serviceInstanceRef ref="idstore.xml" />
        <serviceInstanceRef ref="idstore.loginmodule" />
        <serviceInstanceRef ref="pip.service.ootb.ldap" />
        <serviceInstanceRef ref="pip.service.ootb.db" />
    </jpsContext>
    <jpsContext name="smsec">
        <serviceInstanceRef ref="credstore" />
    </jpsContext>

</jpsContexts>

</jpsConfig>

```

B.4 Configuring the Custom Attribute Retrievers Manually

To set up a custom attribute retriever manually, use the following section as an example.

Configuration information for attribute retrievers is defined in the `jps-config.xml` configuration file (used by Java EE containers) located in the `$DOMAIN_HOME/config/fmwconfig` directory. To set up custom attribute retrievers manually, use the following section as an example.

B.4.1 Configuring the `jps-config.xml` Configuration File

Review the following sections for examples on how to configure the `jps-config.xml` file for custom attribute retrievers.

Declaring the Custom Attribute Retriever Service Provider

[Example B-11](#) illustrates how the `serviceProvider` element defines the use of a custom attribute retriever by defining the internal Oracle Entitlements Server class.

Example B-11 Declaring Custom Attribute Retriever Service Provider

```

<serviceProvider
class="oracle.security.jps.az.internal.runtime.provider.PIPServiceProvider"
name="pip.service.provider" type="PIP" />

```

Specifying Custom Attribute Retriever Type and Classnames

Specify type as `CUSTOM_PIP`, and the classnames to the custom attribute retriever class full qualified name.

Example B-12 Specifying Custom Attribute Retriever Type and Classnames

```

<serviceInstance name="pip.service.MyAttributeRetriever"
provider="pip.service.provider">
    <property name="type" value="CUSTOM_PIP" />
    <property name="application" value="myapp" />
    <property name="description" value="custom pip" />
    <property name="classnames" value="com.mycompany.info.MyPip" />
</serviceInstance>

```

Declaring the Custom Attribute Retriever Reference in `jpsContext`

[Example B-13](#) illustrates how to declare the custom attribute retriever reference in the `jpsContext` element.

Example B-13 Declaring Custom Attribute Retriever Reference in jpsContext

```
<jpsContext name="default">
  <serviceInstanceRef ref="pip.service.MyAttributeRetriever"/>
  <serviceInstanceRef ref="pdp.service"/>
  <serviceInstanceRef ref="audit"/>
  <serviceInstanceRef ref="idstore.xml"/>
  <serviceInstanceRef ref="idstore.loginmodule"/>
  <serviceInstanceRef ref="pip.service.MyAttributeRetriever"/>
</jpsContext>
```

B.4.2 Implementing Custom PIP Interface

The class of custom PIP should implement the following interface, and the class should be added to the classpath of the security module:

Example B-14 Implementing Custom PIP Interface

```
package com.bea.security.providers.authorization.asi;

import java.util.Map;

import javax.security.auth.Subject;

import com.bea.security.providers.authorization.asi.ARME.evaluator.RequestHandle;

import weblogic.security.service.ContextHandler;
import weblogic.security.spi.Resource;

/**Version 2 interface for performing attribute retrieval, an implementation of an
<code>AttributeRetrieverV2</code> may be used to get embedded data from complex
data objects. Multiple retrievers may be registered for the same attribute name,
they will be called in order until one returns a non-null result. The difference
between Version 1 and Version 2 interface: Version 2 interface introduces a
RequestHandle parameter, from which the function is able to get ARME internal
system attributes.
*/

public interface AttributeRetrieverV2 {

    /**Returns the names of attributes handled by this object. An empty or
    <code>null</code> value indicates that the retriever will be considered
    capable of handling any attribute name.
    @return the names associated with this object*/
    String[] getHandledAttributeNames();

    /**retrieve the value of the named attribute. Additional authorization
    request data is made available to allow for more complex attribute
    retrieval.
    @param name the name of the needed attribute
    @param requestHandle the attributes container associated with the request,
    through which the function can get required attribute value.
    @param subject the subject associated with the request
    @param roles the role membership of the subject
    key: role name.
    value: role object
    <code>null</code> if function is called during role mapping
    @param resource the resource associated with the request
    @param contextHandler the context associated with the request, may be
```

```
        <code>>null</code> if non-existent
        @return the attributes value, or <code>>null</code> if not found
    */
    Object getAttributeValue(String name,
                            RequestHandle requestHandle,
                            Subject subject,
                            Map roles,
                            Resource resource,
                            ContextHandler contextHandler);

} //endof AttributeRetrieverV2
```

Configuring an Oracle Service Bus 12.1.3 Domain to Take Use of an OSB Security Module from OES 11.1.2.2

The Oracle Entitlements Server 11.1.2.2 Oracle Service Bus (OSB) Security Module supports an OSB (10.3.6) domain, but if you want to use an OSB 12c domain and you also want to use the OSB Security Module from OES 11.1.2.2 in the 12c OSB domain, follow the instructions in this appendix.

This appendix provides information on configuring the OSB 12c domain to take use of the OSB Security Module from OES 11.1.2.2.

C.1 Configuring an Oracle Service Bus 12.1.3 Domain to Take Use of an OSB Security Module from Oracle Entitlements Server 11.1.2.2

To set up the Oracle Service Bus (OSB) 12.1.3 domain to take use of an OSB Security Module from Oracle Entitlements Server 11g R2 PS2, proceed as follows:

1. Create the standard Oracle Service Bus (OSB) domain.
See "Configuring Your Oracle Service Bus Domain" in *Oracle Fusion Middleware Installing and Configuring Oracle Service Bus*.
2. Reassociate the OSB 12c domain from the 12c policy store to the 11g R2 PS2 (11.1.2.2) policy store.
 - a. Navigate to the `MW_HOME/oracle_common/common/bin` directory by running the following command on the command line:

```
cd MW_HOME/oracle_common/common/bin
```
 - b. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```
 - c. Use the Oracle Platform Security Services (OPSS) script `exportEncryptionKey` to extract the encryption key from the Oracle Entitlements Server 11g R2 PS2 (11.1.2.2) domain and export it into the `ewallet.p12` file.

At the WLST prompt, run the following command:

```
exportEncryptionKey(jpsConfigFile="/r2ps2/user_projects/domains/oes11gr2p2_domain/config/fmwconfig/jps-config.xml",keyFilePath="/tmp/key",keyFilePassword="password");
```

where

jpsConfigFile is the location of the file `jps-config.xml` relative to the location where the script is run.

keyFilePath is the path where you want to export the encryption key; note that the content of file is encrypted and secured by the value passed to *keyFilePassword*.

keyFilePassword is the password to secure the encryption key; note that this same password must be used when importing that file.

- d. Start the OSB 12.1.3 Administration Server and create a data source (`jdbc/opssds`) and target this data source to the Administration and Managed Servers of the OSB 12.1.3 domain. Make sure that the data source points to the OES Administration Server policy store.

For details on creating a JDBC data source, refer to "Create JDBC generic data sources" in the *Oracle Fusion Middleware Administering Oracle WebLogic Server with Fusion Middleware Control*.

- e. Navigate to the `MW_HOME/oracle_common/common/bin` directory by running the following command on the command line:

```
cd MW_HOME/oracle_common/common/bin
```

- f. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

- g. Reassociate the security store by running the following command:

```
reassociateSecurityStore(domain="oes_domain", servertype="DB_
ORACLE", jpsroot="cn=jpsroot", datasourcename="jdbc/opssds", jdbcurl="jdbc:or
acle:thin:@host:1521:orcl", dbUser="R2PS20SE_OPSS", dbPassword="db_
password", jdbcdriver="oracle.jdbc.xa.client.OracleXADataSource", join="true
", migrate="true",
skip="true", keyFilePath="/tmp/key", keyFilePassword="password")
```

where

domain is the `oracle.security.jps.farm.name` value in the Oracle Entitlements Server Administration Server `jps-config.xml`.

jpsroot is the `oracle.security.jps.ldap.root.name` value in the Oracle Entitlements Server Administration Server `jps-config.xml`.

keyFilePath is the path of the directory where the encryption key was exported. Use the same *keyFilePath* that was used for the `exportEncryptionKey` command.

keyFilePassword is the password that secures the encrypted key. You must use the same password that was used for the `exportEncryptionKey` command.

For details, refer to "Reassociating Domain Stores with the Command `reassociateSecurityStore`" in *Oracle Fusion Middleware Securing Applications with Oracle Platform Security Services*.

3. Copy the `jps-atz-wls-proxyproviders.jar` file, which can be obtained from the 11g R2 PS2 (11.1.2.2) OES client, to the WebLogic 12c location:

```
WLS_HOME/wlserver/server/lib/mbeantypes
```

4. Restart all servers.

5. Configure the Authorization provider.

For details on configuring an Authorization provider, refer to "Configuring Authentication Providers" in the *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

6. Configure the Role Mapping provider.

For details on configuring a Role Mapping provider, refer to "Configuring a Role Mapping Provider" in the *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

7. Restart all servers including the Administration and Managed Servers.

C.2 Configuring OSB Security

To configure OSB security, perform the following steps:

1. Start the Oracle Service Bus Console by entering:

```
http://osb_domain_host:osb_admin_port/servicebus/
```

2. Create the OESAAuthorizationProxy and OESRoleMapperProxy in the Oracle Service Bus Console under Realm.
3. Configure transport-level security as follows:
 - a. Navigate to the Proxy Service which you want to protect.
 - b. Click **Configuration** and then **Transport Details**.
 - c. Change **Authentication** to **Basic**.
4. Configure message-level security as follows:
 - a. Navigate to the Proxy Service which you want to protect.
 - b. Click **Security** and then **Security Setting**.
 - c. Change **Custom Authentication** to **Custom User Name and Password**.

Configuring Enterprise Role Based Authorization for Oracle API Gateway and OES Integration

This chapter provides instructions on how to configure services and PEP calls for authorization against a group based policy. Group (also known as enterprise role) based access control is the best practice recommended by Oracle Entitlements Server. Oracle Entitlements Server can retrieve group information by user name with the OPSS user assertion login module. This will require an identity store configured in the OES configuration (jps-config.xml).

D.1 Configure LDAP Identity Store

To configure the LDAP Identity Store, you need to perform the following tasks:

- [Section D.1.1, "Add LDAP Identity Store Instance"](#)
- [Section D.1.2, "Add idstore.oid Instance into Default Context"](#)
- [Section D.1.3, "Add LDAP Principal to Bootstrap Credential Store"](#)

D.1.1 Add LDAP Identity Store Instance

Add the following Identity store service instance into *SM_INSTANCE_HOME/config/jps-config.xml*, within the `<serviceInstances>` tag. For more information about identity store configuration, see "Configuring the Identity Store Service" in *Oracle Fusion Middleware Application Security Guide*.

Update the bold attribute values according to your LDAP information.

```
<serviceInstance name="idstore.oid" provider="idstore.ldap.provider">
  <property name="subscriber.name" value="dc=usmedium,dc=oracle,dc=com" />
  <property name="idstore.type" value="OID" />
  <property name="ldap.url" value="ldap://<host>:<port>" />
  <property name="bootstrap.security.principal.map" value="oidstore"/>
  <property name="bootstrap.security.principal.key" value="mykey"/>
  <extendedProperty>
    <name>user.search.bases</name>
    <values>
      <value>cn=users,dc=us,dc=oracle,dc=com</value>
    </values>
  </extendedProperty>
  <extendedProperty>
    <name>group.search.bases</name>
    <values>
      <value>cn=groups,dc=us,dc=oracle,dc=com</value>
    </values>
  </extendedProperty>
</serviceInstance>
```

```
        </values>
    </extendedProperty>
    <property name="username.attr" value="uid" />
    <property name="groupname.attr" value="cn" />
</serviceInstance>
```

D.1.2 Add idstore.oid Instance into Default Context

Add the identity store instance into the default context as shown below:

```
<jpsContexts default="default">
  <jpsContext name="default">
    <serviceInstanceRef ref="audit"/>
    <serviceInstanceRef ref="credstore"/>
    <serviceInstanceRef ref="idstore.oid"/>
    <serviceInstanceRef ref="pdp.service"/>
  </jpsContext>
</jpsContexts>
```

D.1.3 Add LDAP Principal to Bootstrap Credential Store

Use `oesPassword.sh/bat` to set the LDAP Principal to the bootstrap credential store. In [Section D.1.1](#), "oidstore", "mykey" were used as the map-key in the bootstrap credential store. You need to use `oesPassword.sh/bat` to set up the LDAP connection user and the password into bootstrap credential store.

```
bash-3.2$ ./oesPassword.sh -setpass
Enter credential map name: oidstore
Enter credential key name: mykey
Enter username for map:oidstore key:mykey: cn=orcladmin
Enter password for map:oidstore key:mykey:
Enter password for map:myid key:mykey again:
```

D.2 Use Username in String as SubjectObj for PepRequest

```
PepRequestFactory pepRequestFactory =
PepRequestFactoryImpl.getPepRequestFactory();

String username; // get username from your OAG integration context
String resource; // get request resource from OAG integration context
String action; // get request action from OAG integration context

PepRequest request = pepRequestFactory.newPepRequest(username, action, resource);
PepResponse response = request.decide();
```

Managing Advanced Policies with WLST

The WebLogic Scripting Tool (WLST) is a command-line scripting interface that system administrators and operators use to monitor and manage WebLogic Server instances and domains. This Appendix documents the commands to manage advanced policies with Oracle Entitlements Server using the WLST. It contains the following sections.

- Section E.1, "Using the WebLogic Scripting Tool with Oracle Entitlements Server"
- Section E.2, "Using the WLST Commands"
- Section E.3, "Creating Policy with a Script"

E.1 Using the WebLogic Scripting Tool with Oracle Entitlements Server

The WLST scripting environment is based on Jython, the Java scripting interpreter. By following the Jython language syntax, Oracle Entitlements Server extends the scripting language to allow for management of advanced policies. The new scripts are supported on the WebLogic Application Server, the WebSphere Application Server and the JBossApplication Server in both offline and online modes. The following links offer more information on the WLST and related subjects.

- <http://www.jython.org/>
- *Oracle Fusion Middleware Oracle WebLogic Scripting Tool*

The following sections in this book document the general process for creating a simple policy and adding advanced elements to it.

- Section 4.2, "Defining an Authorization Policy And Its Components"
- Section 4.3, "Adding Fine-Grained Elements to an Authorization Policy"

E.2 Using the WLST Commands

This section describes the WLST commands in both online mode. Offline mode is not supported.

- `createApplicationPolicy`
- `updateResourceType`
- `updateResource`
- `createPolicy`
- `updatePolicy`
- `deletePolicy`

- listPolicies
- createAttribute
- updateAttribute
- deleteAttribute
- listAttributes
- createFunction
- updateFunction
- deleteFunction
- listFunctions
- getFunction
- listAppRoles

E.2.1 createApplicationPolicy

Create an Application (also referred to as an Application Policy) using the specified name.

Interactive Mode

```
createApplicationPolicy(appStripe="<appStripeName>")
```

Script Mode

```
./wlst.sh createAdvancedPolicy.py -appStripe <appStripeName>
```

Arguments

- appStripeName – name of the Application Policy to be created.

E.2.2 updateResourceType

Update the specified Resource Type with the new properties.

Interactive Mode

```
updateResourceType(appStripe="<appStripeName>",  
resourceTypeName="<resourceTypeName>",  
displayName="<displayName>", description="<description>",  
allowedActions="<actions>", delimiter="<delimiter>",  
attributes="<attributes>", provider="<resTypeProvider>",  
matcher="<matcherClass>", hierarchicalResource="<hierarchicalResource>",  
resourceNameDelimiter="<resourceNameDelimiter>")
```

Script Mode

```
./wlst.sh updateResourceType.py -appStripe <appStripeName>  
-resourceTypeName <resourceTypeName> [-displayName <displayName>]  
[-description <description>] [-allowedActions <actions>]  
[-delimiter <delimiter>]  
[-attributes <attributes>] [-provider <resTypeProvider>]  
[-matcher <matcherClass>]  
[-hierarchicalResource <hierarchicalResource>  
[-resourceNameDelimiter <resourceNameDelimiter>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `resourceTypeName` – Name of the Resource Type to be updated. Required.
- `displayName` – Display name for the Resource Type. Optional.
- `description` – Short description of the Resource Type. Optional.
- `actions` - A comma-separated list of the allowed action(s) to be added or removed from the Resource Type. Actions prefixed with a dash (-) will be removed from the list; those without the prefix will be added to the list. Optional.
- `delimiter` – The delimiter used in the actions list. If unspecified, a comma is the default (,). Optional.
- `attributes` – A comma-separated list of attribute name(s) to be added or removed from the attribute set of the Resource Type. Attribute names prefixed with a dash (-) will be removed from the list; those without the prefix will be added to the list. Optional. Can be null.
- `resTypeProvider` – Provider class name for this Resource Type. Optional. Can be null.
- `matcherClass` – Matcher class name for this Resource Type. If unspecified, the default matcher class used is `oracle.security.jps.ResourcePermission`. Optional. Can be null.
- `hierarchicalResource` - Flag showing whether the Resource Type supports hierarchical resources. It is an optional parameter with a default value of false. Can be null.
- `resourceNameDelimiter` - Character to be used as a delimiter in names of hierarchical resources of this Resource Type. It is an optional parameter with a default value of a forward slash (/). A value should not be provided if the `hierarchicalResource` parameter is not given a value of true.

E.2.3 updateResource

Update the specified Resource with the new properties.

Interactive Mode

```
updateResource (appStripe="<appStripeName>", resourceName="<resourceName>",
  type="<resourceType>", displayName="<displayName>", description="<description>",
  attributes="<attributes>")
```

Script Mode

```
./wlst.sh updateResource.py -appStripe <appStripeName>
  -resourceName <resourceName> -type <resourceType> [-displayName <displayName>]
  [-description <description>] [-attributes <attributes>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `resourceName` – Name of Resource to be updated. Required.
- `type` – Name of the Resource Type associated with the Resource. Required.
- `displayName` – Display name for the Resource Type. Optional.

- description – Short description of the Resource Type. Optional.
- attributes – A semi-colon separated list of attribute(s) to be added or removed from the Resource's attribute set. Optional. The following rules govern how to write an attribute value.
 1. To add a single-valued attribute, the format is <attribute name>:<value>
 2. To add a multi-valued attribute, the format is <attribute name>:<value 1>,<value 2>,...,<value n>
 3. To remove an attribute, the format is -<attribute name>

E.2.4 createPolicy

Create a new Policy within the specified Application.

Interactive Mode

```
createPolicy (appStripe="<appStripeName>", policyName="<policyName>",
  [displayName="<displayName>"], [description="<description>"],
  ruleExpression="<ruleExpression> {entitlements="<entitlements>" |
  resourceActions="<resActions>"},
  {principals="<principals>"|-codeSource="<codeSource>"}",
  [obligations="<obligations>"], [semantic="<semantic>"]
```

Script Mode

```
./wlst.sh createPolicy.py -appStripe <appStripeName>
-policyName <policyName> [-displayName <displayName>]
[-description <description>] -ruleExpression <ruleExpression>
{-entitlements <entitlements>|-resourceActions <resActions>}
{-principals <principals>|-codeSource <codeSource>}
[-obligations <obligations>] [-semantic <semantic>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- policyName – Name of policy to be created. Required.
- displayName – Display name for the Policy. Optional.
- description – Short description of the Policy. Optional.
- ruleExpression – A rule expression is evaluated for the policy decision. Required. The following rules govern how to write an expression.
 1. The ruleExpression begins with a name. The name is followed by a colon (:) which is then followed by an effect (GRANT/DENY). The effect is followed by a second colon (:) and an expression. The expression is comprised of functions and attributes. If there is no Condition to be evaluated for the ruleExpression, the second colon (:) and the expression following it are not required.
 2. All functions, including built-in ones are specified as a valid function name followed by a list of parameters enclosed within parentheses [()].
 3. Attributes and function names must be valid Java identifiers.
 4. Integer literal parameters begin with a digit between 1-9 followed by digits between 0-9. They can optionally be prefixed by a dash (-) for negative integers.
 5. String literals are enclosed within double quotes (" ").

6. Date and Time literals are specified as GMT strings followed by the letter `d` and `t`, respectively. Case-insensitive.
 7. Standard DataTypes supported are `string`, `int`, `boolean`, `date` and `time`.
 8. Supported Operators: `&&` and `||` are used to combine two boolean expressions. `!` is used on a boolean expression. `==` is used to check equality between two strings, integers, dates or times. `>`, `<`, `>=` and `<=` is used to compare two integers, dates or times.
 9. All operators and functions besides `&&`, `||` and `!` take only values and attributes as parameters. The others can take boolean expressions as well as parameters.
- entitlements – A comma-separated list of Permission Set entry name(s). Should be present only if `resActions` (Resource actions) is absent.
 - resActions – A comma-separated list of Resource action(s). Should be present only if entitlements is absent. Resource actions are specified as an existing Resource Type followed by a colon (:). This is then followed by an existing Resource name, followed by a comma-separated list (within parentheses) of valid actions for the Resource. For example:

`resType1:res1(act1, act2),resType2:res2(act1),resType2:res3(act2)`
 - principals – A comma-separated list of Principals. Should be present only if `codeSource` is absent. Principals are specified as a name followed by a colon (:) and a fully-qualified class-name. For example:

`admin:com.example.myPrincipal, manager:com.example.myPrincipal`
 - codeSource – Code-source as a string. It should be present only if Principals are absent. Optional.
 - obligations – A comma-separated list of Obligations. Optional. Obligations are specified as an Obligation name followed by a comma-separated list of Obligation attribute assignments within parentheses. If the assignment is a literal, it must be prefixed by a name followed by a colon (:). When assignment is an attribute, the name is optional. For example:

`obl(attr1,str1:"a String"),ob2(a2:attr2)`
 - semantic – Either `and` or `or` can be chosen as the policy semantic. Optional.

E.2.5 updatePolicy

Update an existing Policy in the specified application.

Interactive Mode

```
updatePolicy (appStripe="<appStripeName>", policyName="<policyName>",
 [displayName="<displayName>"], [description="<description>"],
 [ruleExpression="<ruleExpression>"], [obligations="<obligations>"],
 [entitlements="<entitlements>"]|resourceActions="<resActions>"],
 [principals="<principals>"]|codeSource="<codeSource>"])
```

Script Mode

```
./wlst.sh updatePolicy.py -appStripe <appStripeName>
-policyName <policyName> [-displayName <displayName>]
[-description <description>] [-ruleExpression <ruleExpression>]
[-obligations <obligations>]
```

```
[-entitlements <entitlements>|-resourceActions <resActions>]
[-principals <principals>|-codeSource <codeSource>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `policyName` – Name of policy to be updated. Required.
- `displayName` – Display name for the Policy. Optional.
- `description` – Short description of the Policy. Optional.
- `ruleExpression` – A rule expression is evaluated for the policy decision. Required. The following rules govern how to write an expression.
 1. The `ruleExpression` begins with a name. The name is followed by a colon (:) which is then followed by an effect (GRANT/DENY). The effect is followed by a second colon (:) and an expression. The expression is comprised of functions and attributes. If there is no Condition to be evaluated for the `ruleExpression`, the second colon (:) and the expression following it are not required.
 2. All functions, including built-in ones are specified as a valid function name followed by a list of parameters enclosed within parentheses [()].
 3. Attributes and function names must be valid Java identifiers.
 4. Integer literal parameters begin with a digit between 1-9 followed by digits between 0-9. They can optionally be prefixed by a dash (-) for negative integers.
 5. String literals are enclosed within double quotes (" ").
 6. Date and Time literals are specified as GMT strings followed by the letter `d` and `t`, respectively. Case-insensitive.
 7. Standard DataTypes supported are `string`, `int`, `boolean`, `date` and `time`.
 8. Supported Operators: `&&` and `||` are used to combine two boolean expressions. `!` is used on a boolean expression. `==` is used to check equality between two strings, integers, dates or times. `>`, `<`, `>=` and `<=` is used to compare two integers, dates or times.
 9. All operators and functions besides `&&`, `||` and `!` take only values and attributes as parameters. The others can take boolean expressions as well as parameters.
- `entitlements` – A comma-separated list of Permission Set entry name(s). Should be present only if `resActions` (Resource actions) is absent.
- `resActions` – A comma-separated list of Resource action(s). Should be present only if `entitlements` is absent. Resource actions are specified as an existing Resource Type followed by a colon (:). This is then followed by an existing Resource name, followed by a comma-separated list (within parentheses) of valid actions for the Resource. For example:


```
resType1:res1(act1, act2),resType2:res2(act1),resType2:res3(act2)
```
- `principals` – A comma-separated list of Principals. Should be present only if `codeSource` is absent. Principals are specified as a name followed by a colon (:) and a fully-qualified class-name. For example:


```
admin:com.example.myPrincipal, manager:com.example.myPrincipal
```

- `codeSource` – Code-source as a string. It should be present only if Principals are absent. Optional.
- `obligations` – A comma-separated list of Obligations. Optional. Obligations are specified as an Obligation name followed by a comma-separated list of Obligation attribute assignments within parentheses. If the assignment is a literal, it must be prefixed by a name followed by a colon (:). When assignment is an attribute, the name is optional. For example:

```
ob1(attr1,str1:"a String"),ob2(a2:attr2)
```

E.2.6 deletePolicy

Remove an existing Policy from the specified application.

Interactive Mode

```
deletePolicy (appStripe="<appStripeName>", policyName="<policyName>")
```

Script Mode

```
./wlst.sh deletePolicy.py -appStripe <appStripeName> -policyName <policyName>
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `policyName` – Name of policy to be updated. Required.

E.2.7 listPolicies

List the Policies in the specified Application.

Interactive Mode

```
listPolicies (appStripe="<appStripeName>")
```

Script Mode

```
./wlst.sh listPolicies.py -appStripe <appStripeName>
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.

E.2.8 createAttribute

Create a new Attribute in an application. Default attributes are not supported.

Interactive Mode

```
createAttribute (appStripe="<appStripeName>", attributeName="<attributeName>",
 [displayName="<displayName>"], [description="<description>"], type="<type>",
 category="<category>", [isSingle="<true/false>"], [values="<values>"])
```

Script Mode

```
./wlst.sh createAttribute.py -appStripe <appStripeName>
-attributeName <attributeName> [-displayName <displayName>]
[-description <description>] -type <type> -category <category>
```

```
[-isSingle <true/false>][-values <values>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- attributeName – Name of the attribute to be created. Required.
- displayName – Display name for the attribute. Optional.
- description – Short description of the attribute. Optional.
- type - Fully qualified class name of the type. Required.
- category - Attribute category. Either "Dynamic" or "Resource". Required.
- isSingle – Whether the attribute is single-valued or multiple-valued. Default value is true. Optional.
- values – Initial attribute values. Optional.

E.2.9 updateAttribute

Update values of an Attribute already defined in an Application. Default attributes are not supported.

Interactive Mode

```
updateAttribute (-appStripe=<appStripeName>, attributeName=<attributeName>,
 [displayName=<displayName>], [description=<description>],
 [values=<values>])
```

Script Mode

```
./wlst.sh updateAttribute.py -appStripe <appStripeName>
-attributeName <attributeName> [-displayName <displayName>]
[-description <description>] [-values <values>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- attributeName – Name of the Attribute to be created. Required.
- displayName – Display name for the Attribute. Optional.
- description – Short description of the attribute. Optional.
- values - A comma-separated list of Attribute values. In the case where this value is an empty string, the Attribute will be updated to have no assigned value. Optional.

E.2.10 deleteAttribute

Delete the specified Attribute from the specified Application. Default Attributes are not supported.

Interactive Mode

```
deleteAttribute (appStripe=<appStripeName>, attributeName=<attributeName>,
 [cascade=<true/false>])
```

Script Mode

```
./wlst.sh deleteAttribute.py -appStripe <appStripeName>
-attributeName <attributeName>
[-cascade <true/false>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- attributeName – Name of the Attribute to be created. Required.
- cascade – A boolean value indicating whether the delete is to be cascaded. If unspecified, the value defaults to false. Optional.

E.2.11 listAttributes

List all Attributes defined in the given Application.

Online Mode

```
listAttributes (appStripe="<appStripeName>", [hideBuiltIn="<hideBuiltIn>"])
```

Offline Mode

```
./wlst.sh listAttributes.py -appStripe <appStripeName>
[-hideBuiltIn <hideBuiltIn>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- hideBuiltIn – A boolean value indicating whether to hide built-in attributes. The value defaults to true. Optional.

E.2.12 createFunction

Create a Function in the specified Application.

Interactive Mode

```
createFunction (appStripe="<appStripeName>", functionName="<functionName>",
[displayName="<displayName>"], [description="<description>"],
className="<className>", returnType="<returnType>",
[paramTypes="<paramTypes>"])
```

Script Mode

```
./wlst.sh createFunction.py -appStripe <appStripeName>
-functionName <functionName> [-displayName <displayName>]
[-description <description>] -className <className>
-returnType <returnType> [-paramTypes <paramTypes>]
```

Arguments

- appStripeName – The Application (also referred to as an Application Policy) name. Required.
- functionName – Name of the Function being created. Required.
- displayName – Display name for the Function. Optional.
- description – Short description of the Function. Optional.

- `className` - Name of the class to which the function belongs. Required.
- `returnType` – Return type of the Function. Required.
- `paramTypes` – List the types of parameters concatenated using a comma (,). If unspecified, the function doesn't take any parameter as input. Optional.

E.2.13 updateFunction

Update the Function with the given values.

Interactive Mode

```
updateFunction (appStripe="<appStripeName>", functionName="<functionName>"
 [displayName="<displayName>"], [description="<description>"],
 [-className="<className>"], [returnType="<returnType>"],
 [paramTypes="<paramTypes>"])
```

Script Mode

```
./wlst.sh updateFunction.py -appStripe <appStripeName>
 -functionName <functionName> [-displayName <displayName>]
 [-description <description>] [-className <className>]
 [-returnType <returnType>] [-paramTypes <paramTypes>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `functionName` – Name of the Function being updated. Required.
- `displayName` – Display name for the Function. Optional.
- `description` – Short description of the Function. Optional.
- `className` - Name of the class to which the Function belongs. Required.
- `returnType` – Return type of the Function. Required.
- `paramTypes` – List the types of parameters concatenated using a comma (,). If unspecified, parameter types of the function are not changed. If an empty string is the value, the Function is updated to take no input parameter. Optional.

E.2.14 deleteFunction

Delete the Function in the specified Application.

Interactive Mode

```
deleteFunction (appStripe="<appStripeName>", functionName="<functionName>",
 [cascade="<true/false>"])
```

Script Mode

```
./wlst.sh deleteFunction.py -appStripe <appStripeName>
 -functionName <functionName> [-cascade <true/false>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `functionName` – Name of the Function being updated. Required.

- `cascade` – A boolean value indicating whether the delete is to be cascaded. If unspecified, the value defaults to false. Optional.

E.2.15 listFunctions

List all Functions in the specified Application.

Interactive Mode

```
listFunctions (appStripe="<appStripeName>", [hideBuiltIn="<hideBuiltIn>"])
```

Script Mode

```
./wlst.sh listFunctions.py -appStripe <appStripeName>
[-hideBuiltIn <hideBuiltIn>]
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `hideBuiltIn` – A boolean value indicating whether to hide built-in functions. The value defaults to true. Optional.

E.2.16 getFunction

Get details of the given Function in the specified Application.

Interactive Mode

```
getFunction (appStripe="<appStripeName>", functionName="<functionName>")
```

Script Mode

```
./wlst.sh getFunction.py -appStripe <appStripeName>
-functionName <functionName>
```

Arguments

- `appStripeName` – The Application (also referred to as an Application Policy) name. Required.
- `functionName` – Name of the Function being obtained.

E.2.17 listAppRoles

Lists all roles with a given application stripe.

Interactive Mode

```
listAppRoles (appStripe="<appName>")
```

Script Mode

```
./wlst.sh listAppRoles.py -appStripe <myApp>
```

Arguments

- `appStripe` - Specifies an application stripe. Required

E.2.18 getResourceType

Online command that fetches a resource type from the domain policy store within a given application stripe.

Interactive Mode

```
getResourceType(appStripe, resourceName)
```

Script Mode

```
wls:/mydomain/serverConfig> getResourceType(appStripe="myApplication",
resourceTypeName="myResType")
```

Arguments

- appStripe - Specifies the application stripe from where to fetch the resource type.
- resourceName - Specifies the name of the resource type to fetch.

E.2.19 getResource

Prints the Resource of a given ResourceType.

E.3 Creating Policy with a Script

[Example E-1](#) illustrates how to create a single policy with a rule (containing one attribute comparison and one function invocation) and with an Obligation (containing two Obligation attributes).

Example E-1 Sample Script For Policy Creation

```
createApplicationPolicy(appStripe="jpsWebApp_wlst_test")
createResourceType(appStripe="jpsWebApp_wlst_test", resourceName="resType1",
  provider="myProvider", matcher="myMatcher",
  allowedActions="action1,action2", delimiter=",")
createResourceType(appStripe="jpsWebApp_wlst_test", resourceName="resType2",
  provider="myProvider", matcher="myMatcher",
  allowedActions="action1,action2", delimiter=",")
createResource(appStripe="jpsWebApp_wlst_test",name="res1",type="resType1")
createResource(appStripe="jpsWebApp_wlst_test",name="res2",type="resType2")
createResource(appStripe="jpsWebApp_wlst_test",name="res3",type="resType2")
createAttribute(appStripe="jpsWebApp_wlst_test", attributeName="attr1",
  type="date", category="dynamic")
createAttribute(appStripe="jpsWebApp_wlst_test", attributeName="attr2",
  type="time", category="dynamic")
createAttribute(appStripe="jpsWebApp_wlst_test", attributeName="abc",
  type="int", category="dynamic")
createAttribute(appStripe="jpsWebApp_wlst_test", attributeName="c",
  type="int", category="dynamic")
createAttribute(appStripe="jpsWebApp_wlst_test", attributeName="aString",
  type="string", category="dynamic")
createFunction(appStripe="jpsWebApp_wlst_test", functionName="boolFunction",
  className="com.example.myClassName",
  returnType="oracle.security.jps.service.policystore.info.OpssBoolean")
paramTypes="oracle.security.jps.service.policystore.infoOpssString,
oracle.security.jps.service.policystore.info.OpssInteger")
createPolicy(appStripe="jpsWebApp_wlst_test", policyName="policy1",
  ruleExpression="rule1:grant: !(abc > -1162) && (c==2)&& (\\"a String\\" ==
  aString)", resourceActions="resType1:res1(act1,
  act2),resType2:res2(act1),resType2:res3(act2)",
```

```
principals="admin:com.example.MyPrincipal", obligations="ob3(attr1, str1:\\"a
String\"), ob4(a2:attr2)", semantic="or"
updatePolicy(appStripe="jpsWebApp_wlst_test", policyName="policy1",
ruleExpression="rule3:deny:boolFunction(\"abc\",c)",
resourceActions="-resType2:res3(act2), resType2:res3(act1)",
obligations="-ob1, email(addr:\\"me@mycompany.com\\")")
listPolicies(appStripe="jpsWebApp_wlst_test")
deletePolicy(appStripe="jpsWebApp_wlst_test", policyName="policy1")
```


A

ABAC, 1-9, 1-10
access control
 and Oracle Entitlements Server, 1-2
 supported standards, 1-9
 understanding, 1-1
Admin Policy
 Administration Role
 Admin Policy, 11-4
Administration Console
 authorization management, 3-8
 customize, 12-1
 Home area, 3-10
 log in, 3-5
 Navigation Panel, 3-8
 online help, 3-11
 overview, 3-4
 searches, 5-1
 sign out, 3-6
 system configuration, 3-8
 using, 3-7
Administrator Roles
 managing, 11-8
 SystemAdmin, 3-4
administrators, 3-4
advanced
 policy simulation, 13-1
advanced search, 5-3
anonymous role, 4-17
Application
 administration, 11-3
 defined, 4-1
 managing, 4-6
Application Roles
 managing, 4-16, 4-21
application roles, 5-6
applications, 5-4
architecture
 authorization process flow, 1-8
 Policy Administration Point, 1-4
 Policy Decision Point, 1-5
 Policy Enforcement Point, 1-5
 Policy Information Point, 1-8
 security modules, 1-7
Attribute

 managing, 4-29
Attribute Retrievers
 predefined, B-1
 attribute retrievers, 1-8, B-1
attribute-based access control
 see ABAC, 1-10
attributes, 5-11
auditing, 13-6
 more information, 13-13
authenticated role, 4-17
authorization
 process flow, 1-8
authorization management, 3-8
authorization policies, 5-9
Authorization Policy, 2-1
 and Obligations, 4-19
 defined, 2-1
 managing, 4-16
Authorization Policy Manager
 as console, 1-2
 see Administration Console, 3-4
Az API, 1-9, 1-11

C

cache
 configuring, 13-22
case sensitivity, 5-13
coarse grained authorization, 1-1
Condition
 managing, 4-33
configuration
 debugging, 13-26, 13-32
 logging, 13-26
console
 and Authorization Policy Manager, 1-2
customizations
 Administration Console, 12-1

D

datastore
 access, B-12
debug parameters, 13-26
debugging, 13-25
 configuration, 13-26

- Java Security Module, 13-26
 - policy distribution, 13-32
 - searching logs, 13-27
 - WebLogic Server Security Module, 13-27
 - with methods, 13-32
- delegating administration, 11-1, 11-3, 11-5, 11-7
- Discovery Mode
 - WebLogic Server, 9-15, 9-16
- documentation
 - additional, xxv

E

- elements
 - of policies, 4-3
- Entitlements
 - managing, 4-13
- entitlements, 5-8
- Extensions
 - managing, 4-29
- external roles, 5-4

F

- fine grained authorization, 1-1
- FIPS, 13-6
- Function
 - managing, 4-29
- functions, 5-12

G

- Global
 - defined, 4-1
 - Security Modules, 10-1
 - system administrators, 11-8
- glossary, 2-4
 - Application, 2-4
 - Application Role, 2-4
 - Attributes, 2-5
 - Authorization Policy, 2-5
 - Condition, 2-5
 - Entitlement, 2-5
 - External Role, 2-5
 - Functions, 2-6
 - Obligation, 2-6
 - Policy Domain, 2-6
 - policy store, 2-6
 - Principal, 2-6
 - Resource, 2-6
 - Resource Type, 2-7
 - Role Category, 2-7
 - Role Mapping Policy, 2-7
- grants
 - OPSS, 3-5, 4-19, 5-11

H

- hierarchical resource types, 4-9
- Home area, 3-10

I

- identity store
 - LDAP configuration, 3-1
- installation, 3-1

J

- Java 2 permissions, 1-9
- Java permissions, 1-10
- JCE providers, 13-6
- jps-config.xml, A-1

L

- log in, 3-5
- log out, 3-6
- logging, 13-23
 - debug configuring, 13-26
 - searching logs, 13-27

M

- methods
 - debugging, 13-32
- migrating policies, 13-13
 - Database to XML, 13-20
 - LDAP to XML, 13-15
 - XML to Database, 13-17
 - XML to LDAP, 13-13

N

- Navigation Panel, 3-8

O

- object names, 5-13
- Obligations
 - creating, 4-19
- online help, 3-11
- OpenAz framework, 1-11
- OPSS
 - system grants, 3-5, 4-19, 5-11
- Oracle Entitlements Server, 1-2
 - architecture, 1-3
 - features, 1-3
 - install, 3-1
 - previous releases, 1-2

P

- PAP, 1-4
- parameters
 - configuration, A-1
 - installation, A-1
 - PDP Proxy Client, A-27
 - policy distribution, A-1
 - policy store, A-30
 - Security Modules, A-17
- PDP, 1-5

- PDP Proxy Client, 8-14
 - parameters, A-27
- PEP, 1-5
- permissions
 - Java, 1-10
- PIP, 1-8
 - see Attribute Retrievers, B-1
- PIP credentials, B-12
- policies
 - simulation, 13-1
- policy
 - creation
 - additional elements, 4-3
 - defining procedure, 4-2
 - definition procedure
 - additional elements, 4-3
 - migrating, 13-13
- Policy Administration Point, 1-4
- policy creation, 4-2
- Policy Decision Point, 1-5
- policy distribution
 - debugging, 13-32
 - overview, 6-2
 - parameters, A-1
 - procedure, 6-4
- Policy Domain
 - administration, 11-7
 - overview, 11-5
- Policy Enforcement Point, 1-5
- policy evaluation, 2-4
- Policy Information Point, 1-8
- policy objects
 - Application, 4-6
 - Application Roles, 4-16, 4-21
 - Attribute, 4-29
 - Authorization Policy, 4-16
 - Condition, 4-33
 - defined, 2-4
 - Application, 2-4
 - Application Role, 2-4
 - Attributes, 2-5
 - Authorization Policy, 2-5
 - Condition, 2-5
 - Entitlement, 2-5
 - External Role, 2-5
 - Functions, 2-6
 - Obligation, 2-6
 - Policy Domain, 2-6
 - policy store, 2-6
 - Principal, 2-6
 - Resource, 2-6
 - Resource Type, 2-7
 - Role Category, 2-7
 - Role Mapping Policy, 2-7
 - definitions, 2-4
 - Entitlements, 4-13
 - Extensions, 4-29
 - Function, 4-29
 - management, 4-1
 - Resource, 4-10

- Resource Types, 4-7
- Role Catalog, 4-16, 4-21
- Role Category, 4-28
- Role Mapping Policy, 4-25
 - search, 5-3, 5-4, 5-5, 5-6, 5-7, 5-8, 5-9, 5-11, 5-12
- policy simulator, 13-1
- policy store
 - parameters, A-30
- policy types, 2-1
 - Authorization Policy, 2-1
 - evaluating, 2-4
 - Role Mapping Policy, 2-2
- policy use case, 2-7
- pop-up search box, 5-1

R

- RBAC, 1-9, 1-10
- Resource
 - managing, 4-10
- Resource Types
 - managing, 4-7
- resource types, 5-5
 - hierarchical, 4-9
- resources, 5-7
 - SharePoint, 9-3
 - WebLogic Server, 9-15
- Role Catalog, 4-16, 4-21
- Role Category
 - defined, 2-7
 - managing, 4-28
- role mapping policies, 5-6
- Role Mapping Policy, 2-2
 - defined, 2-1
 - managing, 4-25
- role-based access control
 - see RBAC, 1-10
- roles
 - assigning, 2-2

S

- search
 - Administration Console, 5-1
 - advanced, 5-3
 - application roles, 5-6
 - applications, 5-4
 - attributes, 5-11
 - authorization policies, 5-9
 - entitlements, 5-8
 - external roles, 5-4
 - functions, 5-12
 - pop-up search, 5-1
 - resource types, 5-5
 - resources, 5-7
 - role mapping policies, 5-6
 - simple, 5-2
 - users, 5-12
- searching logs, 13-27
- Security Modules

- configuring, 10-1
- Java
 - debug, 13-26
 - parameters, A-17
 - WebLogic Server
 - debug, 13-27
- security modules
 - and WebLogic Server, 9-16
 - architecture, 1-7
 - as PDP, 1-5
 - as PDP / PEP, 1-6
 - deploying, 9-1
 - java configuration, 8-5
 - PDP Proxy Client, 8-14
 - start SMConfig UI, 8-2
 - types, 1-7, 9-1, 9-3
- security providers, 13-6
- SharePoint resources, 9-3
- simple
 - policy simulation, 13-1
- simple search, 5-2
- simulation
 - policies, 13-1
- SMConfig UI
 - starting, 8-2
- system administrators, 11-8
- system configuration, 3-8
- system grants, 3-5, 4-19, 5-11
- system policies, 3-5, 4-19, 5-11
- system requirements, 3-1
- SystemAdmin, 3-4

T

- T2P, 13-1
- test-to-production, 13-1

U

- use case, 2-7
- users, 5-12

W

- WebLogic Server
 - Discovery Mode, 9-15, 9-16
 - integration, 9-16
- WebLogic Server resources, 9-15
- weblogic user, 3-4
- WLST
 - commands, E-1
 - sample script, E-12
 - using, E-1

X

- XACML, 1-9, 1-10