



Oracle Insurance Insight

**Oracle Insurance Insight
Administration Guide**

version 7.0.2

Part number: E24031-01

October 2011

Oracle Insurance Insight Administration Guide

Version 7.0.2

Part Number: E24031-01

October 2011

Copyright © 2011, Oracle. All rights reserved.

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

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

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

U.S. GOVERNMENT RIGHTS

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

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

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

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

THIRD PARTY SOFTWARE NOTICES

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 2.0 Copyright (c) 2004 The Apache Software Foundation. All rights reserved.

The Apache Software License, Version 1.1 Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

CONTENTS

Preface

- iii Version
- iii Intended Audience
- iii Related Documents
- iv Relevant Oracle Documentation
- iv OII Documentation on the Oracle Technology Network (OTN)
- iv Customer Support

Chapter 1: Introduction to the OII Application Roles, Groups, and Users

- 2 What are the OII System Administrator's Tasks?
- 3 What Tools will the OII System Administrator Use?
 - 3 Opening the Oracle Fusion Middleware Control
 - 5 Opening the Oracle WebLogic Server Administration Console
- 8 What's Next?

Chapter 2: Creating and Configuring the OII Application Roles, Groups, and Users

- 13 Step 1: Create the Application Roles for OII
- 17 Step 2: Create the Security Groups for OII
- 21 Step 3: Create the OII Users
- 23 Step 4: Add Users to the OII Groups
- 25 Step 5: Map OII Groups to OII Application Roles
- 29 Step 6: Map the OII Application Roles to the BIConsumer and BI-Author Application Roles
- 31 Step 7: Test the OII Users in OBIEE
 - 32 Viewing the Content within OBIEE
- 34 Adding Additional Users

i – Index

Preface

Welcome to the *Oracle Insurance Insight Administration Guide*. This guide presents the information you will need to manage data and user accounts in Oracle Insurance Insight (OII) using the administrative tools of Oracle Business Intelligence Enterprise Edition (OBIEE).

This is not a complete system administrator's guide for OBIEE. The purpose of this manual is to describe the basic administrative duties that you will need to perform in order to maintain the data in OII.

VERSION

This manual corresponds to Oracle Insurance Insight (OII) version 7.0.2.

INTENDED AUDIENCE

This manual is intended for experienced system administrators with advanced knowledge of OBIEE 11g and OII.

RELATED DOCUMENTS

For more information, refer to the following documents:

- *Oracle Insurance Insight Release Notes* - This document describes the latest enhancements and updates to OII as well as issues that have been resolved in this version.
- *Oracle Insurance Insight Installation Guide* - This manual describes the steps for configuring and installing OII.
- *Oracle Insurance Insight Warehouse Palette User Guide* - This manual describes how to use the Warehouse Palette, an application that provides users with an easy-to-use interface to create and configure a Line of Business (LOB) and “publish” the LOB for incorporation into the OII system.
- *Oracle Insurance Insight Implementation Guide* - This manual describes the concepts and steps involved in implementing the OII system.
- *Oracle Insurance Insight User Guide* - OII uses OBIEE 11g as its front end interface, providing a set of dashboards, reports, and query building tools to use to analyze the OII data. This manual describes how to configure and run the OII reports as well as use the OBIEE analytic features to build custom queries to run against the OII data.
- *Oracle Insurance Insight Data Dictionary* - The data dictionary for the OII system.

RELEVANT ORACLE DOCUMENTATION

For complete documentation on OBIEE and its components, please go to the documentation section of the Oracle website to consult the following manuals:

- *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition (11g Release)*

OII DOCUMENTATION ON THE ORACLE TECHNOLOGY NETWORK (OTN)

The OII documentation set is packaged with the product release. You can also obtain these guides online thought the Oracle Technology Network (OTN) at this address:

<http://www.oracle.com/technology/documentation/insurance.html>

CUSTOMER SUPPORT

If you need help with Oracle Insurance Insight, please log a Service Request using My Oracle Support at <https://support.oracle.com>.

Address any additional inquiries to:

Oracle Corporation

World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Chapter 1

Introduction to the OII APPLICATION ROLES, GROUPS, AND USERS

The OII system administrator must create and configure the necessary OII application roles, security groups, and users to ensure that OII users are granted access to the proper data within Oracle Business Intelligence (OBIEE). Note that this is not a complete administrator's guide to OBIEE security. For that, refer to the *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition*.

An **application role** represents a role a user has when using OBIEE. Within the OII dashboards for OBIEE there are five OII roles:

- Actuary
- Claims Management
- Executive
- Production
- Underwriting

The role(s) assigned to a user determines the content that appears when the user first logs into OBIEE and accesses the OII Scorecard and Analysis dashboards. Users can be assigned one or more application roles. Only the tabs corresponding to an assigned role will appear on the dashboard. Figure 1, for example, shows the OBIEE dashboard for a user who has been assigned all five OII roles.

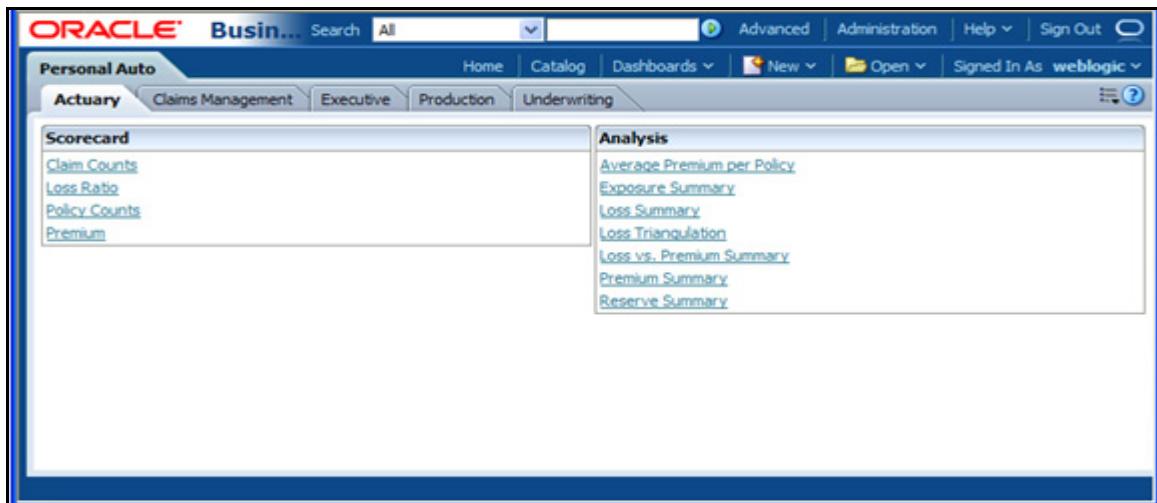


Figure 1: Tabs in OBIEE Correspond to the OII Roles

WHAT ARE THE OII SYSTEM ADMINISTRATOR'S TASKS?

The system administrator's tasks include the following:

1. Create the Application Roles for OII

Use the **Oracle Fusion Middleware Control** to create the OII application roles:

- BIActuary
- BIExecutive
- BIUnderwriter
- BIProducer
- BIClaimsManager

2. Create the Security Groups for OII

The following security groups must be created for OII in the **Oracle WebLogic Server Administration Console**.

- BIActuaries
- BIClaimsManagers
- BIExecutives
- BIProducers
- BIUnderwriters

3. Create the OII Users

Use the **Oracle WebLogic Server Administration Console** to create the OII users who will access the OII data in OBIEE.

4. Assign the OII Users to the OII Groups

Use the **Oracle WebLogic Server Administration Console** to add the OII users to the proper OII groups.

5. Map the OII Groups to the OII Application Roles

Use the **Oracle Fusion Middleware Control** to map each OII group to an appropriate OII application role to grant its permissions to group members.

6. Map the OII Application Roles to the BIAuthor and BIConsumer Application Roles

Use the **Oracle Fusion Middleware Control** to map the OII Application Roles to the BIAuthor and BIConsumer Application Roles that are shipped with OBIEE.

7. Test the OII Users in OBIEE

Log into OBIEE and ensure that the users assigned to a particular role only see the content on the dashboards that has been designated to them.

WHAT TOOLS WILL THE OII SYSTEM ADMINISTRATOR USE?

The system administrator will use the following tools to configure the OII components for OBIEE:

- Oracle Fusion Middleware Control
- Oracle WebLogic Server Administration Console

OPENING THE ORACLE FUSION MIDDLEWARE CONTROL

1. Launch the Enterprise Manager by entering the following URL in your browser:

<http://<hostname>:7001/em>

Note In the above URL, <hostname> can be the server name or IP address where you installed OBIEE.

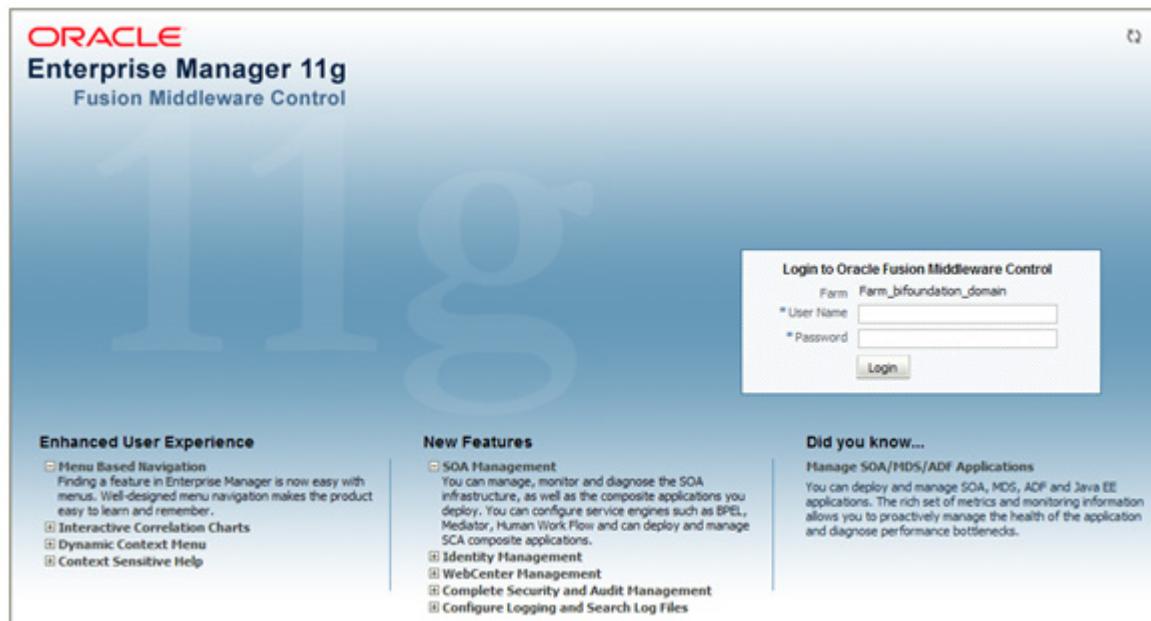


Figure 2: Enterprise Manager Login Screen

2. Log into Enterprise Manager using the administrator name and password that was specified during the OBIEE installation. The Oracle Fusion Middleware Control will open.

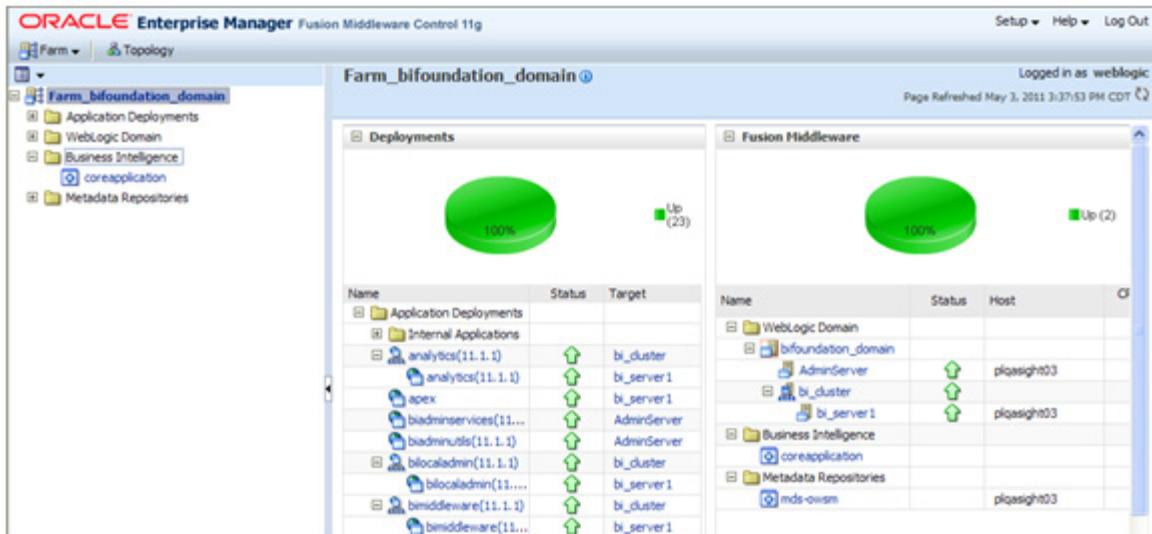


Figure 3: Oracle Fusion Middleware Control

OPENING THE ORACLE WEBLOGIC SERVER ADMINISTRATION CONSOLE

Open the WebLogic Server Administration Console using one of the following methods.

Method 1: Open the WebLogic Server Administration Console in Fusion Middleware Control

1. Launch the Enterprise Manager by entering the following URL in your browser:

<http://<hostname>:7001/em>

Note In the above URL, <hostname> can be the server name or IP address where you installed OBIEE.

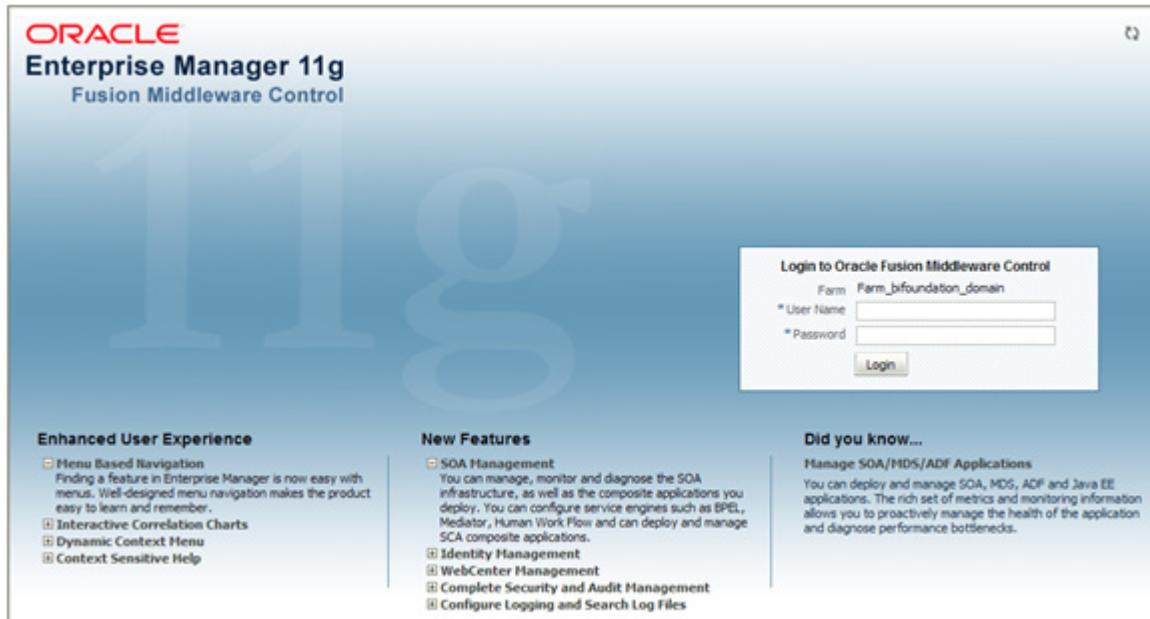


Figure 4: Enterprise Manager Login Screen

2. Log into Enterprise Manager using the administrator name and password that was specified during the OBIEE installation. The Oracle Fusion Middleware Console will open.

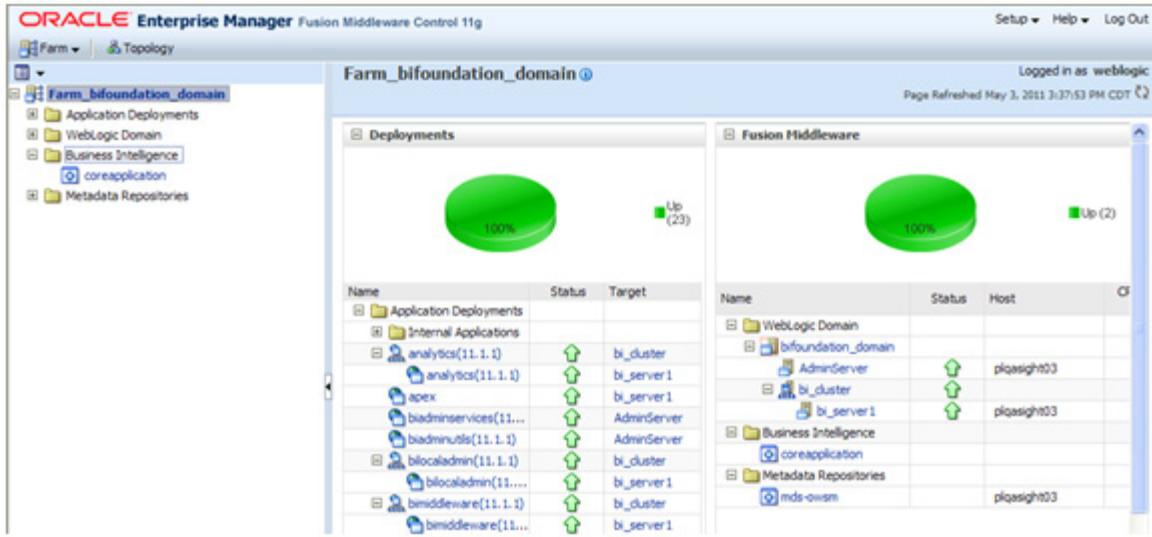


Figure 5: Oracle Fusion Middleware Console

3. In the navigation tree in the left pane expand the WebLogic Domain node and select the bifoundation_domain.
4. Click the **Oracle WebLogic Server Administration Console** link in the Summary region.
5. The Oracle WebLogic Server Administration Console login page is displayed.

Method 2: Using a URL

1. Launch WebLogic by entering the following URL in your browser:

http://<hostname>:7001/console

Note In the above URL, <hostname> can be the server name or IP address where you installed OBIEE.

The WebLogic Server Administration Console login screen will open:



Figure 6: WebLogic Server Administration Console Login Screen

2. Enter the administrator user name and password for the server domain that was specified during the OBIEE installation process. The WebLogic Administration Console opens:

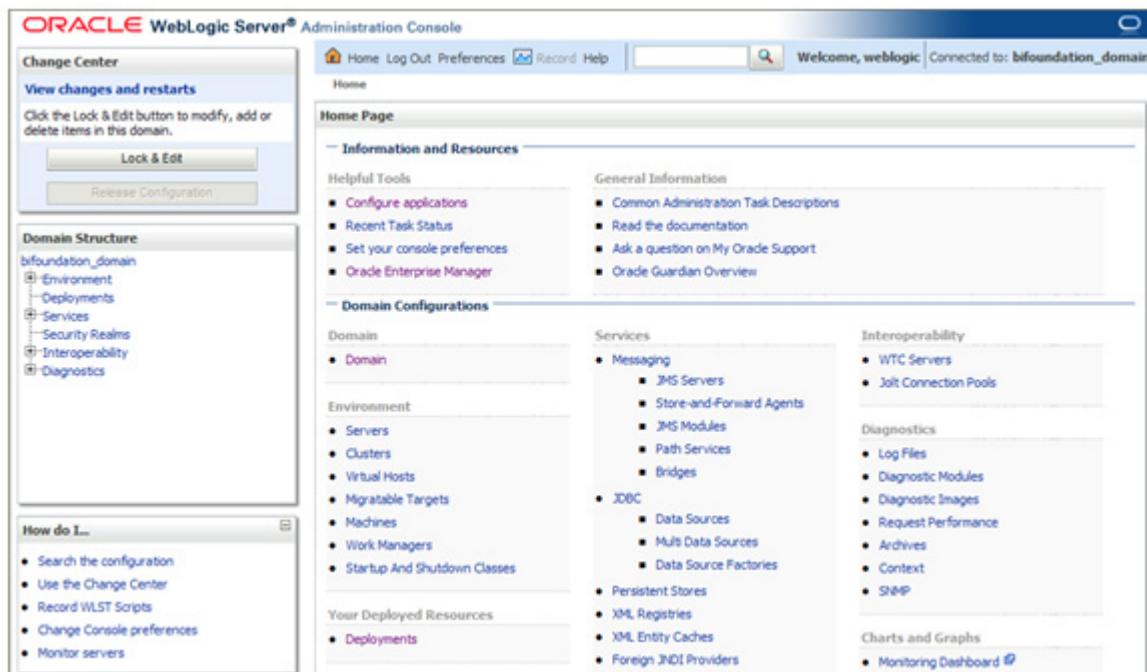


Figure 7: WebLogic Server Administration Console

WHAT'S NEXT?

Go to *Chapter 2: Creating and Configuring the OII Application Roles, Groups, and Users* for a step-by-step description on how to create all of the required OII application roles, users, and groups.

Chapter 2

Creating and Configuring the OII Application Roles, Groups, and Users

This chapter will walk you through the steps to configure the OII application roles, groups, and users:

1. Create the application roles for OII
2. Create the security groups for OII
3. Create the OII users
4. Add the OII users to the OII groups
5. Map the OII groups to the OII application roles
6. Map the OII application roles to BIConsumer and BIAuthor roles
7. Test the OII users in OBIEE

STEP 1: CREATE THE APPLICATION ROLES FOR OII

This step requires you to create the following five application roles for OII using the Oracle Fusion Middleware Control:

- BIActuary
- BIClaimsManager
- BIExecutive
- BIProducer
- BIUnderwriter

1. Log into the Oracle Fusion Middleware Control (see *Opening the Oracle Fusion Middleware Control* on page 3).

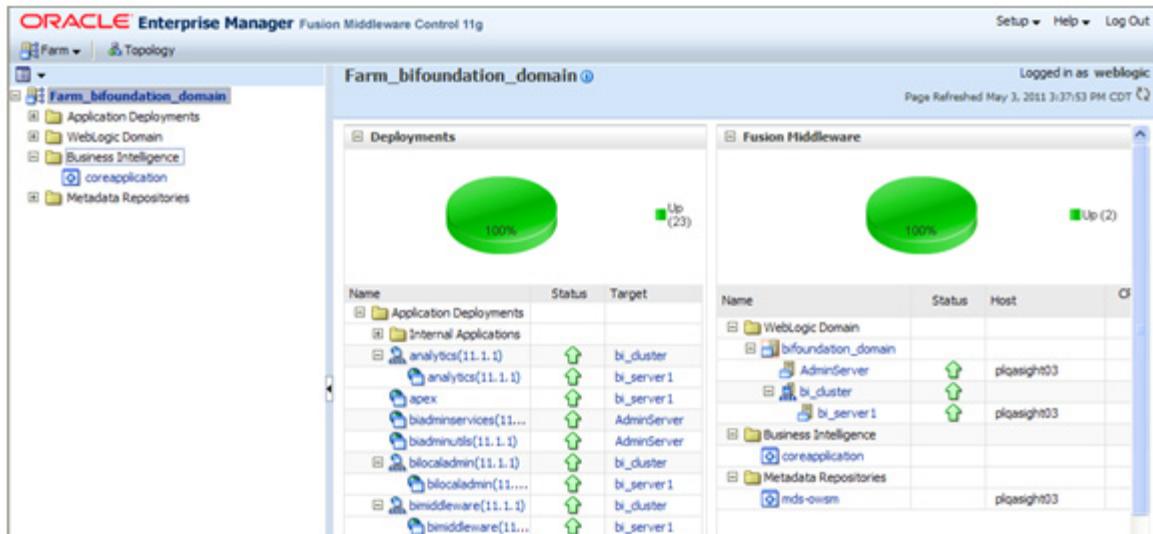


Figure 8: Oracle Fusion Middleware Control

2. In the navigation tree in the left pane expand **Business Intelligence** and select **coreapplication**. When the page refreshes, select the **Security** tab to open the **Security** page.

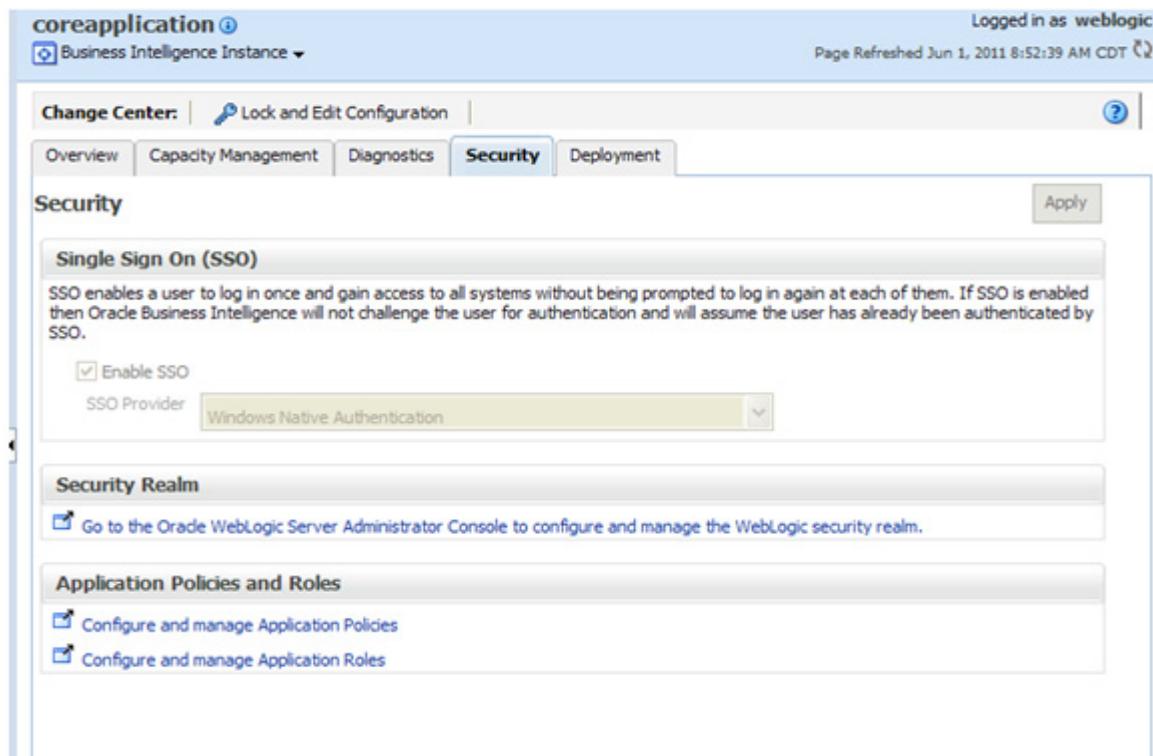


Figure 9: Security Page

3. Click on the **Configure and manage Application Roles** link at the bottom of the page. The **Application Roles** page will open. What you will initially see on this page is a list of the default security roles that are shipped with OBIEE.

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in WebLogic Domain policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is different from application name.

Select Application Stripe to Search obi

Role Name

Create... Create Like... Edit... Delete...

Role Name	Members
BISystem	BISystemUser
BIAdministrator	BIAdministrators
BIAuthor	BIAuthors, BIAdministrator
BIConsumer	BIConsumers, BIAuthor, authenticated-role

Figure 10: Application Roles

4. On the **Application Roles** page, click the **Create** button. The **Create Application Roles** page opens.

coreapplication Business Intelligence Instance Logged in as weblogic Page Refreshed Jun 1, 2011 9:56:37 AM CDT

Application Roles > Create Application Role

Create Application Role

General

Application Stripe

* Role Name

Display Name

Description

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Roles

Add Application Role Add Group Delete...

Name	Type
No groups or application roles added.	

Figure 11: Create Application Roles Page

5. Enter the following parameters under the **General** section:
 - **Role Name** - Enter the name of one of the OII application roles listed on page 13. For example, **BIActuary**.
 - (Optional) **Display Name** - Enter the display name for the application role.
 - (Optional) **Description** - Enter a description for the application role.
6. Click **OK** to return to the Application Roles page. The application role you just created will appear in the table.
7. Repeat steps 5-7 to create the four remaining OII application roles.
 - BIClaimsManager
 - BIExecutive
 - BIProducer
 - BIUnderwriter

When you are finished the OII application roles will appear in the table on the Application Roles page:

Role Name	Members
BISystem	BISystemUser
BIAdministrator	BIAdministrators
BIAuthor	BIAuthors, BIAdministrator
BIConsumer	BIConsumers, BIAuthor, authenticated-role
BIActuary	
BIExecutive	
BIUnderwriter	
BIProducer	
BIClaimsManager	

Figure 12: OII Application Roles

STEP 2: CREATE THE SECURITY GROUPS FOR OII

This step requires you to create the following OII Security Groups within the **Oracle WebLogic Server Administration Console**.

- BIActuaries
- BIClaimsManagers
- BIExecutives
- BIProducers
- BIUnderwriters

Note In OBIEE, groups are set to match the corresponding application roles but with their names set as plural. For example, BIProducers (group) vs. BIProducer (application role).

1. Open the **Oracle WebLogic Server Administration Console** (see *Opening the Oracle WebLogic Server Administration Console* on page 5).:

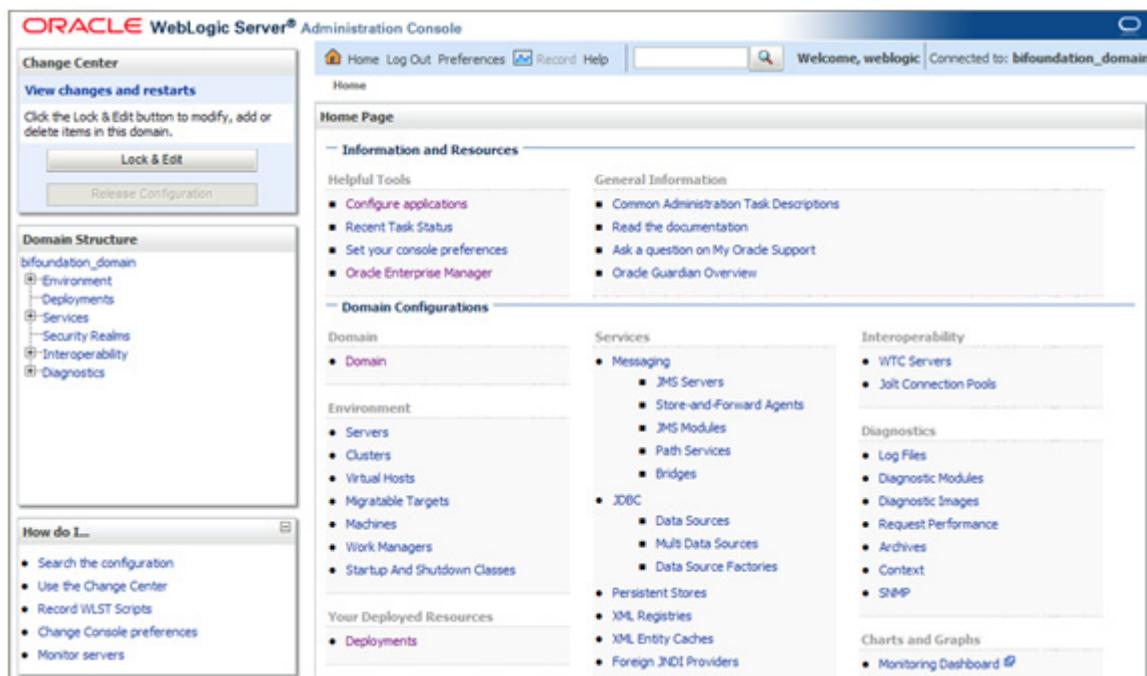


Figure 13: WebLogic Server Administration Console

2. Select **Security Realms** in the left pane. The **Summary of Security Realms** page will appear on the right.

The screenshot shows the 'Summary of Security Realms' page. At the top, there is a header bar with 'Home', 'Log Out', 'Preferences', 'Record', 'Help', a search bar, and the text 'Welcome, weblogic' and 'Connected to: bifoundation_domain'. Below the header, the URL 'Home > Summary of Security Realms' is displayed. The main content area is titled 'Summary of Security Realms' and contains a brief description of what a security realm is. It then lists each security realm that has been configured in the domain. A table titled 'Realms (Filtered - More Columns Exist)' is shown, with one row for 'myrealm'. The table has columns for 'Name' and 'Default Realm'. The 'Name' column shows 'myrealm' and the 'Default Realm' column shows 'true'. Navigation buttons for 'New', 'Delete', 'Showing 1 to 1 of 1', 'Previous', and 'Next' are visible at the top and bottom of the table.

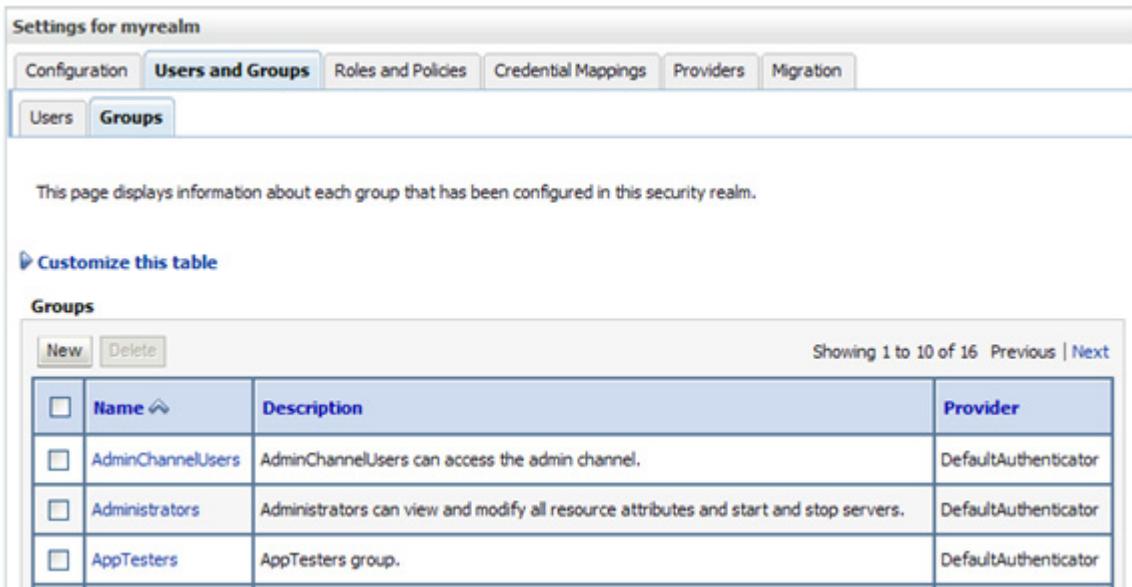
Figure 14: Summary of Security Realms Page

3. Click on **myrealm**. The **Settings for myrealm** page will open.

The screenshot shows the 'Settings for myrealm' page. At the top, there is a header bar with 'Configuration', 'Users and Groups', 'Roles and Policies', 'Credential Mappings', 'Providers', and 'Migration'. Below the header, there is a sub-header with tabs: 'General', 'RDBMS Security Store', 'User Lockout', and 'Performance'. A note says 'Click the Lock & Edit button in the Change Center to modify the settings on this page.' Below this, there is a 'Save' button. The main content area is titled 'General' and contains a note: 'Use this page to configure the general behavior of this security realm.' A 'Note:' section states: 'If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.' Below this, there are several configuration fields: 'Name:' set to 'myrealm' (with a note: 'The name of this security realm.'), 'Security Model Default:' set to 'DD Only' (with a note: 'Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment.'), and a checked checkbox for 'Combined Role Mapping Enabled' (with a note: 'Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors.').

Figure 15: Settings for myrealm Page

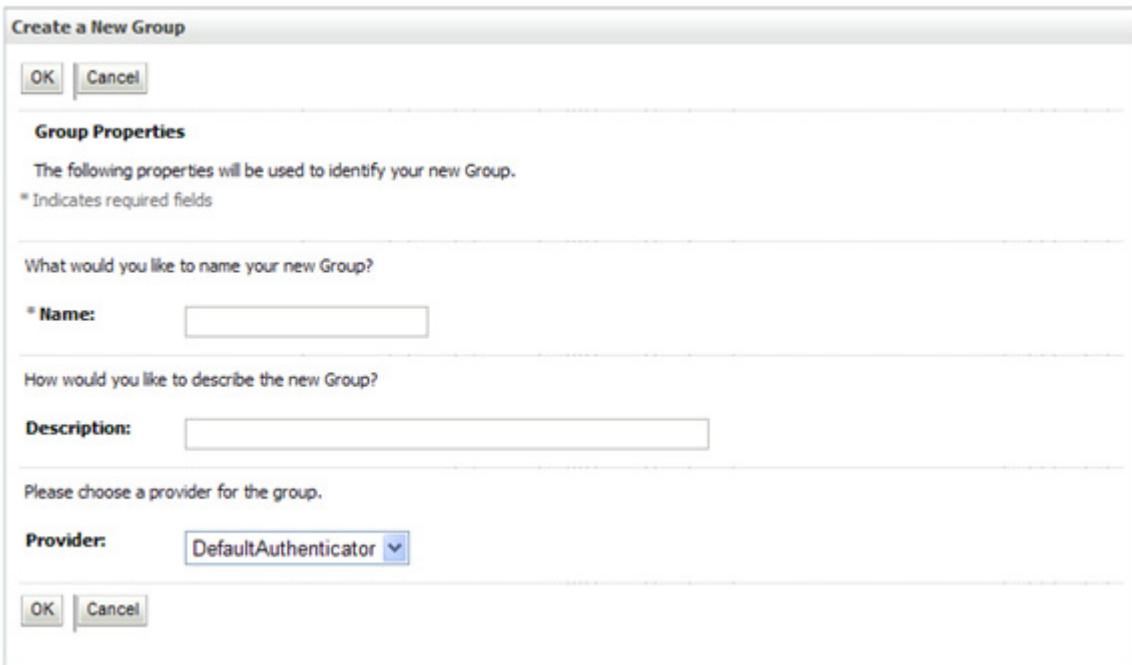
4. Click on the **Users and Groups** tab at the top of the page, and then click on the **Groups** tab to display a list of configured groups in **myrealm**.



<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
<input type="checkbox"/>	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	AppTesters	AppTesters group.	DefaultAuthenticator

Figure 16: List of Configured Groups

5. Select the **New** button. The **Create a New Group** page will open.



Create a New Group

OK Cancel

Group Properties

The following properties will be used to identify your new Group.
* Indicates required fields

What would you like to name your new Group?

*** Name:**

How would you like to describe the new Group?

Description:

Please choose a provider for the group.

Provider:

OK Cancel

Figure 17: Create a New Group Page

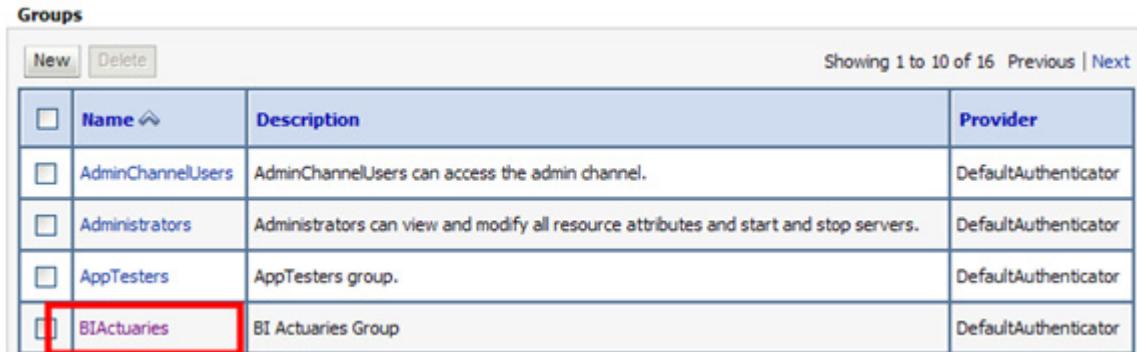
6. Enter the following information on this page:

- **Name** - Enter the name of a of the OII security groups listed on page 17. For example, **BIActuaries**.

- **(Optional) Description** - Enter a description
- **Provider** - Accept the default provider: **DefaultAuthenticator**.

7. Click **OK**. You will be returned to the Groups tab where the group you just created will appear in the list of groups.

Groups



The screenshot shows a table titled "Groups" with a "New" and "Delete" button at the top. The table has columns for "Name", "Description", and "Provider". The "Name" column is sorted by a blue arrow. The "BIActuaries" row is highlighted with a red border. The "Description" for BIActuaries is "BI Actuaries Group". The "Provider" for all groups is "DefaultAuthenticator".

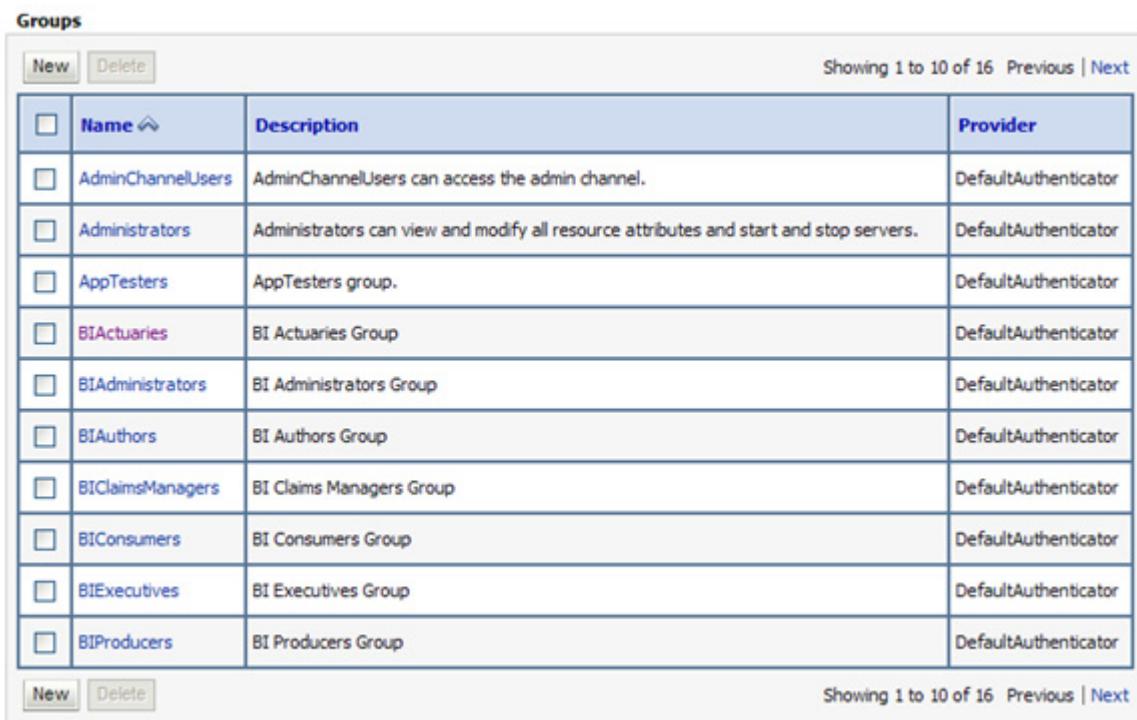
<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
<input type="checkbox"/>	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	AppTesters	AppTesters group.	DefaultAuthenticator
<input type="checkbox"/>	BIActuaries	BI Actuaries Group	DefaultAuthenticator

Figure 18: The BIActuaries Group has been Completed

8. Repeat steps 5-7 to create the remaining OII groups:

- BIClaimsManagers
- BIExecutives
- BIProducers
- BIUnderwriters

Groups



The screenshot shows a table titled "Groups" with a "New" and "Delete" button at the top. The table has columns for "Name", "Description", and "Provider". The "Name" column is sorted by a blue arrow. The "BIActuaries" row is highlighted with a red border. The "BIAdministrators" row has just been added and is empty. The "Description" for BIActuaries is "BI Actuaries Group". The "Provider" for all groups is "DefaultAuthenticator".

<input type="checkbox"/>	Name	Description	Provider
<input type="checkbox"/>	AdminChannelUsers	AdminChannelUsers can access the admin channel.	DefaultAuthenticator
<input type="checkbox"/>	Administrators	Administrators can view and modify all resource attributes and start and stop servers.	DefaultAuthenticator
<input type="checkbox"/>	AppTesters	AppTesters group.	DefaultAuthenticator
<input type="checkbox"/>	BIActuaries	BI Actuaries Group	DefaultAuthenticator
<input type="checkbox"/>	BIAdministrators	BI Administrators Group	DefaultAuthenticator
<input type="checkbox"/>	BIAuthors	BI Authors Group	DefaultAuthenticator
<input type="checkbox"/>	BIClaimsManagers	BI Claims Managers Group	DefaultAuthenticator
<input type="checkbox"/>	BIConsumers	BI Consumers Group	DefaultAuthenticator
<input type="checkbox"/>	BIExecutives	BI Executives Group	DefaultAuthenticator
<input type="checkbox"/>	BIProducers	BI Producers Group	DefaultAuthenticator

Figure 19: Create the Rest of the OII Groups

STEP 3: CREATE THE OII USERS

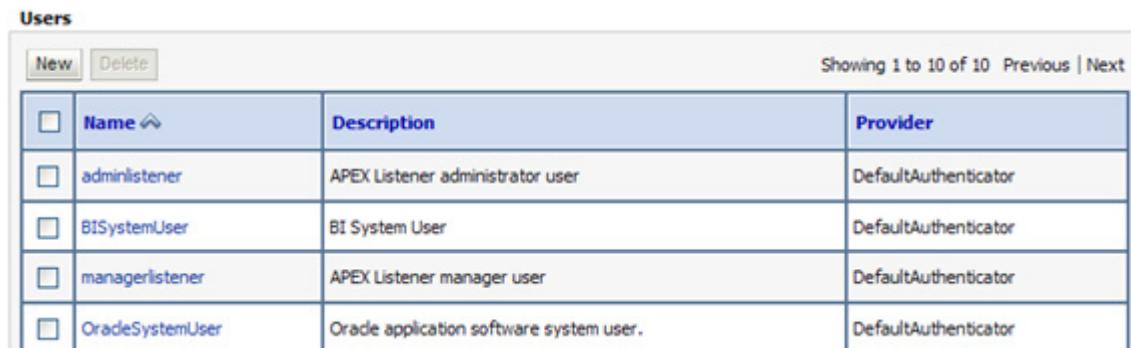
This step requires you to create the OII users who will be logging into OBIEE.

For the purpose of testing OBIEE, this scenario will require you to create five separate users, one for each OII application role. These sample user names will be:

- actuary
- claims
- executive
- producer
- underwriter

In the subsequent steps we will then add each user to its corresponding OII group and in turn map the OII group to its corresponding OII application role.

1. Select the **Users** tab at the top of the page to display the list of configured users.



The screenshot shows a table titled 'Users' with a 'New' and 'Delete' button at the top. The table has columns for 'Name', 'Description', and 'Provider'. There are five rows of data, each with a checkbox in the first column. The data is as follows:

	Name	Description	Provider
<input type="checkbox"/>	adminlistener	APEX Listener administrator user	DefaultAuthenticator
<input type="checkbox"/>	BISystemUser	BI System User	DefaultAuthenticator
<input type="checkbox"/>	managerlistener	APEX Listener manager user	DefaultAuthenticator
<input type="checkbox"/>	OracleSystemUser	Oracle application software system user.	DefaultAuthenticator

Figure 20: List of Users

2. Click on the **New** button at the top of this table. The **Create a New User Page** opens.

The screenshot shows the 'Create a New User' dialog box. At the top, there are 'OK' and 'Cancel' buttons. Below them is a section titled 'User Properties' with the sub-instruction: 'The following properties will be used to identify your new User.' and a note: '* Indicates required fields'. The 'Name' field is marked with an asterisk and is empty. The 'Description' field is also empty. The 'Provider' dropdown menu is set to 'DefaultAuthenticator'. Below the provider section, there is a note: 'The password is associated with the login name for the new User.' followed by 'Password' and 'Confirm Password' fields, both marked with asterisks and empty. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 21: Create a New User Page

3. Enter the following information on this page:
 - **Name** - Enter a name of the OII user. For example, **actuary**.
 - **(Optional) Description** - Enter a description
 - **Provider** - Accept the default provider: **DefaultAuthenticator**.
 - **Password** - Enter a password that is at least 8 characters long.
 - **Confirm Password** - Re-enter the password.
4. Click **OK**. You will be returned to the **Users** tab where the user you just created will appear in the list of users.

5. Repeat steps 1-4 to add the four additional users.

Users			
	New	Delete	Showing 1 to 10 of 10 Previous Next
	Name	Description	Provider
<input type="checkbox"/>	adminlistener	APEX Listener administrator user	DefaultAuthenticator
<input type="checkbox"/>	BISystemUser	BI System User	DefaultAuthenticator
<input type="checkbox"/>	managerlistener	APEX Listener manager user	DefaultAuthenticator
<input type="checkbox"/>	OradeSystemUser	Orade application software system user.	DefaultAuthenticator
<input type="checkbox"/>	executive		DefaultAuthenticator
<input type="checkbox"/>	managerlistener	APEX Listener manager user	DefaultAuthenticator
<input type="checkbox"/>	OradeSystemUser	Orade application software system user.	DefaultAuthenticator
<input type="checkbox"/>	producer		DefaultAuthenticator
<input type="checkbox"/>	underwriter		DefaultAuthenticator
<input type="checkbox"/>	weblogic		DefaultAuthenticator

Figure 22: OII Users Added to the List

STEP 4: ADD USERS TO THE OII GROUPS

This step requires you to add the users you created in the previous section to their corresponding OII group.

User	Add to...	Group
actuary		BIActuaries
claims		BIClaimsManagers
executive		BIExecutives
producer		BIProducers
underwriter		BIUnderwriters

1. If you are not already there, return to the **Users** page to display the table listing the configured users.

2. Click on the name of an OII user. For example, **actuary**. A settings page for the selected user will open.

The screenshot shows the 'Settings for actuary' page. At the top, there are tabs: General (selected), Passwords, Attributes, and Groups. Below the tabs is a 'Save' button. A note says: 'Use this page to change the description for the selected user.' The 'Name:' field contains 'actuary' with a note: 'The login name of this user. [More Info...](#)'. The 'Description:' field is empty with a note: 'A short description of this user. For example, the user's full name. [More Info...](#)'. At the bottom is another 'Save' button.

Figure 23: Settings Page for the Selected User

3. Select the **Groups** tab. The **Groups** page opens:

The screenshot shows the 'Groups' page for the 'actuary' user. At the top, there are tabs: General, Passwords, Attributes, and Groups (selected). Below the tabs is a 'Save' button. A note says: 'Use this page to configure group membership for this user.' The 'Parent Groups:' section has two sections: 'Available' (listing AdminChannelUsers, Administrators, AppTesters, BIAdministrators, BIAuthors, BIClaimsManagers) and 'Chosen' (listing BIActuaries). A note next to 'Chosen' says: 'This user can be a member of any of these parent groups. [More Info...](#)'. At the bottom is a 'Save' button.

Figure 24: Groups Page

4. Add the **actuary** user to the **BIActuaries** group by selecting **BIActuaries** in the **Available** list box. The selected group will appear in the **Chosen** list.
5. Click the **Save** button.
6. Repeat steps 2-5 to add the remaining four users to their appropriate OII group.
7. Recycle WebLogic to apply your changes.

STEP 5: MAP OII GROUPS TO OII APPLICATION ROLES

This step requires you to map the following OII groups to their corresponding OII application roles.

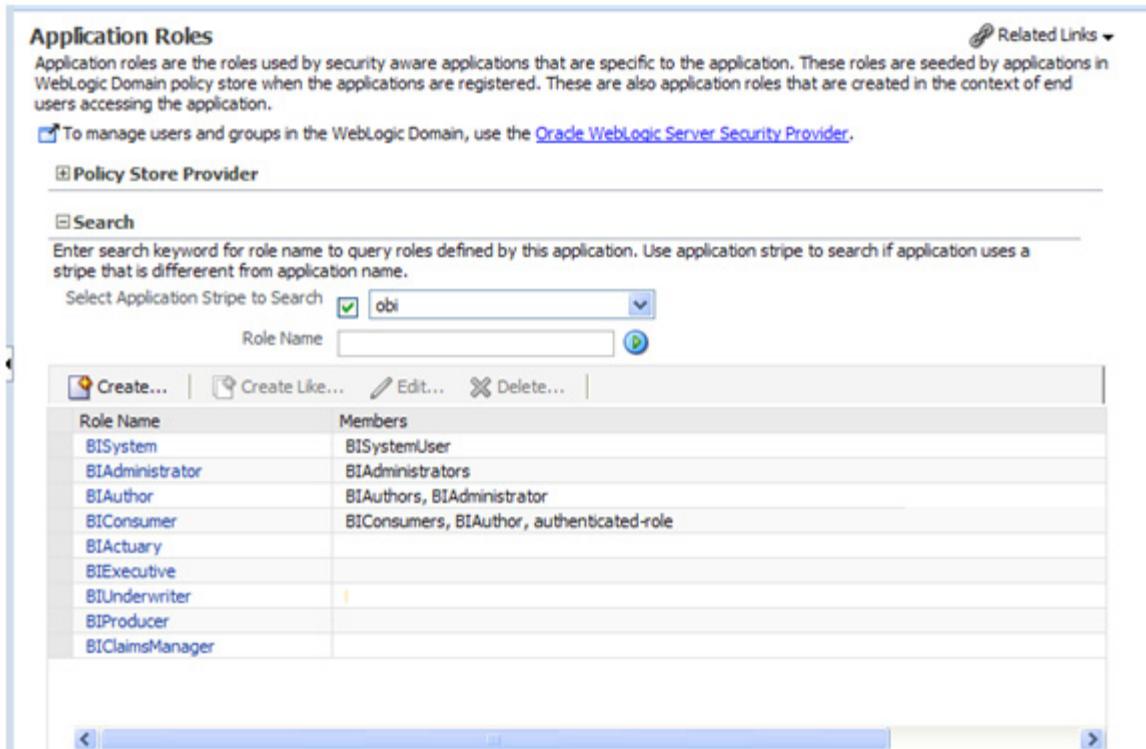
Group	Map to...	Application Role
BIActuaries		BIActuary
BIClaimsManagers		BIClaimsManager
BIExecutives		BIExecutive
BIProducers		BIProducer
BIUnderwriters		BIUnderwriter

1. Return to the Oracle Fusion Middleware Control (see *Opening the Oracle Fusion Middleware Control* on page 3).
2. In the navigation tree in the left pane expand **Business Intelligence** and select **coreapplication**.
3. When the page refreshes, select the **Security** tab to open the **Security** page.

The screenshot shows the Oracle Fusion Middleware Control interface for the 'coreapplication' instance. The top navigation bar includes 'coreapplication' and 'Business Intelligence Instance'. The top right shows 'Logged in as weblogic' and 'Page Refreshed Jun 1, 2011 8:52:39 AM CDT'. The main content area has a 'Change Center' header with 'Lock and Edit Configuration' and tabs for 'Overview', 'Capacity Management', 'Diagnostics', 'Security' (which is selected), and 'Deployment'. The 'Security' tab contains three main sections: 'Single Sign On (SSO)', 'Security Realm', and 'Application Policies and Roles'. The 'Single Sign On (SSO)' section has a checkbox for 'Enable SSO' (checked) and a dropdown for 'SSO Provider' set to 'Windows Native Authentication'. The 'Security Realm' section has a link to 'Go to the Oracle WebLogic Server Administrator Console to configure and manage the WebLogic security realm'. The 'Application Policies and Roles' section has two links: 'Configure and manage Application Policies' and 'Configure and manage Application Roles'.

Figure 25: Security Page

4. Click on the **Configure and manage Application Roles** link at the bottom of the page. The **Application Roles** page will open.

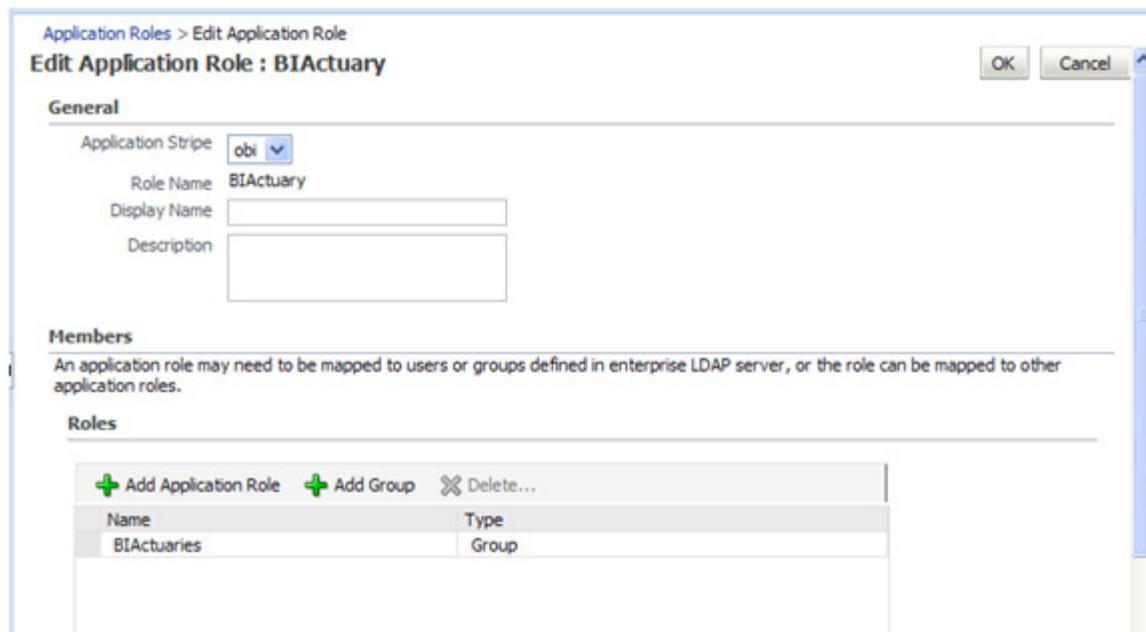


The screenshot shows the 'Application Roles' page. At the top, there is a brief description of what application roles are and a link to manage users and groups using the Oracle WebLogic Server Security Provider. Below this, there are sections for 'Policy Store Provider' and 'Search'. The 'Search' section includes a dropdown for 'Select Application Stripe to Search' (set to 'obi') and a text input for 'Role Name'. A toolbar below these includes buttons for 'Create...', 'Create Like...', 'Edit...', and 'Delete...'. The main table lists application roles with their members:

Role Name	Members
BISystem	BISystemUser
BIAdministrator	BIAdministrators
BIAuthor	BIAuthors, BIAdministrator
BIConsumer	BIConsumers, BIAuthor, authenticated-role
BIActuary	
BIExecutive	
BIUnderwriter	
BIProducer	
BIClaimsManager	

Figure 26: Application Roles Page

5. Click on **BIActuary**. The **Edit Application Role** page for **BIActuary** opens.



The screenshot shows the 'Edit Application Role : BIActuary' dialog. It has tabs for 'General', 'Members', and 'Roles'. The 'General' tab shows the 'Application Stripe' set to 'obi', 'Role Name' set to 'BIActuary', and empty 'Display Name' and 'Description' fields. The 'Members' tab contains a note about mapping the role to users or groups. The 'Roles' tab shows a table with one entry:

Name	Type
BIActuaries	Group

Figure 27: Edit Application Role

6. Select the **Add Group** button to add the **BIActuaries** group to the Roles list.

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or application roles.

Roles

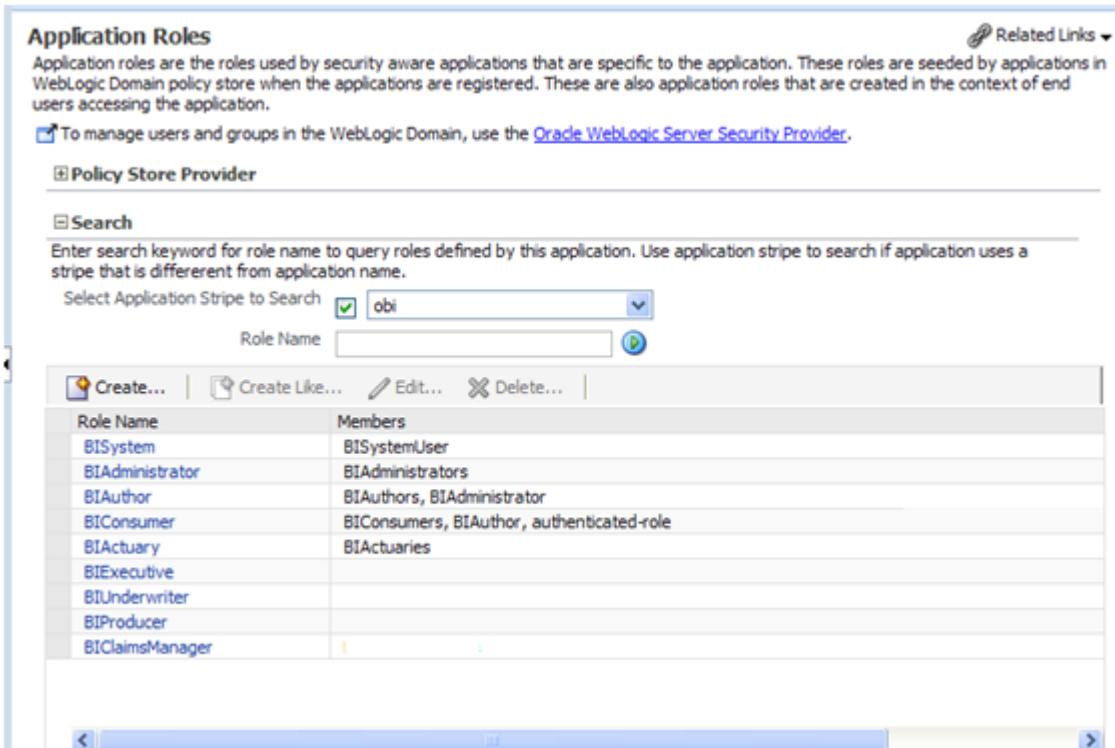


A screenshot of a user interface showing a table of application roles. At the top, there are three buttons: 'Add Application Role' (green plus icon), 'Add Group' (green plus icon), and 'Delete...' (cross icon). The 'Add Group' button is highlighted with a red box. The table has two columns: 'Name' and 'Type'. One row is visible, showing 'BIActuaries' in the Name column and 'Group' in the Type column.

Name	Type
BIActuaries	Group

Figure 28: Add Group Button

7. Click **OK** to return to the **Application Roles** page. The **BIActuaries** group is now mapped to the **BIActuary** role.

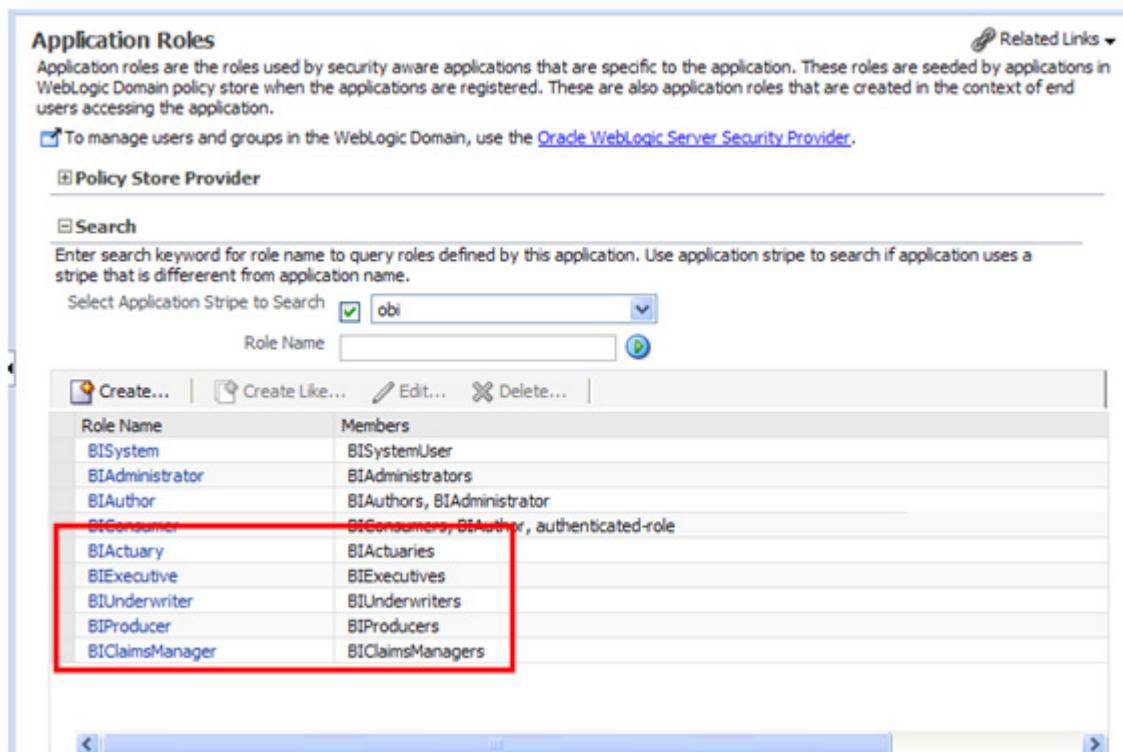


A screenshot of the 'Application Roles' page. The page header includes 'Related Links' and a link to 'Oracle WebLogic Server Security Provider'. Below the header, there are sections for 'Policy Store Provider' and 'Search'. The 'Search' section contains a dropdown for 'Select Application Stripe to Search' (set to 'obi') and a text input for 'Role Name' with a search icon. The main content is a table of application roles. The table has two columns: 'Role Name' and 'Members'. The 'Role Name' column lists roles like BISystem, BIAdministrator, BIAuthor, BIConsumer, BIActuary, BIExecutive, BIUnderwriter, BIProducer, and BIClaimsManager. The 'Members' column lists the 'BIActuaries' group for the BIActuary role. Navigation buttons for the table are visible at the bottom.

Role Name	Members
BISystem	BISystemUser
BIAdministrator	BIAdministrators
BIAuthor	BAAuthors, BIAdministrator
BIConsumer	BIConsumers, BIAuthor, authenticated-role
BIActuary	BIActuaries
BIExecutive	
BIUnderwriter	
BIProducer	
BIClaimsManager	

Figure 29: BIActuaries Group is Mapped to BIActuary Application Role

8. Repeat steps 5-7 to map the remaining OII groups to the corresponding OII application roles. When you are done the Application Roles page will appear as follows:



Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in WebLogic Domain policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is different from application name.

Select Application Stripe to Search obi

Role Name	Members
BIConsumer	BIConsumers, BIAuthor, authenticated-role
BIActuary	BIActuaries
BIExecutive	BIExecutives
BIUnderwriter	BIUnderwriters
BIProducer	BIProducers
BIClaimsManager	BIClaimsManagers

Figure 30: OII Groups Mapped to OII Application Role

STEP 6: MAP THE OII APPLICATION ROLES TO THE BIConsumer AND BIAuthor APPLICATION ROLES

This step requires you to map all of the OII application roles that you previously created to the **BIAuthor** and **BIConsumer** application roles. BIAuthor and BIConsumers are pre-configured application roles that are installed with OBIEE.

1. On the **Application Roles** page, click on the **BIAuthor** application role to open it for editing.
2. Use the **Add Application Role** button to map the OII application roles to **BIAuthor**.

coreapplication Business Intelligence Instance Logged in as web Page Refreshed Jun 1, 2011 5:15:25 PM CT

Application Roles > Edit Application Role

Display Name: BI Author Role

Description:

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Roles

Role	Type
BIConsumer	Group
BIAdministrator	Application Role
BIActuary	Application Role
BIExecutive	Application Role
BIUnderwriter	Application Role
BIProducer	Application Role
BIClaimsManager	Application Role

Figure 31: Add OII Application Roles to BIAuthor

3. Click **OK** to return to the **Application Roles** page.
4. Repeat steps 1-3 to map the OII application roles to the **BIConsumer** application role.

5. When you are finished the **Application Roles** page will appear as follows.

Role Name	Members
BISystem	BISystemUser
BIAdministrator	BIAdministrators
BIAuthor	BIAuthors, BIAdministrator, BIActuary, BIExecutive, BIUnderwriter, BIProducer, BIClaimsManager
BICConsumer	BIConsumers, BIAuthor, authenticated-role, BIActuary, BIExecutive, BIUnderwriter, BIProducer, BIC
BIActuary	BIActuaries
BIExecutive	BIExecutives
BIUnderwriter	BIUnderwriters
BIProducer	BIProducers
BIClaimsManager	BIClaimsManagers

Figure 32: OII Application Roles Mapped to BIAuthors and BIConsumers Application Roles

6. In the navigation tree in the left pane expand **Business Intelligence** and select **coreapplication**.
 7. When the page refreshes, select the **Capacity Management** tab to open the **Capacity Management** page.

Name	Status	Host	Port	Oracle Instance	Note
BI Presentation Servers	Up				
coreapplication_obips1	Up	plqasight03	9710	instance1	
BI Servers	Up				
BI Schedulers	Up				
BI Cluster Controllers	Up				
BI JavaHosts	Up				

Figure 33: Select “Restart All” Button

8. Select **Restart All** to restart all the services and apply your changes.

STEP 7: TEST THE OII USERS IN OBIEE

This step requires you to log into OBIEE using the five user accounts that you created and configured in the previous steps.

1. Open a new browser window and enter the following URL:

`http://<hostname>:<port>/analytics`

Note In the above URL:

- <hostname> - is the server name or IP address where you installed OBIEE
- <port> - is the port assigned to OBIEE. The default port will be different depending on whether or not you selected a “Simple” or “Enterprise” Install for OBIEE.
 - **Simple Install** - the default port is 7001.
 - **Enterprise Install** - the default port is 9704 but the user has the option to specify ports during the installation.

2. A login screen for OBIEE will appear.

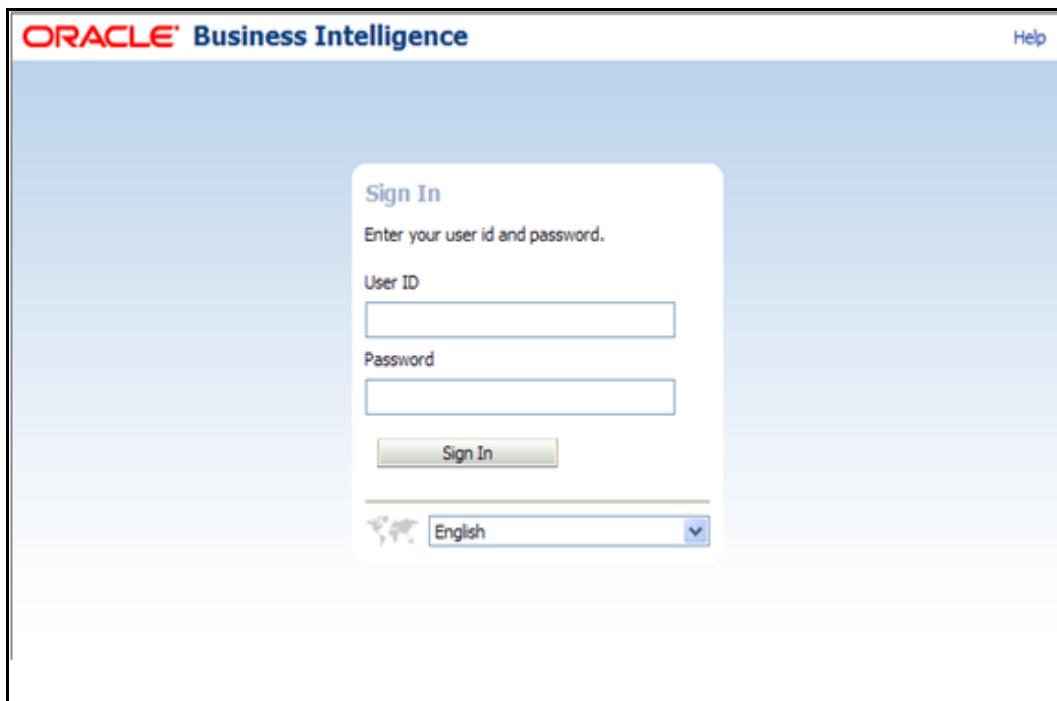


Figure 34: Oracle Business Intelligence Login Screen

3. Login separately as the test user for each of the OII groups you created.

Viewing the Content within OBIEE

Once you are logged into OBIEE, only the data for the role that was assigned to that particular user is displayed in the dashboards. For example, the **executive** user will only display the contents associated with the **executive** role. The Analysis reports listed in the Analysis Dashboard are directly related to the role(s) of the current user as well as the selected Line of Business and Corporate mart. Note that since only one role is associated with the user there are no tabs along the top of the page.

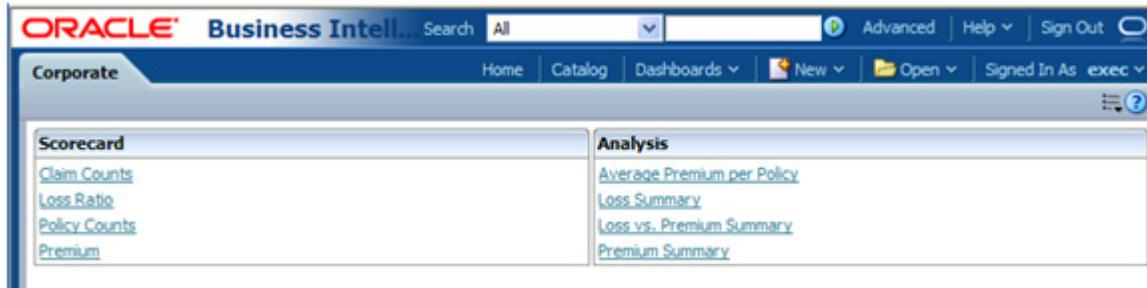


Figure 35: Executive User (Corporate)

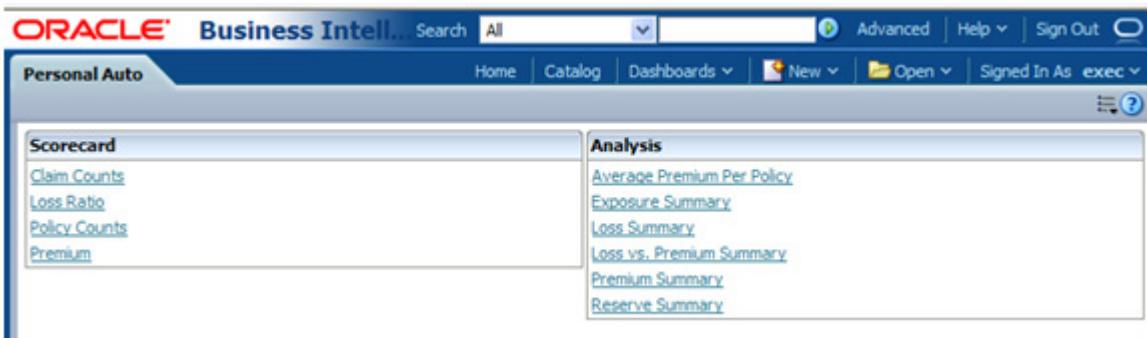


Figure 36: Executive User (Personal User)

Corporate

Corporate has the following four Analysis Dashboard reports assigned across the five OII roles:

Table 1: Corporate - Analysis Dashboard Reports by Role

Report	Actuary	Claims Management	Executive	Production	Underwriting
Average Premium per Policy	X		X		X
Loss Summary	X	X	X		X
Loss vs. Premium Summary	X		X		X
Premium Summary	X		X		X

Lines of Business

The Lines of Business have the following Analysis Dashboard reports assigned across these roles:

Table 2: Line of Business - Analysis Dashboard Reports by Role

Report	Actuary	Claims Management	Executive	Production	Underwriting
Average Premium per Policy	X		X		X
Claims Summary		X			
Exposure Summary	X	X	X		X
Loss Summary	X	X	X		X
Loss Triangulation	X	X			
Loss vs. Premium Summary	X		X		X
Premium Summary	X		X		X
Reserve Summary	X	X	X		

ADDING ADDITIONAL USERS

Now that you have successfully created and mapped the OII application roles and groups, you can add others OII users by following the instructions outlined in *Step 3: Create the OII Users* on page 21.

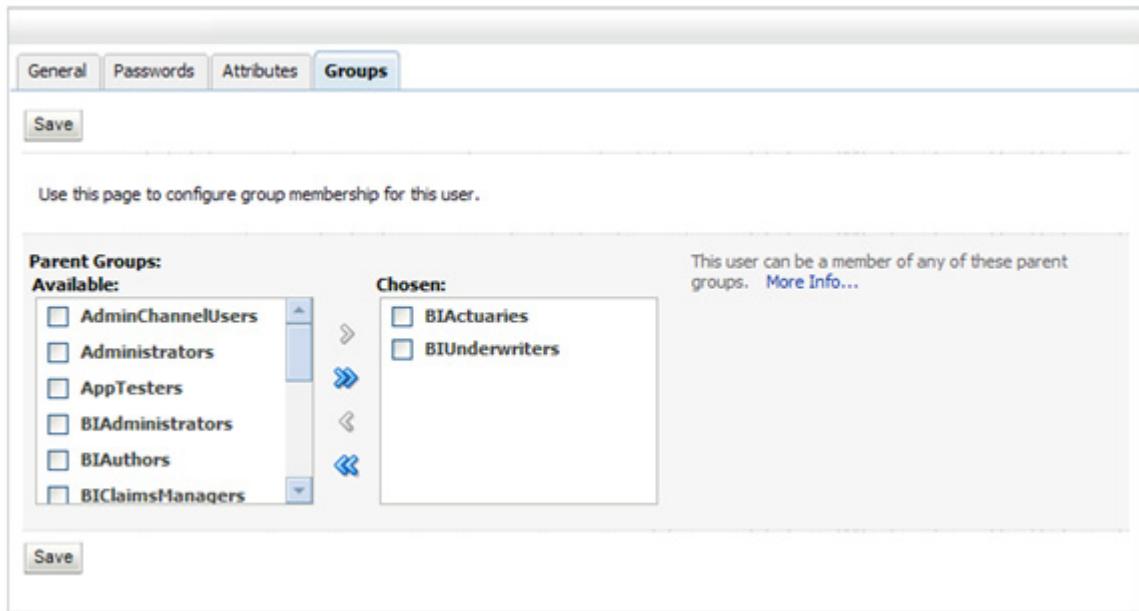


Figure 37: Add User to Multiple OII Groups.

Users can be assigned to multiple groups as required and inherit the roles that are assigned to those groups to determine the content available to them within OBIEE.

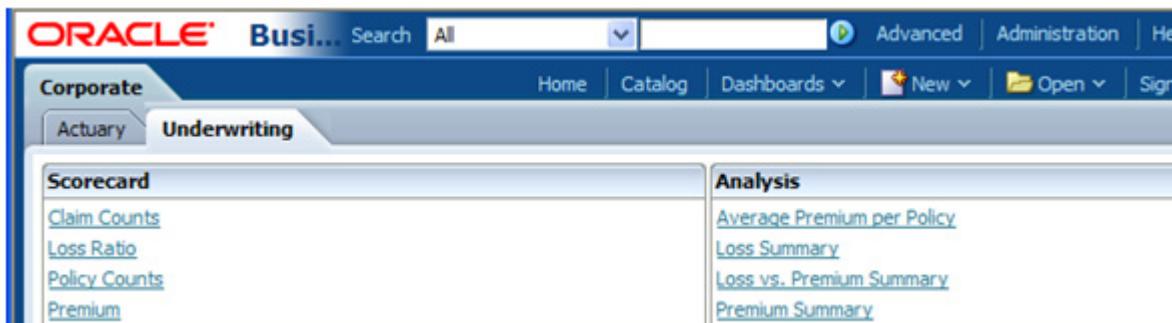


Figure 38: User Assigned to Actuary and Underwriting Role

INDEX

A

Actuary, 1
Adding users to the OII groups, 23
Application Roles
 creating, 13
application roles, 1

B

BIActuary, 13
BIAuthor, 29
BIClaimsManager, 13
BIConsumer, 29
BIExecutive, 13
BIProducer, 13
BIUnderwriter, 13

C

Claims Management, 1

E

Executive, 1

G

Groups (OII)
 mapping to OII application Roles, 25

M

Mapping OII groups to OII application roles, 25

O

OII Users
 creating, 21
Oracle Fusion Middleware Control
 opening, 3
Oracle WebLogic Server Administration Console
 opening, 5

P

Production, 1

R

Roles
 Analysis Dashboard Reports, 32

S

Security Groups
 creating, 17

U

Underwriting, 1

