Oracle® Fusion Middleware

Security Guide for Oracle Business Intelligence Enterprise Edition

12*c* (12.2.1)

E57380-03

December 2015

Explains how to configure Oracle Business Intelligence Enterprise Edition security, including settings for SSO, SSL, external authentication, and Presentation Services privileges.

ORACLE

Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition, 12*c* (12.2.1)

E57380-03

Primary Author: Nick Fry

Contributors: Oracle Business Intelligence development, product management, and quality assurance teams.

Contents

3 Using Alternative Authentication Providers

4 Enabling SSO Authentication

5 Configuring SSL in Oracle Business Intelligence

A Legacy Security Administration Options

B Understanding the Default Security Configuration

C Troubleshooting Security in Oracle Business Intelligence

D Managing Security for Dashboards and Analyses

Preface

The Oracle Business Intelligence Foundation Suite is a complete, open, and integrated solution for all enterprise business intelligence needs, including reporting, ad hoc queries, OLAP, dashboards, scorecards, and what-if analysis. The Oracle Business Intelligence Foundation Suite contains Oracle Business Intelligence Enterprise Edition.

Oracle Business Intelligence Enterprise Edition (Oracle BI EE) is a comprehensive set of enterprise business intelligence tools and infrastructure, including a scalable and efficient query and analysis server, an ad-hoc query and analysis tool, interactive dashboards, proactive intelligence and alerts, and an enterprise reporting engine.

The components of Oracle BI EE share a common service-oriented architecture, data access services, analytic and calculation infrastructure, metadata management services, semantic business model, security model and user preferences, and administration tools. Oracle BI EE provides scalability and performance with data-source specific optimized request generation, optimized data access, advanced calculation, intelligent caching services, and clustering.

This guide contains information about system administration tasks and includes topics on enabling and managing a secure environment.

Audience

This guide is intended for system administrators who are responsible for managing Oracle Business Intelligence security.

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 and Other Resources

See the Oracle Business Intelligence documentation library for a list of related Oracle Business Intelligence documents.

See also the following related document:

- *Oracle Fusion Middleware Application Security Guide*

In addition:

- Go to the Oracle Learning Library for Oracle Business Intelligence-related online training resources.
- Go to the Product Information Center support note (Article ID 1267009.1) on My Oracle Support at https://support.oracle.com.

System Requirements and Certification

Refer to the system requirements and certification documentation for information about hardware and software requirements, platforms, databases, and other information. Both of these documents are available on Oracle Technology Network (OTN).

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

Conventions

The following text conventions are used in this document:

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

New Features in Oracle Business Intelligence Security

This preface describes changes in securing Oracle Business Intelligence Enterprise Edition 12*c* (12.2.1).

If you are upgrading to Oracle BI EE from a previous release, read the following information carefully, because there are significant differences in features, tools, and procedures. For more information about upgrading to Oracle BI EE 12*c*, see *Oracle Fusion Middleware Upgrade Guide for Oracle Business Intelligence Enterprise Edition*.

This preface contains the following topics:

New Features for Oracle BI EE 12*c* (12.2.1)

New security features in Oracle BI EE 12*c* (12.2.1) include:

BISystemUser and BISystem Removed

To simplify administration and configuration in this release Oracle Business Intelligence no longer requires a real user called BISystemUser (or equivalent) for internal communication. The system user concept is now deemed "virtual" and is represented by the credential oracle.bi.system/system.user, for which the values are securely randomly generated by the Configuration Assistant. Oracle BI components continue to use this credential for internal communication, backed by Oracle BI Security. The application role BISystem is also no longer present in the Policy Store, and will be removed from any upgraded 11*g* environment.

User GUIDs Removed

In this release user GUIDs have been removed to make administration easier. There is no longer any need to refresh GUIDs as part of lifecycle operations. GUIDs are replaced with user names. Users now authenticate by user ID, which means that a user authenticating with a particular user ID is granted access permissions associated with their user ID. Therefore, a user leaving the system must have their user ID completely

removed. Your administrator is now responsible for ensuring that users leaving the system are totally removed from Oracle Business Intelligence.

For more information, see Section 2.9, "Deleting a User".

Database Security Store

In this release the Security Store (Policy and Credential Stores) is configured in a relational database rather than in a file. The database is the same as used by RCU. This change makes scaling easier, and makes clusters more reliable.

For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*.

Easier SSL Configuration

In this release configuring SSL end to end is now less complex and uses offline commands.

The key differences in SSL support in this release (from 11*g*) are as follows:

- SSL uses the WebLogic trust store

  No additional BI-specific trust configuration is required.

- Offline commands

  There is no need to use Fusion Middleware Control UI to configure processes.

- Diagnostics for WebLogic certificate issues
- Higher security - TLSv1.2 only
- Configuration is central and not intermingled with user configuration.
- Supports advanced options with no risk of settings being overwritten.

For more information about SSL, see Chapter 5, "Configuring SSL in Oracle Business Intelligence".

Migrating Catalog Groups to Application Roles

In this release a new process enables you to migrate Catalog groups to application roles.

For more information, see Section D.2.2.1, "Migrating Catalog Groups to Application Roles".

1

Introduction to Security in Oracle Business Intelligence

This chapter introduces the Oracle Business Intelligence security model, discusses the tools used to configure security, and provides a detailed road map for configuring security in Oracle Business Intelligence.

Note: For a high-level road map for setting up security, see Section 1.1, "High-Level Roadmap for Setting Up Security in Oracle Business Intelligence".

Note: If you have installed BI Publisher on its own and you plan to use Oracle Fusion Middleware Security, then see "Understanding the Security Model" in *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*.

This chapter contains the following sections:

1.1 High-Level Roadmap for Setting Up Security in Oracle Business Intelligence

To set up security in Oracle Business Intelligence, you must do the following:

1. Read the rest of this chapter to get an overview of security concepts, tools, and terminology.

2. Learn about users, groups, and application roles by reading the summary in Section 2.1, "Working with Users, Groups, and Application Roles".
3. Decide which authentication provider to use to authenticate users.
4. Set up the required users and groups.
5. Set up the required application roles.
6. Assign each group to an appropriate application role.
7. Fine-tune the permissions that users and groups have in the Oracle BI repository.
8. Fine-tune the permissions that users and groups have in the Oracle BI Presentation Catalog.
9. If required, configure Single Sign-On (SSO).
10. If required, configure Secure Sockets Layer (SSL).

For a detailed list of setup steps, see Section 1.7, "Detailed List of Steps for Setting Up Security in Oracle Business Intelligence".

1.2 Overview of Security in Oracle Business Intelligence

Oracle Business Intelligence 12*c* is tightly integrated with the Oracle Fusion Middleware Security architecture and delegates core security functionality to components of that architecture. Specifically, any Oracle Business Intelligence installation makes use of the following types of security providers:

- An **authentication provider** that knows how to access information about the users and groups accessible to Oracle Business Intelligence and is responsible for authenticating users.
- A **policy store provider** that provides access to application roles and application policies, which forms a core part of the security policy and determines what users can and cannot see and do in Oracle Business Intelligence.
- A **credential store provider** that is responsible for storing and providing access to credentials required by Oracle Business Intelligence.

By default, an Oracle Business Intelligence installation is configured with an authentication provider that uses the Oracle WebLogic Server embedded LDAP server for user and group information. The Oracle Business Intelligence default policy store provider and credential store provider store credentials, application roles and application policies in a database.

After installing Oracle Business Intelligence you can reconfigure the domain to use alternative security providers, if desired. For example, you might want to reconfigure your installation to use an Oracle Internet Directory, Oracle Virtual Directory, Microsoft Active Directory, or another LDAP server for authentication. You might also decide to reconfigure your installation to use Oracle Internet Directory, rather than a database, to store credentials, application roles, and application policies.

Several Oracle Business Intelligence legacy authentication options are still supported for backward compatibility. The best practice is to perform authentication and authorization using an identity store and authentication provider through the default security model described in this chapter. However, there are certain scenarios where this is not possible or where certain aspects of the legacy approach to authentication and authorization are required. Typically the use of these alternative methods requires that your user population and groups are not held in the identity store referenced by the authentication provider configured in the Oracle WebLogic domain. Consequently,

when using alternative authentication methods, several sections of this chapter are not relevant. Instead, refer to Appendix A, "Legacy Security Administration Options". Note that application roles described in this chapter are still used with alternative authentication and authorization mechanisms.

1.3 About Authentication

Each Oracle Business Intelligence 12*c* installation has an associated Oracle WebLogic Server domain. Oracle Business Intelligence delegates user authentication to the authentication providers configured for that domain.

The default authentication provider accesses user and group information that is stored in the LDAP server that is embedded in the Oracle WebLogic Server domain for Oracle Business Intelligence. You can use the Oracle WebLogic Server Administration Console to create and manage users and groups in the embedded LDAP server.

You might choose to configure an authentication provider for an alternative directory. You can use the Oracle WebLogic Server Administration Console to view the users and groups in the directory. However, you must continue to use the appropriate tools to make any modifications to the directory. For example, if you reconfigure Oracle Business Intelligence to use Oracle Internet Directory (OID), you can view users and groups in Oracle WebLogic Server Administration Console but you must manage them using the OID Console. Refer to the BI certification matrix for information on supported LDAP directories.

For more information about managing users and groups in the embedded LDAP server, see Chapter 2, "Managing Security Using a Default Security Configuration".

For more information about Oracle WebLogic Server domains and authentication providers, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

1.4 About Authorization

After a user has been authenticated, the next critical aspect of security is ensuring that the user can do and see what they are authorized to do and see. Authorization for Oracle Business Intelligence 12*c* is controlled by a security policy defined in terms of application roles.

1.4.1 About Application Roles

Instead of defining the security policy in terms of users in groups in a directory server, Oracle Business Intelligence uses a role-based access control model. Security is defined in terms of application roles that are assigned to directory server groups and users. For example, application roles BIServiceAdministrator, BI Consumer, and BIContentAuthor.

Application roles represent a functional role that a user has, which gives that user the privileges required to perform that role. For example, having the Sales Analyst application role might grant a user access to view, edit and create reports on a company's sales pipeline.

This indirection between application roles and directory server users and groups allows the administrator for Oracle Business Intelligence to define the application roles and policies without creating additional users or groups in the corporate LDAP server. Instead, the administrator defines application roles that meet the authorization requirements and assigns those roles to preexisting users and groups in the corporate LDAP server.

In addition, the indirection afforded by application roles allows the artifacts of a business intelligence system to be easily moved between development, test and production environments. No change to the security policy is needed and all that is required is to assign the application roles to the users and groups available in the target environment.

Figure 1-1 shows an example set of users, groups, and application roles.

Figure 1–1 Example Users, Groups, Application Roles, and Permissions

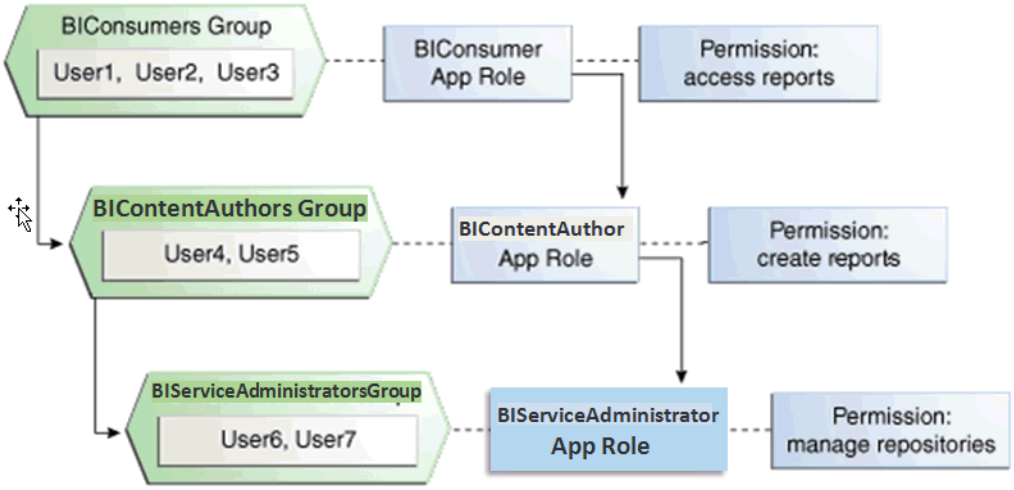


Figure 1-1 shows the following:

- The group named BIConsumers contains User1, User2, and User3. Users in the group BIConsumers are assigned the application role BIConsumer, which enables the users to view reports.
- The group named BIContentAuthors contains User4 and User5. Users in the group BIContentAuthors are assigned the application role BIContentAuthor, which enables the users to create reports.
- The group named BIServiceAdministrators contains User6 and User7. Users in the group BIServiceAdministrators are assigned the application role BIServiceAdministrator, which enables the users to manage responsibilities.

1.4.2 About the Security Policy

The security policy definition is split across the following components:

- Oracle BI Presentation Services – This defines which catalog objects and Oracle BI Presentation Services functionality can be accessed by which users with specific application roles. Access to functionality is defined in the Managing Privileges page in terms of Oracle BI Presentation Services privileges and access to Oracle BI Presentation Catalog objects is defined in the Permission dialog.
- Repository – This defines which metadata items within the repository can be accessed by which application roles and users. The Oracle BI Administration Tool is used to define this security policy.
- Policy Store – This defines which BI Server and Oracle BI Publisher functionality can be accessed by given users or users with given application roles. In the default Oracle Business Intelligence configuration, the policy store is managed using Oracle Enterprise Manager Fusion Middleware Control or by using WebLogic

scripting (WLST). For more information about the policy store, see *Oracle Fusion Middleware Application Security Guide*.

To find out about using these components, see Section 1.6, "Using Tools to Configure Security in Oracle Business Intelligence".

1.5 About Users, Groups, and Application Roles

In Oracle Business Intelligence 12*c* the author of a BI application is free to define and name the application roles and permission grants for their application as they choose. They are no longer constrained to include the handful of default application roles and permission grants that existed in Oracle BI 11*g*. However, they can still use a starting set of application roles and permission set grants if they choose.

When you initially configure Oracle Business Intelligence, you will choose to create the initial BI service instance based on either a supplied BI Archive (BAR) file, or an 11*g* upgrade bundle (see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence*). The set of application roles and memberships that are initially available in your service instance will depend on which BAR file or 11*g* upgrade bundle you import into your service instance. For more information about the content of a BAR file, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*. In summary, the security policy imported includes the application role definitions, the application role memberships, permission set definitions, permission definitions, permission set grants, permission grants, plus Presentation Services and repository security policy.

For example, if you select to create your initial BI service instance based on the Sample App Lite BAR file or the Starter BAR file, your initial service instance will import the sample application roles and application policies for that application. This will leave you with a service instance provisioned with similar application roles to what you would see in a new 11*g* installation.

Alternatively, if you select to create your initial service instance as a clean slate, the system will import a special empty BAR file into your service instance which results in a minimal set of application roles and policies being added to your service instance (just a BIServiceAdministrator application role). You are then able to create your own security policy specific to your own BI application.

If you create your initial service instance by importing an 11*g* upgrade bundle your service instance will have the same application roles, application role memberships, permissions and permission grants that you had in 11*g*.

For the purposes of the remainder of this chapter, we will describe the security policy included in the Sample App Lite and Starter BAR files. These BAR files can be used as either examples or starting points for building your own BI applications.

1.6 Using Tools to Configure Security in Oracle Business Intelligence

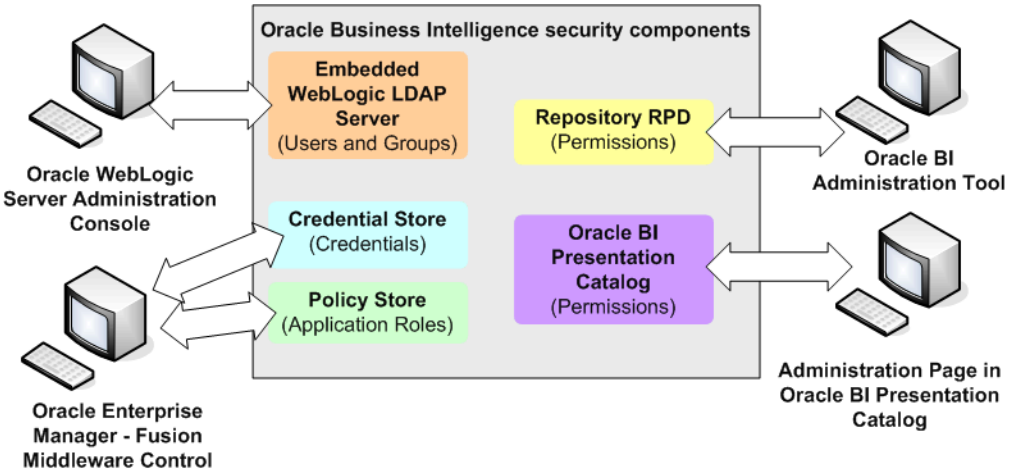
To configure security in Oracle Business Intelligence, you use the following tools:

- "Using Oracle WebLogic Server Administration Console"
- "Using Oracle Fusion Middleware Control"
- "Using Oracle BI Administration Tool"
- "Using Presentation Services Administration"

Note: To see an example of using the Oracle Business Intelligence tools to configure the installed users, groups, and application roles, see Section 2.2, "An Example Security Setup of Users, Groups, and Application Roles".

Figure 1–2 summarizes the tools that you use to configure security in an example installation of Oracle Business Intelligence that uses the embedded WebLogic LDAP Server.

Figure 1–2 Summary of Tools for Configuring Security in an Example Installation



For more information about managing security, see Chapter 2, "Managing Security Using a Default Security Configuration").

1.6.1 Using Oracle WebLogic Server Administration Console

You use Oracle WebLogic Server Administration Console to manage the WebLogic LDAP Server that you can use to authenticate users and groups.

Oracle WebLogic Server is automatically installed and serves as the default administration server. The Oracle WebLogic Server Administration Console is browser-based and is used, among other things, to manage the embedded directory server.

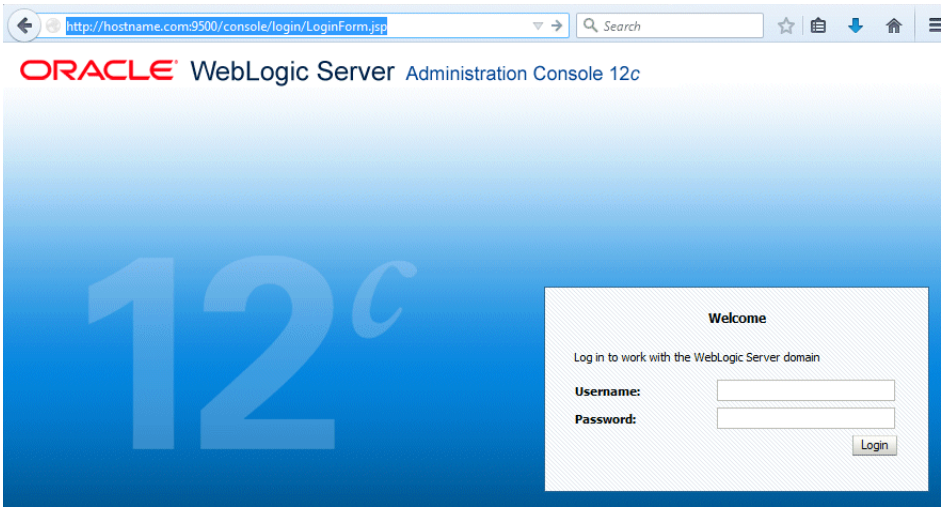
Note that when you configure Oracle Business Intelligence the initial security configuration uses the embedded Weblogic LDAP directory - the default authenticator - as the Identity Store. However, whereas in 11*g* the BI installation seeded some specific users and groups into this LDAP directory, in 12*c* we no longer seed default BI groups into this directory. Consequently, if your application expects LDAP groups such as BIConsumers, BIContentAuthors and BIServiceAdministrators to exist in the Identity Store, you will need to add these groups manually or configure the domain to use a different Identity Store where these groups are already provisioned after the initial BI configuration has finished.

You launch the Oracle WebLogic Server Administration Console by entering its URL into a web browser. The default URL takes the following form: http://*hostname:port_number*/console. The port number is the same as used for the Administration Server; 9500 is the default port. For more information about using the Oracle WebLogic Server Administration Console, see *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

To log in to the Oracle WebLogic Server Administration Console:

1. Display the Oracle WebLogic Server login page by entering its URL into a web browser.

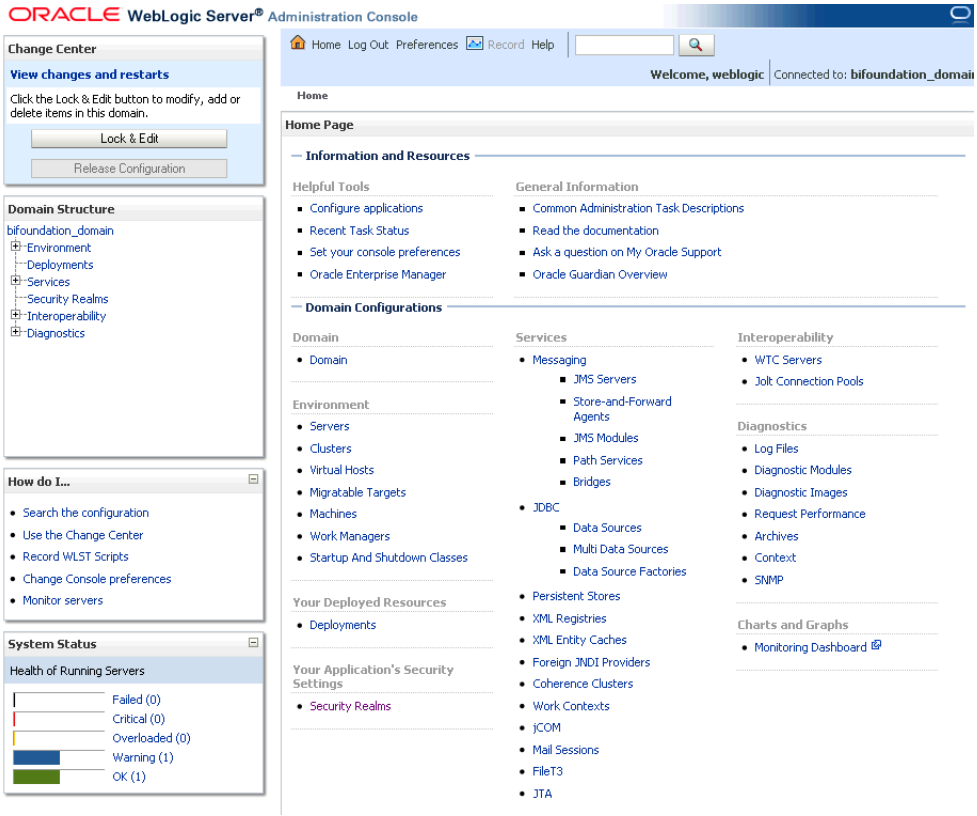
   For example, http://*hostname:9500*/console.



2. Log in using the Oracle Business Intelligence administrative user and password credentials and click **Login**.

   The user name and password were supplied during the installation of Oracle Business Intelligence. If these values have since been changed, then use the current administrative user name and password combination.

   The Administration Console displays.



3. Use the tabs and options in the Domain Structure as required to configure users, groups, and other options.

> **Note:** If you use an alternative authentication provider, such as Oracle Internet Directory instead of the default the WebLogic LDAP Server, then you must use the alternative authentication provider administration application (for example an administration console) to manage users and groups.

1.6.2 Using Oracle Fusion Middleware Control

Fusion Middleware Control is a web browser-based graphical user interface that enables you to administer a collection of components called a farm. A farm contains Oracle WebLogic Server domains, one Administration Server, one or more Managed Servers, clusters, and the Oracle Fusion Middleware components that are installed, configured, and running in the domain. During configuration of Oracle Business Intelligence an Oracle WebLogic Server domain is created and Oracle Business Intelligence is configured into that domain. The domain is named **bi** (in Enterprise installations), and is found under the **WebLogic Domain** folder in the Fusion Middleware Control navigation pane.

You use Oracle Fusion Middleware Control to manage Oracle Business Intelligence security as follows:

- Manage the application roles and application policies that control access to Oracle Business Intelligence resources.
- Configure multiple authentication providers for Oracle Business Intelligence.

To log in to Fusion Middleware Control, open a web browser and enter the Fusion Middleware Control URL, in the following format:

```
http://hostname.domain:port/em
```

The port number is the number of the Administration Server, and the default port number is 9500.

For more information about using Fusion Middleware Control, see *Oracle Fusion Middleware Administrator's Guide*.

To use Fusion Middleware Control:

1. Enter the URL in a web browser. For example:

   ```
   http://host1.example.com:9500/em
   ```

   The Fusion Middleware Control login page is displayed, as shown in Figure 1–3.

Figure 1–3 Login Page for Fusion Middleware Control

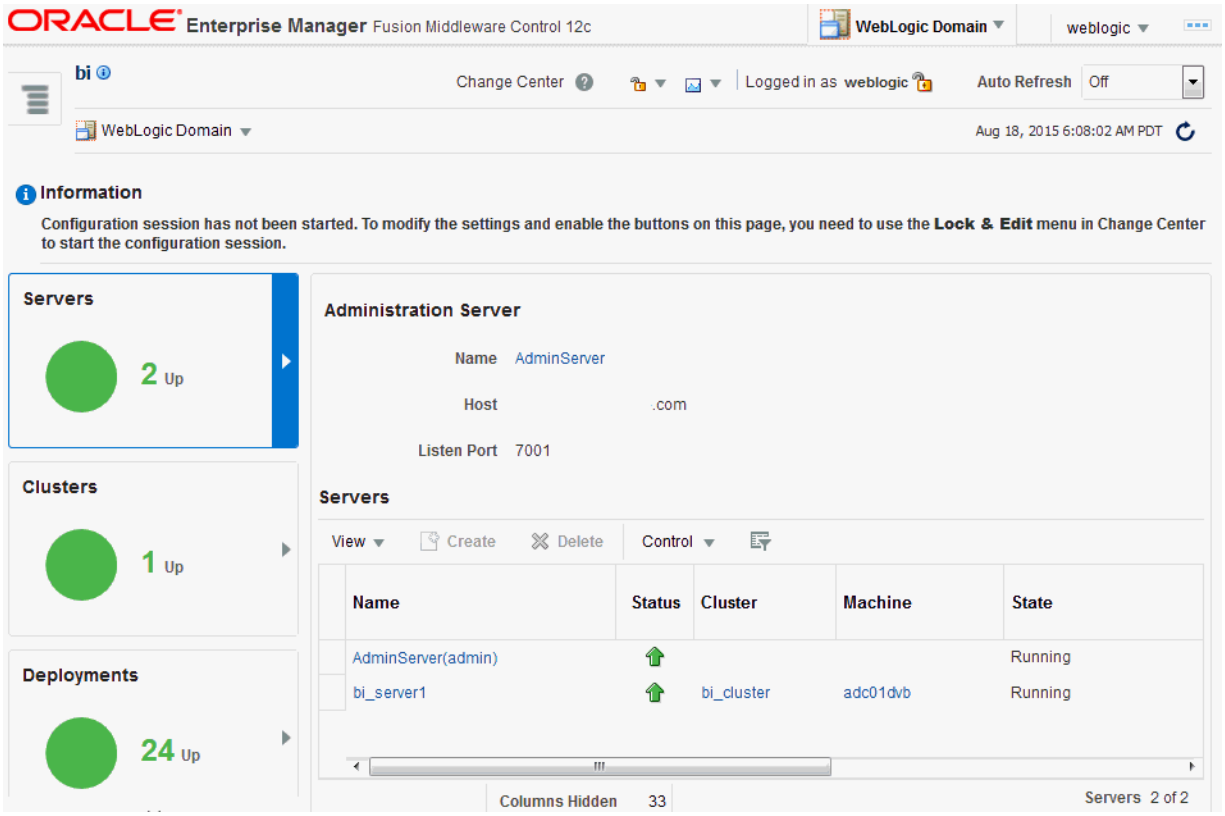
2. Enter the system administrator user name and password and click **Login**.

   This system-wide administration user name and password was specified during the installation process, and you can use it to log in to Oracle WebLogic Server Administration Console, Fusion Middleware Control, and Oracle Business Intelligence.

   Alternatively, enter any other user name and password that has been granted the WEbLogic Global Admin role.

   Fusion Middleware Control opens, as shown in Figure 1–4.

Figure 1–4 Main Page in Fusion Middleware Control



3. From the main page, click the target navigation icon in the top left of the page, then expand the **Business Intelligence** folder.
4. Select **biinstance** to display pages specific to Oracle Business Intelligence.
5. Manage Oracle Business Intelligence security using Fusion Middleware Control as follows:
   - Manage application roles and application policies.

     For more information, see Section 2.4, "Managing Application Roles and Application Policies Using Fusion Middleware Control".
   - Configure Secure Sockets Level (SSL).

     For more information, see:
     - Section 5.2.2.2, "Configuring HTTPS Ports"
     - Section 5.14.1, "Configuring SSL for the SMTP Server Using Fusion Middleware Control"

1.6.3 Using Oracle BI Administration Tool

You use the Oracle BI Administration Tool to configure permissions for users and application roles against objects in the metadata repository.

To use the Administration Tool:

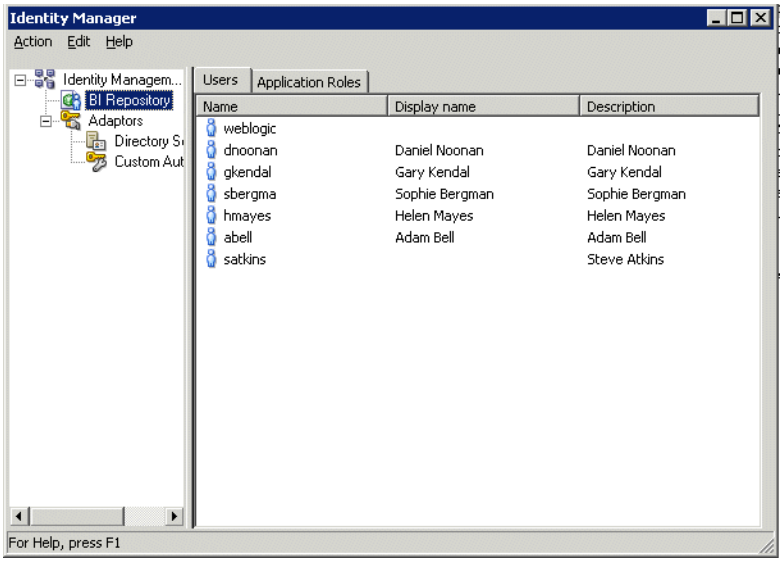
1. Log in to the Administration Tool.

Note: If you log in to the Administration Tool in online mode, then you can view all users from the WebLogic Server. If you log in to the Administration Tool in offline mode, then you can only view references to users that have previously been assigned metadata repository permissions directly in the RPD. Please note that best practice is to assign metadata repository permissions to application roles rather than directly to users.

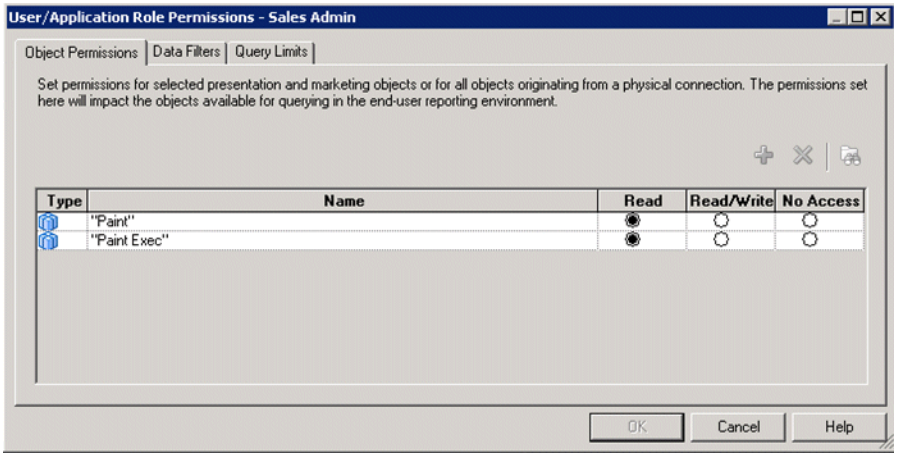
2. (Optional) Select **Manage**, then **Identity** to display the Identity Manager dialog.

   Figure 1–5 shows the Identity dialog.

Figure 1–5 Identity Manager Dialog



If you double-click an application role to display the Application Role <*Name*> dialog, then click Permissions, you can use the Object Permissions tab to view or configure (in the repository) the Read and Write permissions for that application role, in relation to objects and folders in the Oracle BI Presentation Catalog.

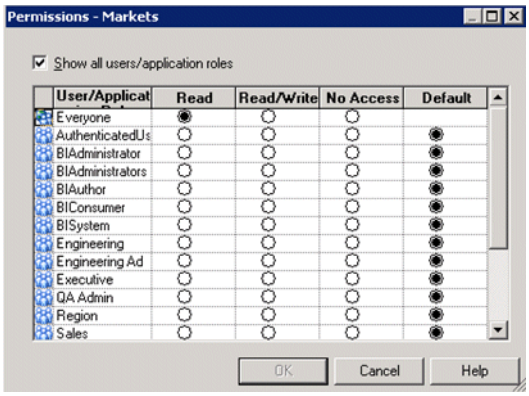


3. Close Identity Manager.

4. In the Presentation pane, expand a folder, then right-click an object to display the Presentation Table <*Table name*> dialog.
5. Click **Permissions** to display the Permissions <*Table name*> dialog.

   Figure 1–6 shows users and some application roles and the radio buttons Read, Read/Write, No Access, and Default that you use to set the permissions for the application roles.

Figure 1–6 Permissions Dialog Showing Application Roles



1.6.4 Using Presentation Services Administration

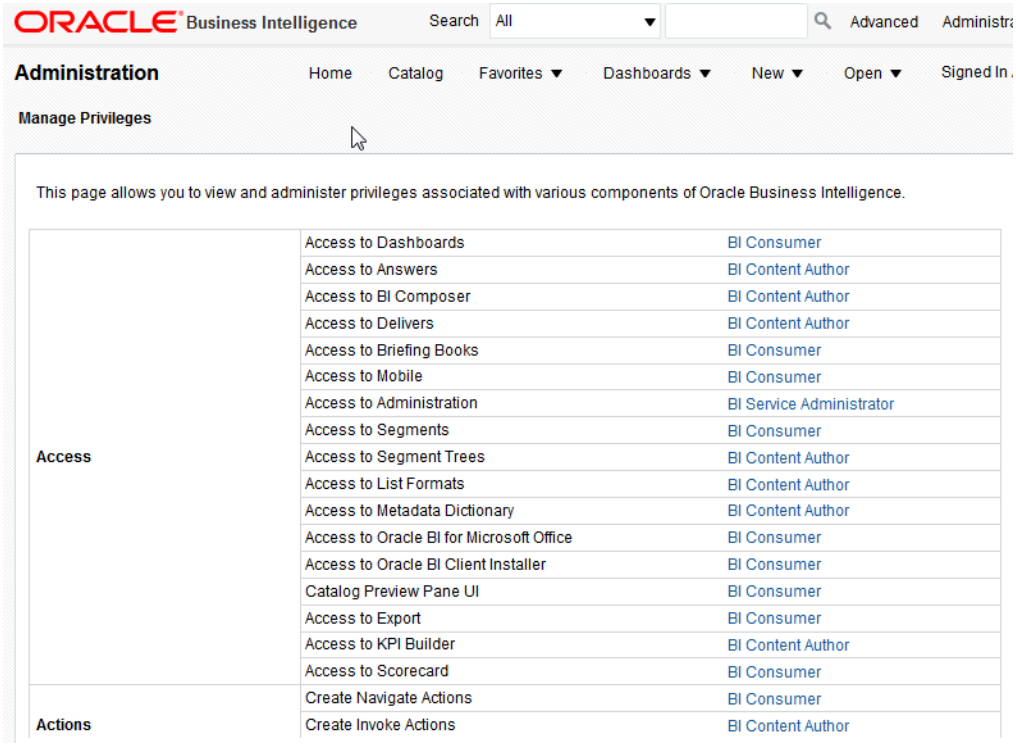
You use the Presentation Services Administration page to configure user privileges.

To use the Presentation Services Administration page:

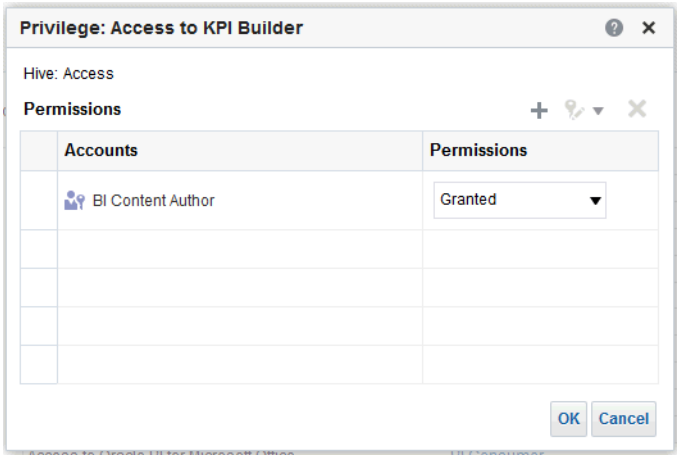
1. Log in to Oracle Business Intelligence with Administrator privileges.
2. Select the **Administration** link to display the Administration page.
3. Select the **Manage Privileges** link.

   Figure 1–7 shows application roles listed against the privileges to which they are assigned.

Figure 1–7 Manage Privileges Page in Presentation Services Administration Showing Application Roles



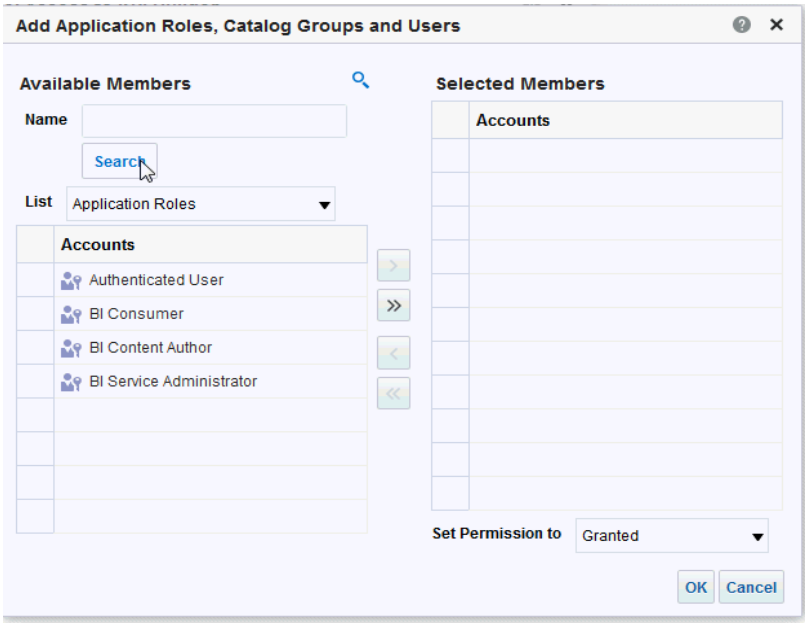
4. Select a link (for example BIContentAuthor) for a particular privilege (for example, Access to KPI Builder), to display the Privilege <*Privilege name*> dialog.



5. Click the Add users/roles icon (+) to display the Add Application Roles, Catalog Groups, and Users dialog.

   Use this dialog to assign application roles (for example, BIServiceAdministrator, BIContentAuthor, and BIConsumer) to this privilege.

   Please note that best practice is to assign Presentation Services permissions to application roles rather than directly to users.



1.7 Detailed List of Steps for Setting Up Security in Oracle Business Intelligence

This section explains how to set up security in a new installation of Oracle Business Intelligence. Some tasks are mandatory, some are optional, and some are conditionally required depending on the configuration choices that you make. You might also refer to this section if you are maintaining an existing installation of Oracle Business Intelligence.

After you have installed Oracle Business Intelligence, you typically evaluate the product using the sample application. Later, you typically create and develop your own users, groups, and application roles iteratively to meet your business requirements.

After you have installed Oracle Business Intelligence, Oracle recommends that you complete these tasks in the following order:

1. Read this chapter to get an overview of security concepts, tools, and terminology. In particular, you should familiarize yourself with the Oracle Business Intelligence components and tools for configuring security by reading Section 1.6, "Using Tools to Configure Security in Oracle Business Intelligence"
2. Learn about users, groups, and application roles by reading the summary in Section 2.1, "Working with Users, Groups, and Application Roles".
3. Decide which authentication provider to use to authenticate users, as follows:
   - If you want to use the default embedded WebLogic LDAP Server, then follow the tasks listed in Step 4.
   - If you want to reconfigure Oracle Business Intelligence to use an alternative authentication provider such as Oracle Internet Directory (OID), then follow the tasks listed in Step 5.

Tip: Oracle does not recommend using WebLogic Embedded LDAP Server in an environment with more than 1000 users. If you require a production environment with high-availability and scalability, then you should use a directory server such as Oracle Internet Directory (OID) or a third-party directory server.

For information about where to find the full list of supported authentication providers, see "System Requirements and Certification".

4. (Embedded WebLogic LDAP Server-specific) If you are using the default embedded WebLogic LDAP Server as the authentication provider, do the following:
   a. Set up the users that you want to deploy as described in Section 2.3.2, "Creating a New User in the Embedded WebLogic LDAP Server".

      For example, if you want to deploy Oracle Business Intelligence to 20 people who need to view analyses, you might create 20 users.
   b. If you want to create new groups, set up the groups that you want to use as described in Section 2.3.3, "Creating a New Group in the Embedded WebLogic LDAP Server".
   c. Assign your users to appropriate groups, as described in Section 2.3.4, "Assigning a User to a Group in the Embedded WebLogic LDAP Server".
   d. Assign groups of users to application roles.

      For detailed steps, see Section 2.3.1, "Assigning a User to a New Group, and a New Application Role".
5. (Oracle Internet Directory (OID) specific) If you are using OID as the authentication provider, do the following:
   a. Configure OID as the authentication provider as described in Section 3.2, "High-Level Steps for Configuring an Alternative Authentication Provider".
   b. Use your authentication provider tools (for example, OID Console) to create your users and groups as required.
6. Set up the application roles that you want to deploy as described in Section 2.4.2, "Creating and Deleting Application Roles Using Fusion Middleware Control".

   For example, you might use BIConsumer, BIContentAuthor, and BIServiceAdministrator, or you might create your own application roles.
7. (Optional) If you do not want to use existing application policies, you can set up the application policies that you want to deploy as described in Section 2.4.3, "Creating Application Policies Using Fusion Middleware Control".

   For example, you might use the application policies that are used by the sample application roles BIConsumer, BIContentAuthor, and BIServiceAdministrator, or you might create your own application policies.
8. Assign each group to an appropriate application role, as follows:
   - If you have created new groups, you must assign the new groups to appropriate application roles as described in Section 2.4.2.3, "Assigning a Group to an Application Role".
   - If you are using a commercial authentication provider such as Oracle Internet Directory, then you must assign the groups to appropriate application roles as

described in Section 2.4.2.3, "Assigning a Group to an Application Role".

9. If you want to fine-tune the permissions that users and groups have in the Oracle BI repository, use the Administration Tool to update the permissions as described in Section 2.5, "Managing Metadata Repository Privileges Using the Oracle BI Administration Tool".

   For example, you might want to enable an application role called BISuperConsumer to create analyses, so you use the Administration Tool to change the Read access to a subject area to Read/Write access.

   Note: If you are using the default SampleAppLite.rpd file in a production system, you should change the password from its installed value, using the Administration Tool. For more information about the SampleAppLite repository file, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

10. If you want to fine-tune the permissions that users and groups have in the Presentation Services Administration page to change the permissions as described in Section 2.6, "Managing Presentation Services Privileges Using Application Roles".

    For example, you might want to prevent an application role called BISuperConsumer from viewing scorecards, so you use Presentation Services Administration Page to change the Scorecard\View Scorecard privileges for BISuperConsumer from Granted to Denied.

11. If you want to deploy Single Sign-On, follow the steps in Chapter 4, "Enabling SSO Authentication".

12. If you want to deploy secure sockets layer (SSL), follow the steps in Chapter 5, "Configuring SSL in Oracle Business Intelligence".

    Oracle Business Intelligence is installed with SSL turned off. If you want to deploy Oracle Business Intelligence in an SSL environment, follow the steps in Chapter 5, "Configuring SSL in Oracle Business Intelligence".

1.8 Comparing the Oracle Business Intelligence 11*g* and 12*c* Security Models

The Release 11*g* and Release 12*c* security models differ in the following ways:

- BI System User - in Oracle Business Intelligence 11g a BI System User was used for inter-process communication and when impersonating BI users. In Oracle Business Intelligence 12c internal trust mechanisms replace this functionality and the BI System User is no longer required or provisioned.
- Application security policies - In Oracle Business Intelligence 11g a default BI installation provisioned a default security policy in a file. Oracle Business Intelligence 12c uses a database policy store and the active security policy is imported from a BI Application Archive file or amended directly in the service instance.
- Permissions and permission sets - in 11g the policy store specifies permissions which are (typically) assigned to application roles. In 12c a collection of Permission Sets have been added to collect together permissions that are typically assigned together as an entitlement. Permissions are still available, but in 12c

Permission Sets are the preferred unit for assigning permissions to application roles.

- User GUIDs - in Oracle Business Intelligence 11*g* user GUIDs were referenced at login and for security lookups in order to prevent inadvertent re-use of UserIds. In Oracle Business Intelligence 12*c* the user GUIDs are no longer referenced. Instead a cleaner approach to deleting a user from BI has been introduced. Refer to Section 2.9, "Deleting a User".

The following aspects of the Oracle Business Intelligence Release 11*g* security model remain in Release 12*c*:

- BI Server Initialization Blocks – The BI Server in Release 12c continues to support the use of initialization blocks for authentication and authorization. In Release 12*c* Oracle Business Intelligence falls back to use initialization blocks if the user cannot be authenticated by the installation's configured authentication provider.

  For more information, see "Working With Initialization Blocks" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*

- Catalog Groups – Oracle Business Intelligence Release 12*c* continues to support the definition of Catalog groups within the Oracle BI Presentation Catalog however, this functionality has been formally deprecated. These groups are only visible within Oracle BI Presentation Services. Oracle recommends that Oracle BI Presentation Catalog groups be used for backward compatibility only and that application roles be used instead for new installations.

  For more information, see Section D.2.2, "Working with Catalog Groups".

- SA System Subject Area – Oracle Business Intelligence Release 12*c* supports the use of SA System Subject Area, in combination with the BI Server initialization blocks, to access user, group and profile information stored in database tables.

  For more information, see "Setting Up the SA System Subject Area" in *Oracle Fusion Middleware Scheduling Jobs Guide for Oracle Business Intelligence Enterprise Edition*.

1.9 Terminology

The following terms are used throughout this guide:

Application Policy
Oracle Business Intelligence permissions are granted by its application roles. In the default security configuration, each role conveys a predefined set of permissions. An application policy is a collection of Java EE and JAAS policies that are applicable to a specific application. The application policy is the mechanism that defines the permissions each application role grants. Permission grants are managed in the application policy corresponding to an application role.

Application Role
Represents a role a user has when using Oracle Business Intelligence. Is also the container used by Oracle Business Intelligence to grant permissions to members of a role. Application roles are managed in the policy store provider.

Authentication
The process of verifying identity by confirming the credentials presented during log in.

Authentication Provider
A security provider used to access user and group information and responsible for authenticating users. Oracle Business Intelligence default authentication provider is Oracle WebLogic Server embedded directory server and is named DefaultAuthenticator.

Authorization
The process of granting an authenticated user access to a resource in accordance to their assigned privileges.

Catalog Groups
A Catalog group is defined locally in Oracle BI Presentation Services and is used to grant privileges in the Oracle Business Intelligence user interface in addition to granting Oracle BI Presentation Catalog permissions.

Catalog Permissions
These rights grant access to objects that are stored in the Oracle BI Presentation Catalog. The rights are stored in the catalog and managed by Presentation Services.

Catalog Privileges
These rights grant access to features of the Oracle BI Presentation Catalog. The rights are stored in the catalog and managed by Presentation Services. These privileges are either granted or denied.

Credential Store
An Oracle Business Intelligence credential store is a file used to securely store system credentials used by the software components. This file is automatically replicated across all machines in the installation.

Credential Store Provider
The credential store is used to store and manage credentials securely that are used internally between Oracle Business Intelligence components. For example, SSL certificates are stored here.

Encryption
A process that enables confidential communication by converting plain text information (data) to unreadable text which can be read-only with the use of a key. Secure Sockets Layer (SSL) enables secure communication over TCP/IP networks, such as web applications communicating through the Internet.

Impersonation
Impersonation is a feature used by Oracle Business Intelligence components to establish a session on behalf of a user without employing the user's password. For example, impersonation is used when Oracle BI Scheduler executes an Agent.

Oracle WebLogic Server Domain
A logically related group of Oracle WebLogic Server resources that includes an instance known as the Administration Server. Domain resources are configured and managed in the Oracle WebLogic Server Administration Console. For more information, see Section B.2.2, "Oracle WebLogic Server Domain".

Identity Store
An **identity store** contains user name, password, and group membership information. In Oracle Business Intelligence, the identity store is typically a directory server and is what an authentication provider accesses during the authentication process. For example, when a user name and password combination is entered at log in, the authentication provider searches the identity store to verify the credentials provided.

Oracle Business Intelligence can be re-configured to use alternative identity stores. For a complete list, see System Requirements and Certification.

Permission Set
Represents a set of permissions.

Policy Store Provider
The policy store is the repository of system and application-specific policies. It holds the mapping definitions between the default Oracle Business Intelligence application roles, permissions, users and groups all configured as part of installation. Oracle Business Intelligence permissions are granted by assigning users and groups from the identity store to application roles and permission grants located in the policy store.

Policy Store
Contains the definition of application roles, application policies, and the members assigned (users, groups, and application roles) to application roles. The default policy store is a file that is automatically replicated across all machines in an Oracle Business Intelligence installation. A policy store can be database-based or LDAP-based.

Secure Sockets Layer (SSL)
Provides secure communication links. Depending upon the options selected, SSL might provide a combination of encryption, authentication, and repudiation. For HTTP based links the secured protocol is known as HTTPS.

Security Policy
The security policy defines the collective group of access rights to Oracle Business Intelligence resources that an individual user or a particular application role have been granted. Where the access rights are controlled is determined by which Oracle Business Intelligence component is responsible for managing the resource being requested. A user's security policy is the combination of permission and privilege grants governed by the following elements:

- Oracle BI Presentation Catalog:

  Defines which Oracle BI Presentation Catalog objects and Oracle BI Presentation Services functionality can be accessed by users. Access to this functionality is managed in Oracle Business Intelligence user interface. These permissions and privileges can be granted to individual users or by membership in corresponding application roles.

- Repository File:

  Defines access to the specified metadata within the repository file. Access to this functionality is managed in the Oracle BI Administration Tool. These permissions and privileges can be granted to individual users or by membership in corresponding application roles.

- Policy Store:

  Defines which Oracle Business Intelligence, Oracle BI Publisher, and Oracle Real-Time Decisions functionality can be accessed. Access to this functionality is managed in Oracle Enterprise Manager Fusion Middleware Control. These permissions and privileges can be granted to individual users or by membership in corresponding application roles.

Security Realm
During deployment an Oracle WebLogic Server domain is created and Oracle Business Intelligence is deployed into that domain. Security for an Oracle WebLogic Server domain is managed in its **security realm**. A security realm acts as a scoping

mechanism. Each security realm consists of a set of configured security providers, users, groups, security roles, and security policies. Only one security realm can be active for the domain. Oracle Business Intelligence authentication is performed by the authentication provider configured for the default security realm for the WebLogic Server domain in which it is installed. Oracle WebLogic Server Administration Console is the Administration Tool for managing an Oracle WebLogic Server domain.

Single Sign-On

A method of authorization enabling a user to authenticate once and gain access to multiple software application during a single browser session.

Users and Groups

A **user** is an entity that can be authenticated. A user can be a person, such as an application user, or a software entity, such as a client application. Every user is given a unique identifier within in the identity store.

Groups are organized collections of users that have something in common. A group is a static identifier that is assigned by a system administrator. Users organized into groups facilitate efficient security management. There are two types of groups: an LDAP group and a Catalog group. A *Catalog group* is used to support the existing user base in Presentation Services to grant privileges in the Oracle Business Intelligence user interface. Using Catalog groups is not considered a best practice and is available for backward compatibility in upgraded systems.

2

Managing Security Using a Default Security Configuration

This chapter explains how to deploy Oracle Business Intelligence security using the embedded WebLogic LDAP Server with the sample application.

> **Note:** For a detailed list of security setup steps, see Section 1.7, "Detailed List of Steps for Setting Up Security in Oracle Business Intelligence".

By deploying the default embedded WebLogic LDAP Server with the sample application, you can use its default users, groups, and application roles. You can also develop your own users, groups, and application roles.

This chapter contains the following sections:

- Working with Users, Groups, and Application Roles
- An Example Security Setup of Users, Groups, and Application Roles
- Managing Users and Groups in the Embedded WebLogic LDAP Server
- Managing Application Roles and Application Policies Using Fusion Middleware Control
- Managing Metadata Repository Privileges Using the Oracle BI Administration Tool
- Managing Presentation Services Privileges Using Application Roles
- Managing Data Source Access Permissions Using Oracle BI Publisher
- Enabling High Availability of the Default Embedded Oracle WebLogic Server LDAP Identity Store
- Deleting a User
- Using the runcat Command Line Interface to Manage Security-Related Tasks in the Oracle BI Presentation Catalog

You can migrate users (with their encrypted passwords), groups, roles and policies from the embedded WebLogic LDAP server and into another one. For more information, see "Exporting and Importing Information in the Embedded LDAP Server" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

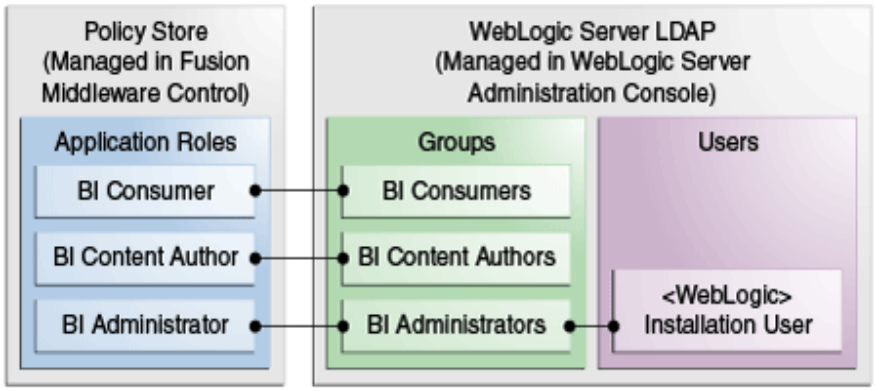
2.1 Working with Users, Groups, and Application Roles

When you configure Oracle Business Intelligence with the Sample Application made available with the BI installation a number of application roles are provided for you to use in order to provision users and groups to be able to use BI functionality and access BI folders, reports, data columns and other objects. For example, following a fresh installation of Oracle BI Enterprise Edition, if you have selected to populate your initial service instance using the sample application, the user specified for creating the BI domain during the configuration step will be assigned to an application role named BIServiceAdministrator. In addition to the BIServiceAdministrator application role, the from the sample application, these sample application roles have been preconfigured to work together. For example, a user who is a member of the BIServiceAdministrator application role will automatically inherit the BIContentAuthor and BIConsumer application roles and will therefore be provisioned with all the privileges and permissions associated with all of these application roles. For a detailed description of this security configuration, refer to Appendix B, "Understanding the Default Security Configuration".

The sample application roles have appropriate permissions and privileges to enable them to work with the sample Oracle BI Presentation Catalog, BI Repository, and Policy Store. For example, the application role BIContentAuthor is preconfigured with permissions and privileges that are required to create dashboards, reports, actions, and so on.

Figure 2–1 shows application roles, groups and users that are preconfigured in the sample and starter applications installation.

Figure 2–1 Application Roles Preconfigured With The Sample Application



When you initially configure your BI domain, a service instance is created based on one of the BI application archive (BAR) files that are included with the BI installation. Each BI application contains an application role that is tagged as the administration application role. The name of this administration application role is determined by the developer or author of the BI application archive. In the case of the sample, starter and empty applications available with the BI installation this administration application role is called BIServiceAdministrator. The authors of these applications have assigned specific permission sets and privileges to this application role to enable members of this application role to administer the system. When the BI service instance is created the BI system adminstrator specifies an owner (a user) for the service instance. The system will assign the administration application role to the service instance owner whenever a BI archive file is imported into the service instance.

Note: When importing an 11*g* upgrade bundle into a 12*c* service instance, the system will automatically tag the application role 'BIAdministrator' as the administration application role.

For more information, see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence* and "importServiceInstance" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

You can use the sample application roles to deploy security. You can then create your own groups and application roles to meet your business needs. For example:

- If you want to enable an employee called Fred to create dashboards and reports, you might create a new user called Fred and assign Fred to the default BIContentAuthors group.
- If you want user Fred to be a Sales dashboard author, you might create an application role called Sales_ Dashboard_ Author that has permissions to see Sales subject areas in the repository and edit Sales dashboards.
- If you want to enable user Fred to perform BIContentAuthors and Sales_ Dashboard_Author duties, you might create a new application role called BIManager, which has both BIContentAuthors privileges and Sales_Dashboard_ Author privileges.

For detailed information about the sample application roles, see Appendix B, "Understanding the Default Security Configuration."

2.2 An Example Security Setup of Users, Groups, and Application Roles

This example uses a small set of users, groups, and application roles to illustrate how you might set up a security model. In this example, you want to implement the following:

- Three users named User1, User2, and User3, who need to view business intelligence reports.
- Two users named User4 and User5, who need to create business intelligence reports.
- Two users named User6 and User7, who administer Oracle Business Intelligence.

Figure 2–2 shows the users, groups, and application roles that you would deploy to implement this example security model.

Figure 2–2 Example Users, Groups, and Application Roles

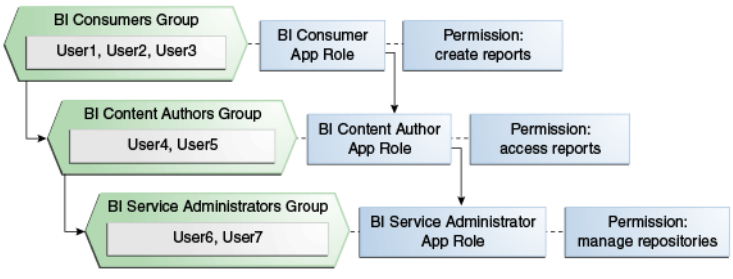


Figure 2–2 shows the following:

- The group named BIConsumers contains User1, User2, and User3. Users in the group BIConsumers are assigned to the application role named BIConsumer, which enables the users to view reports.
- The group named BIContentAuthors contains User4 and User5. Users in the group BIContentAuthors are assigned to the application role named BIContentAuthor, which enables the users to create reports.
- The group named BIServiceAdministrators contains User6 and User7. Users in the group BIServiceAdministrators are assigned to the application role named BIServiceAdministrator, which enables the users to manage repositories.

To implement this example security model:

1. Create seven users named User1 to User 7, as described in Section 2.3.2, "Creating a New User in the Embedded WebLogic LDAP Server".
2. Create the groups BIConsumers and BIContentAuthors and BIServiceAdministrators as described in Section 2.3.3, "Creating a New Group in the Embedded WebLogic LDAP Server".
3. Assign the users to the default groups, as follows:
   - Assign User1, User2, and User3 to the group named BIConsumers.
   - Assign User4 and User5 to the group named BIContentAuthors.
   - Assign User6 and User7 to the group named BIServiceAdministrators.

   For more information, see Section 2.3.4, "Assigning a User to a Group in the Embedded WebLogic LDAP Server".
4. Assign the groups to the sample application roles as follows:
   - Make the BIConsumers group a member of the BIConsumer application role.
   - Make the BIContentAuthors group a member of the BIContentAuthor application role.
   - Make the BIServiceAdministrators group a member of the BIServiceAdministrator application role.

   For more information, see Section 2.4.2.3, "Assigning a Group to an Application Role".

2.3 Managing Users and Groups in the Embedded WebLogic LDAP Server

This section explains how to manage users and groups in the Embedded WebLogic LDAP Server, and contains the following topics:

- Section 2.3.1, "Assigning a User to a New Group, and a New Application Role"
- Section 2.3.2, "Creating a New User in the Embedded WebLogic LDAP Server"
- Section 2.3.3, "Creating a New Group in the Embedded WebLogic LDAP Server"
- Section 2.3.4, "Assigning a User to a Group in the Embedded WebLogic LDAP Server"
- Section 2.9, "Deleting a User"
- Section 2.3.5, "(Optional) Changing a User Password in the Embedded WebLogic LDAP Server"

2.3.1 Assigning a User to a New Group, and a New Application Role

This section describes how to extend the security model by creating your own users, and assigning them to new groups, and new application roles.

For example, you might want to create a user called Jim and assign Jim to a new group called BIMarketingGroup that is assigned to a new application role named BIMarketingRole.

To create a new user and assign the user to a new group and a new application role:

1. Launch WebLogic Administration Console as described in Section 1.6.1, "Using Oracle WebLogic Server Administration Console".
2. Create a new user as described in Section 2.3.2, "Creating a New User in the Embedded WebLogic LDAP Server".
3. Create a new group as described in Section 2.3.3, "Creating a New Group in the Embedded WebLogic LDAP Server".
4. Assign the new user to the new group as described in Section 2.3.4, "Assigning a User to a Group in the Embedded WebLogic LDAP Server".
5. Create a new application role and assign it to the new group as described in Section 2.4.2.2, "Creating an Application Role".

   If you simply want to assign a group to an application role, follow the steps in Section 2.4.2.3, "Assigning a Group to an Application Role".
6. Edit the Oracle BI repository and set up the privileges for the new application role as described in Section 2.5.2, "Setting Repository Privileges for an Application Role".
7. Edit the Oracle BI Presentation Catalog and set up the privileges for the new user and group as described in Section 2.6.3, "Setting Presentation Services Privileges for Application Roles".

2.3.2 Creating a New User in the Embedded WebLogic LDAP Server

You typically create a separate user for each business user in your Oracle Business Intelligence environment. For example, you might plan to deploy 30 report consumers, 3 report authors, and 1 administrator. In this case, you would use Oracle WebLogic Server Administration Console to create 34 users, which you would then assign to appropriate groups.

Repeat this task for each user that you want to deploy.

Note: About the built-in Authenticated User application role.

All users who are able to log in are given a basic level of operational permissions conferred by the built-in Authenticated User application role. . The author of the BI application that is imported into your service instance may have designed the security policy so that all authenticated users are members of an application role that grants them privileges in the BI application. For more information, see Appendix B.4, "Security Configuration Using the Sample Application"

.

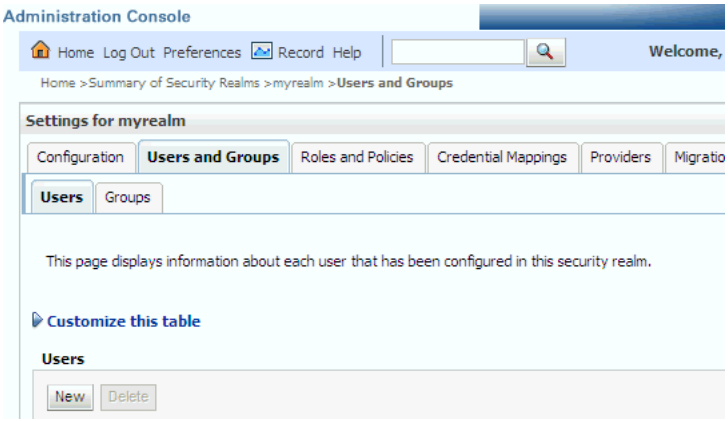
To create a new user in the embedded WebLogic LDAP server:

1. Log in to the Oracle WebLogic Server Administration Console.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

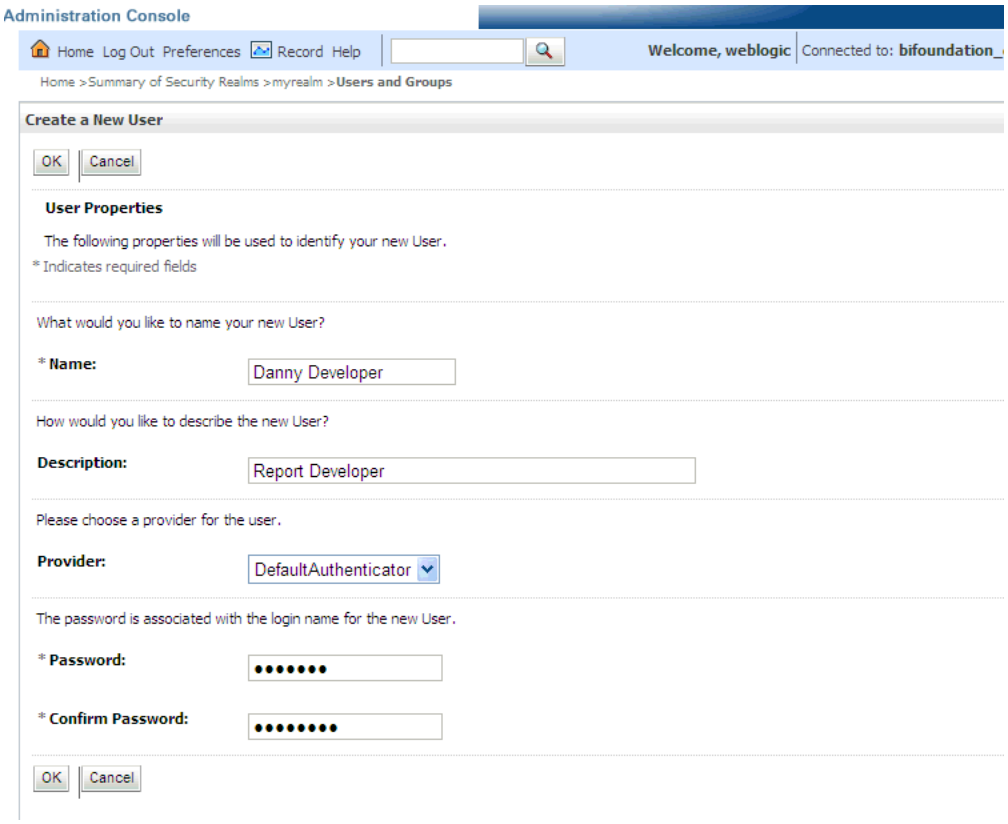
2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**.

3. Select **Users and Groups** tab, then **Users**. Click **New**.



4. In the **Create a New User** page provide the following information:

   - **Name**: Enter the name of the user. See the online help for a list of invalid characters.
   - (Optional) **Description**: Enter a description.
   - **Provider**: Select the authentication provider from the list that corresponds to the identity store where the user information is contained. DefaultAuthenticator is the name for the default authentication provider.
   - **Password**: Enter a password for the user that is at least 8 characters long.
   - **Confirm Password**: Re-enter the user password.



5. Click **OK**.

   The user name is added to the User table.

2.3.3 Creating a New Group in the Embedded WebLogic LDAP Server

You typically create a separate group for each functional type of business user in your Oracle Business Intelligence environment. For example, a typical deployment might require three groups: BIConsumers, BIContentAuthors, and BIServiceAdministrators. In this case, you could create groups named BIConsumers, BIContentAuthors, and BIServiceAdministrators that you can configure to use with Oracle Business Intelligence, or you might create your own custom groups.

> **Tip:** For an example security model showing a set of users, groups, and application roles, see Section 2.2, "An Example Security Setup of Users, Groups, and Application Roles".

Repeat this task for each new group that you want to deploy

To create a new group in the embedded WebLogic LDAP server:

1. Launch Oracle WebLogic Server Administration Console.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**.

3. Select **Users and Groups** tab, then **Groups**. Click **New**

4. In the **Create a New Group** page provide the following information:

- **Name**: Enter the name of the group. Group names are case insensitive but must be unique. See the online help for a list of invalid characters.
- (Optional) **Description**: Enter a description.
- **Provider**: Select the authentication provider from the list that corresponds to the identity store where the group information is contained. DefaultAuthenticator is the name for the default authentication provider.

5. Click **OK**

   The group name is added to the Group table.

2.3.4 Assigning a User to a Group in the Embedded WebLogic LDAP Server

You typically assign each user to an appropriate group. For example, a typical deployment might require user IDs created for report consumers to be assigned to a group named BIConsumers. In this case, you could either assign the users to the default group named BIConsumers, or you could assign the users to your own custom group that you have created.

> **Tip:** For an example security model showing a set of users, groups, and application roles, see Section 2.2, "An Example Security Setup of Users, Groups, and Application Roles".

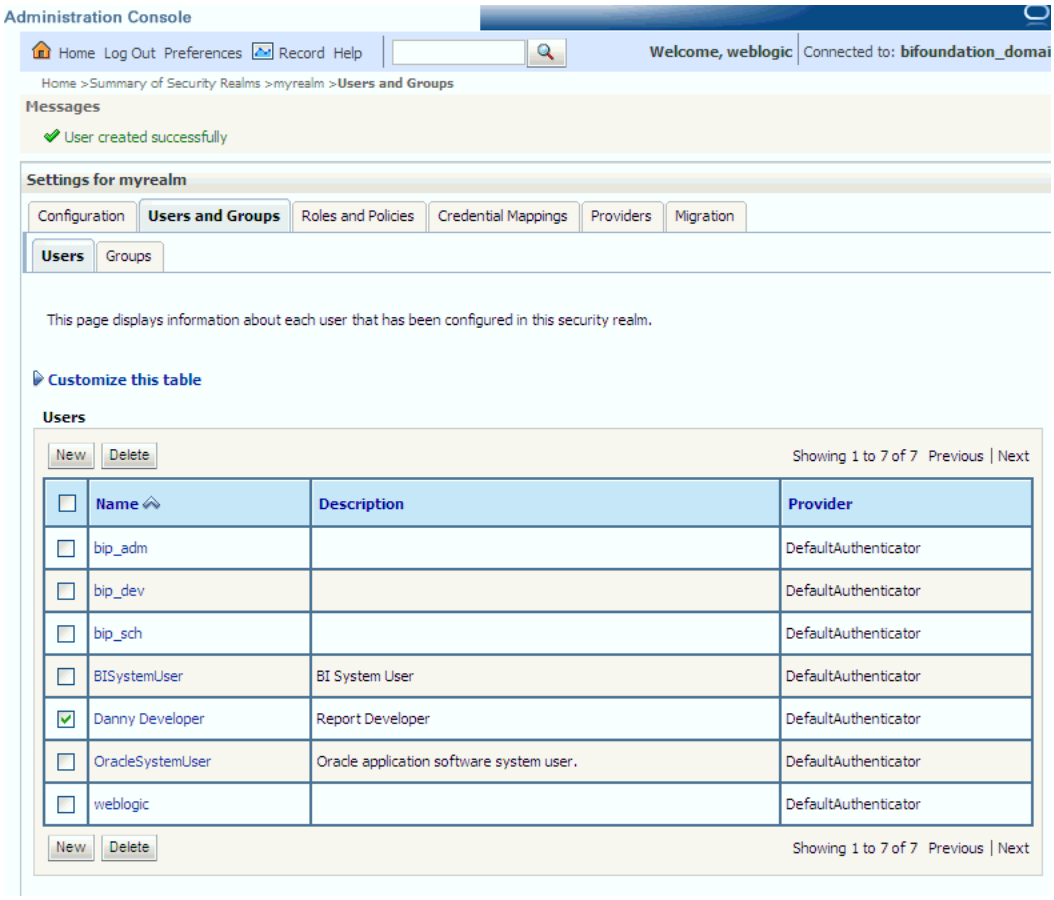
Repeat this task to assign each user to an appropriate group.

To add a user to a group in the embedded WebLogic LDAP server:

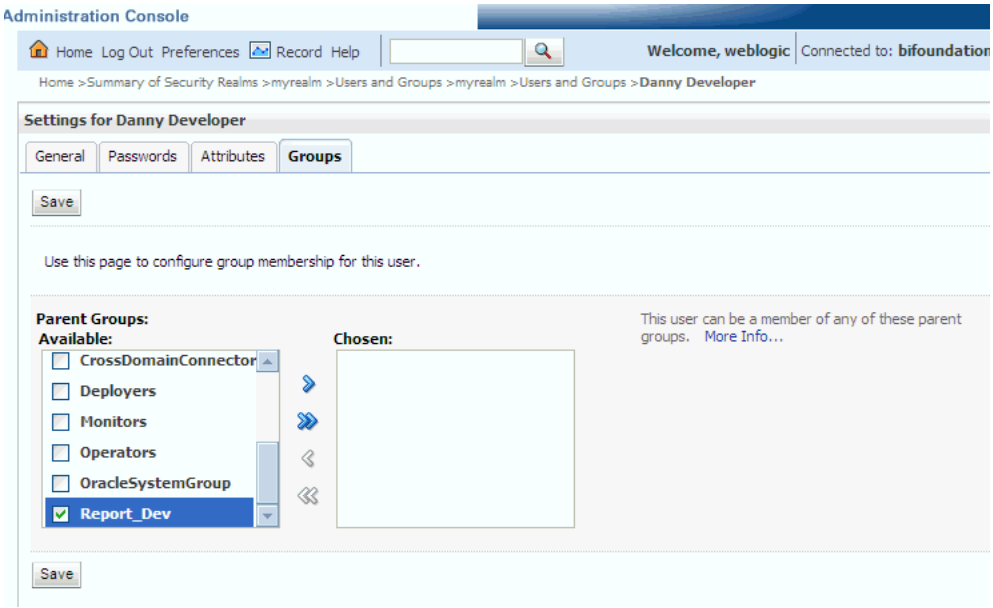
1. Launch Oracle WebLogic Server Administration Console.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**.
3. Select **Users and Groups** tab, then **Users**.
4. In the Users table select the user you want to add to a group.



5. Select the **Groups** tab.
6. Select a group or groups from the **Available** list box.



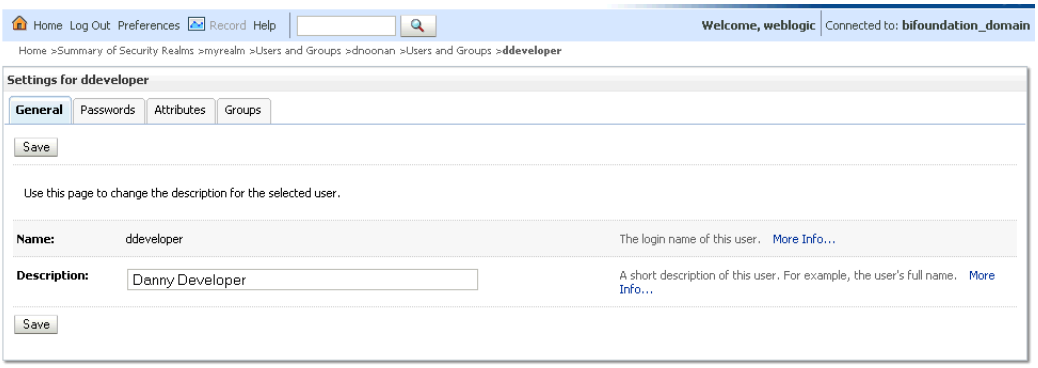
7. Click **Save**.

2.3.5 (Optional) Changing a User Password in the Embedded WebLogic LDAP Server

Perform this optional task if you want to change the default password for a user.

To change a user password in the embedded WebLogic LDAP server:

1. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**.
2. Select **Users and Groups** tab, then **Users**
3. In the Users table select the user you want to change the password for. The user's **Settings** page displays.



4. Select the **Passwords** tab and enter the password in the **New Password** and **Confirm Password** fields.
5. Click **Save**.

Note: If you change the password of the system user, you also need to change it in the credential store.

2.4 Managing Application Roles and Application Policies Using Fusion Middleware Control

In Oracle Business Intelligence, you use Fusion Middleware Control to manage application roles and application policies that provide permissions for users and groups. For detailed information about using Fusion Middleware Control, see *Oracle Fusion Middleware Administrator's Guide*.

- Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control"
- Section 2.4.2, "Creating and Deleting Application Roles Using Fusion Middleware Control"
- Section 2.4.3, "Creating Application Policies Using Fusion Middleware Control"
- Section 2.4.4, "Modifying Application Roles Using Fusion Middleware Control"

> **Tip:** After creating a new service instance or importing a BI application archive (BAR) file into a service instance, you should first check the security policy in the service instance to ensure that the users and groups from your Identity Store are mapped correctly to the application roles defined in the service instance. Each BI application archive file can contain its own security policy. Therefore it is good practice to check the security policy on your service instance after importing a BI application archive file..

Typically a BI application archive file that contains the BI metadata for an application will contain pre-defined application roles that can be used to provision users with permission to use BI functionality and access BI folders, analyses, subject areas etc. For example, the sample application contains the sample application roles BIConsumer, BIContentAuthor and BIServiceAdministrator. In order to provisin users with permissions and privileges, you map users and (where possible) groups from the Identity Store (usually an LDAP directory) to the defined application roles. You use Enterprise Manager Fusion Middleware Control or WLST to perform this task.

If you want to create a more complex or fine grained security model, you might create your own application roles and application policies as described in this section. For example, you might want report authors in a Marketing department to only have write-access to the Marketing area of the metadata repository and Oracle BI Presentation Catalog. To achieve this, you might create a new application role called BIContentMarketing, and provide it with appropriate privileges.

To set up the application roles that you want to deploy, do the following:

- If required, create new application roles. For more information, see Section 2.4.2, "Creating and Deleting Application Roles Using Fusion Middleware Control".

> **Note:** You can create application roles based on preconfigured Application policies, or you can create your own Application policies. For more information about the default users, groups, and application roles, see Section 2.1, "Working with Users, Groups, and Application Roles".

- If required, create new Application policies. For more information, see Section 2.4.3, "Creating Application Policies Using Fusion Middleware Control".
- (Optional) If required, modify the permission grants or membership for an application role. For more information, see Section 2.4.4, "Modifying Application Roles Using Fusion Middleware Control".

2.4.1 Displaying Application Policies and Application Roles Using Fusion Middleware Control

This section explains how to use Fusion Middleware Control to access the pages that manage application roles and application policies.

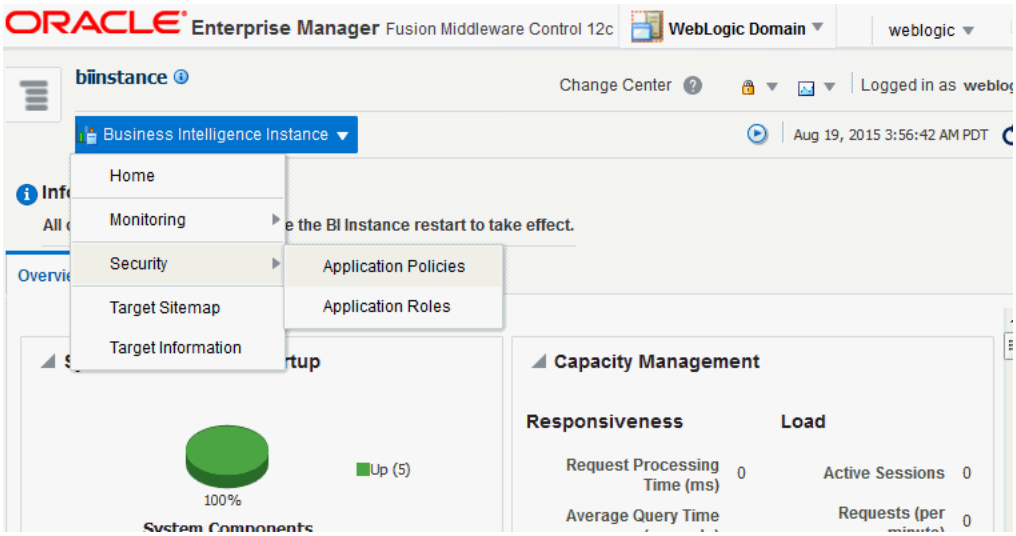
To display application policies and application roles using Fusion Middleware Control:

This method explains how to display **application policies** or **application roles** for Oracle Business Intelligence

1. Log in to Fusion Middleware Control.

For more information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".

2. Select the Target Navigation icon to open the navigation pane.
3. From the navigation pane expand the **Business Intelligence** folder and select **biinstance**.
4. Choose one of the following options:
   - Right-click **biinstance** and choose **Security** from the menu, then **Application Policies** or **Application Roles**.



   - Alternatively from the content pane, click **Business Intelligence Instance** to display a menu, then choose **Security**, and **Application Policies** or **Application Roles**.

     Other Fusion Middleware Control Security menu options are not available from these menus.

5. (Optional) An alternative option to Steps 3 and 4 is to expand the **WebLogic Domain** folder, right-click on the domain name (or click the **WebLogic Domain** menu).

   A **Security** menu displays with appropriate menu options.

   Other Fusion Middleware Control menu options are available from this menu.

6. Choose **Application Policies** or **Application Roles** to display either the Application Policies page or the Application Roles page.
   - If the `obi` application stripe is displayed by default

     Oracle Business Intelligence policies or roles are displayed.
   - If the `obi` application stripe is not displayed by default

     You must search using the `obi` application stripe to display Oracle Business Intelligence policies or roles.

   Figure 2–3 shows the **Application Policies** page.

Figure 2–3 Application Policies Page

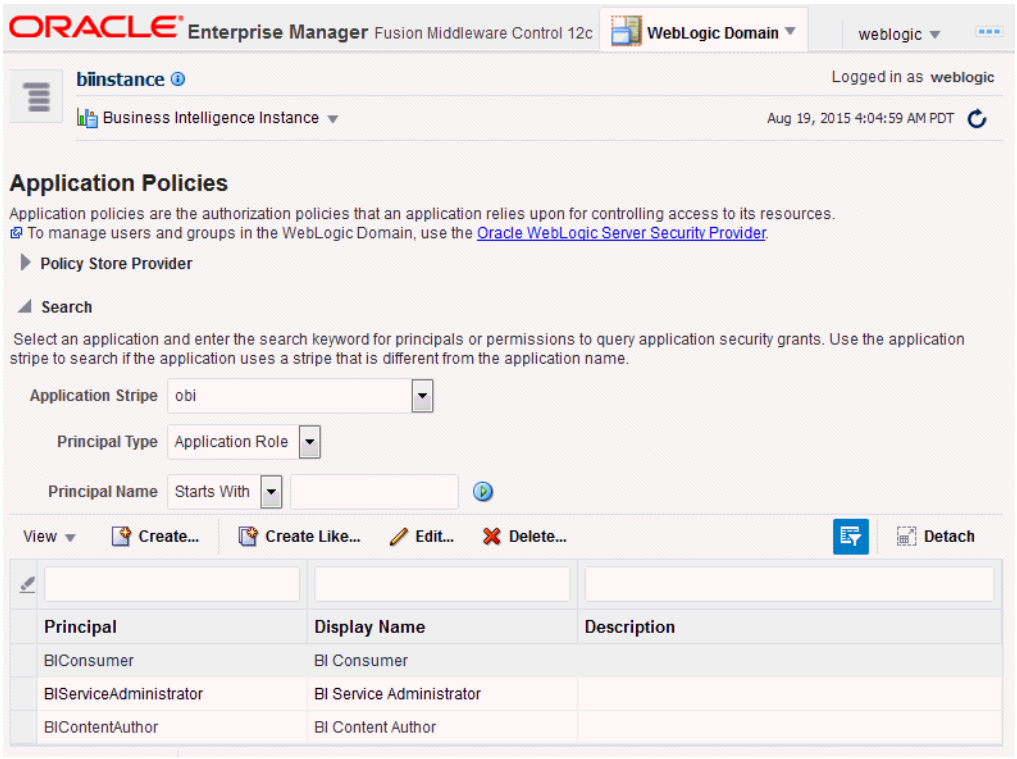
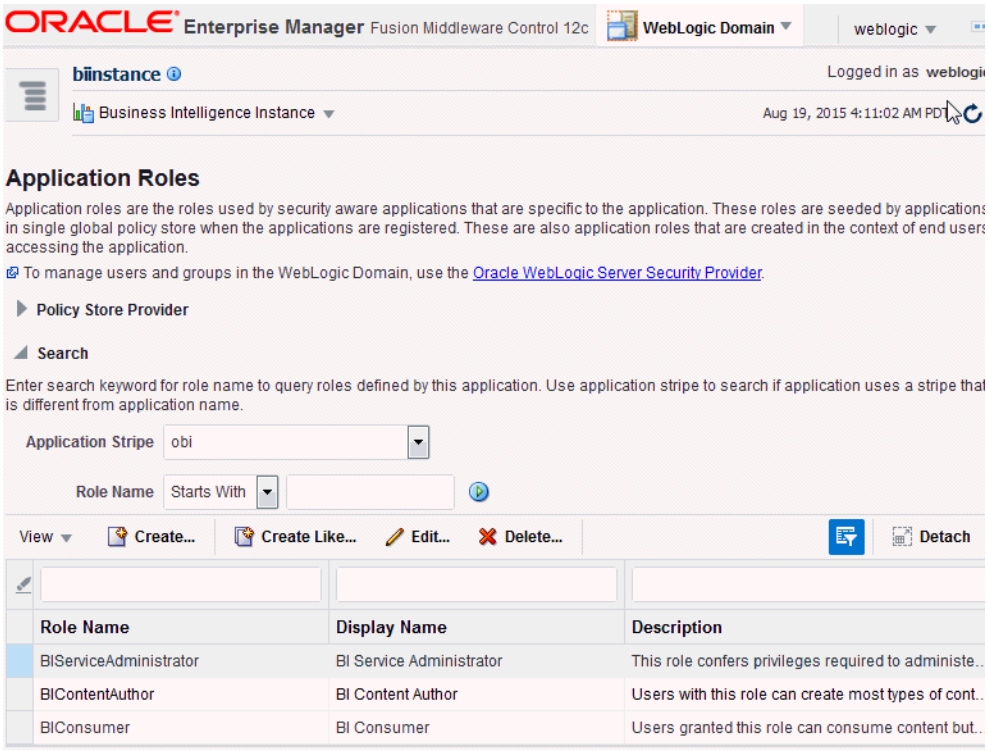


Figure 2–4 shows the **Application Roles** page.

Figure 2–4 Application Roles Page



2.4.2 Creating and Deleting Application Roles Using Fusion Middleware Control

This section explains how to create, delete, and manage application roles using Oracle Fusion Middleware Control, and contains the following topics:

- Section 2.4.2.1, "Overview"
- Section 2.4.2.2, "Creating an Application Role"
- Section 2.4.2.3, "Assigning a Group to an Application Role"
- Section 2.4.2.4, "Deleting an Application Role"

2.4.2.1 Overview

In a new Oracle Business Intelligence deployment, you typically create an application role for each type of business user activity in your Oracle Business Intelligence environment. For example, a typical deployment based on either the sample application or the starter application might include three application roles: BIConsumer, BIContentAuthor, and BIServiceAdministrator. As a BI system administrator or service administrator, you should not change the application roles or the permission sets assigned to the application roles that have been delivered in a BAR file.

Oracle Business Intelligence application roles represent a role that a user has. For example, having the Sales Analyst application role might grant a user access to view, edit and create reports on a company's sales pipeline. The administrator of a service instance can create and modify application roles in your service instance. Keeping application roles separate and distinct from the directory server groups enables you to better accommodate authorization requirements. You can create new application roles to match business roles for your environment without needing to change the groups defined in the corporate directory server. To control authorization requirements more efficiently, you can then assign existing groups of users from the directory server to application roles.

Note: Before creating a new application role and adding it to the your Oracle Business Intelligence service instance, familiarize yourself with how permission and group inheritance works. It is important when constructing a role hierarchy that circular dependencies are not introduced. For more information, see Section B.5, "Granting Permissions To Users Using Groups and Application Roles".

For more information about creating application roles, see "Managing the Policy Store" in *Oracle Fusion Middleware Application Security Guide*.

Note: For advanced-level information about using a BI repository in offline mode, see Section 2.5.3, "Managing Application Roles in the Metadata Repository - Advanced Security Configuration Topic".

2.4.2.2 Creating an Application Role

There are two methods for creating a new application role:

- **Create New** - Creates a new application role. You can add members at the same time or you can save the new role after naming it, and add members later.
- **Copy Existing** - Creates an application role by copying an existing application role. The copy contains the same members as the original, and is made a grantee of

the same application policy as is the original. Modifications can be made as needed to the copy to further customize the new application role.

Membership for an application role is controlled using the **Application Roles** page in Fusion Middleware Control. Valid members of an application role are users, groups, and other application roles.

Permission and permission set grants are controlled in the **Application Policies** page in Fusion Middleware Control. The permission and permission set grant definitions are set in the application policy, then the application policy is *granted* to the application role. For more information, see Section 2.4.3, "Creating Application Policies Using Fusion Middleware Control".

To create a new application role:

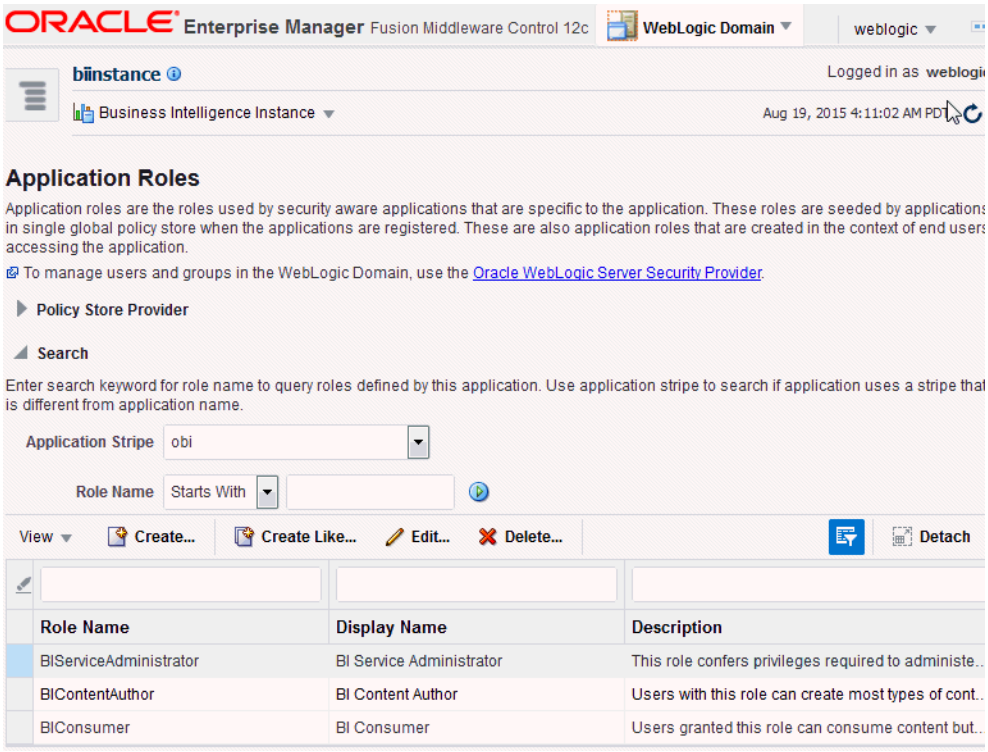
1. Log in to Fusion Middleware Control, and display the **Application Roles** page.

   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

2. Ensure the **Application Stripe** is **obi**, and click the search icon next to **Role Name**.

   The Oracle Business Intelligence application roles display. Figure 2–5 shows some application roles.

Figure 2–5 Application Roles in Fusion Middleware Control



3. Click **Create** to display the **Create Application Role** page. You can enter all information at once or you can enter a **Role Name**, save it, and complete the remaining fields later. Complete the fields as follows:

   In the **General** section:

- **Role Name** - Enter the name of the application role avoiding any invalid characters including spaces (see "Characters in Application Role Names" in *Oracle Fusion Middleware Application Security Guide*).
- (Optional) **Display Name** - Enter the display name for the application role.
- (Optional) **Description** - Enter a description for the application role.

4. In the **Members** section, click **Add** to display the **Add Principal** page.
5. In the **Add Principal** page search for members to assign to the current application role, as follows:
   - Select Application Role, Group, or Users from the **Type** field drop down list.
   - Optionally enter search details into **Principal Name** and **Display Name** fields.
   - Click the search button.
   - Select from the results returned in the **Searched Principals** box.
   - Click **OK** to return to the **Create Application Role** page.
   - Repeat the steps until all desired members are added to the application role.
6. Click **OK** to return to the **Application Roles** page.

   The application role just created displays in the table at the bottom of the page.

To create an application role based on an existing one:

1. Log in to Fusion Middleware Control, and display the **Application Roles** page.

   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

   Whether or not the obi application stripe is pre-selected and the application policies are displayed depends upon the method used to navigate to the **Application Roles** page.
2. If necessary select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.

   The Oracle Business Intelligence application roles display.
3. Select the application role you want to copy from the list to enable the action buttons.
4. Click **Create Like** to display the **Create Application Role Like** page.

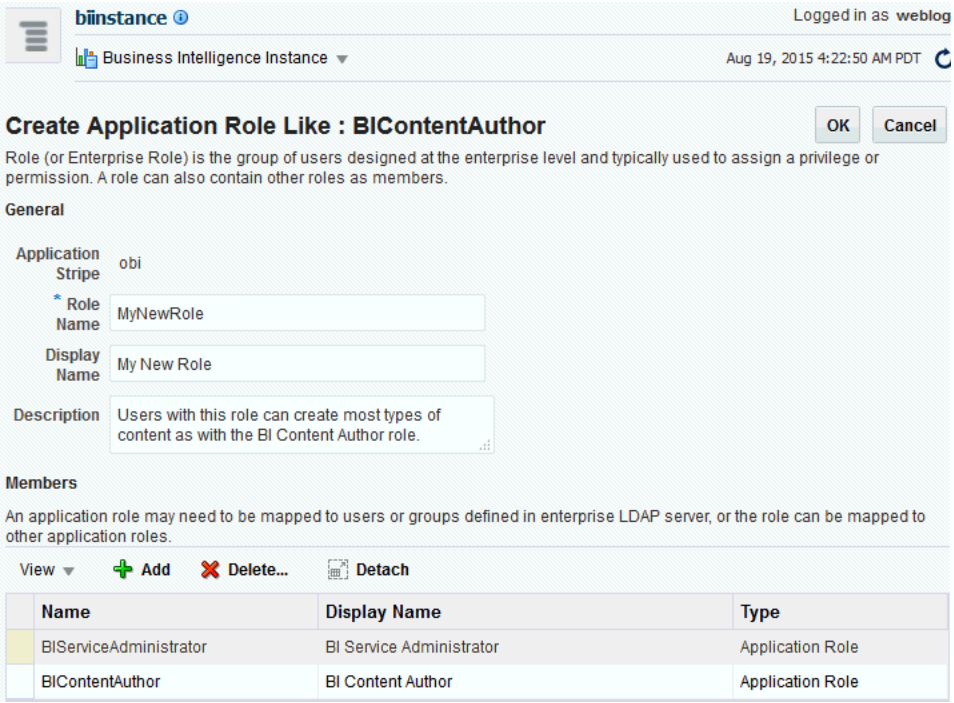
   The **Members** section displays the same application roles, groups, or users that are assigned to the original role. Complete the fields as follows:

   In the **General** section:
   - **Role Name** - Enter the name of the application role avoiding any invalid characters including spaces (see "Characters in Application Role Names" in *Oracle Fusion Middleware Application Security Guide*).
   - (Optional) **Display Name** - Enter the display name for the application role.
   - (Optional) **Description** - Enter a description for the application role.
5. In the **Members** section, click **Add** to display the **Add Principal** page.
6. In the **Add Principal** page you search for members to assign to the current application role, as follows:
   - Select Application Role, Group, or Users from the **Type** field drop down list.

- Optionally enter search details into **Principal Name** and **Display Name** fields.
- Click the search button.
- Select from the results returned in the **Searched Principals** box.
- Click **OK** to return to the **Create Application Role** page.
- Repeat the steps until all desired members are added to the application role.

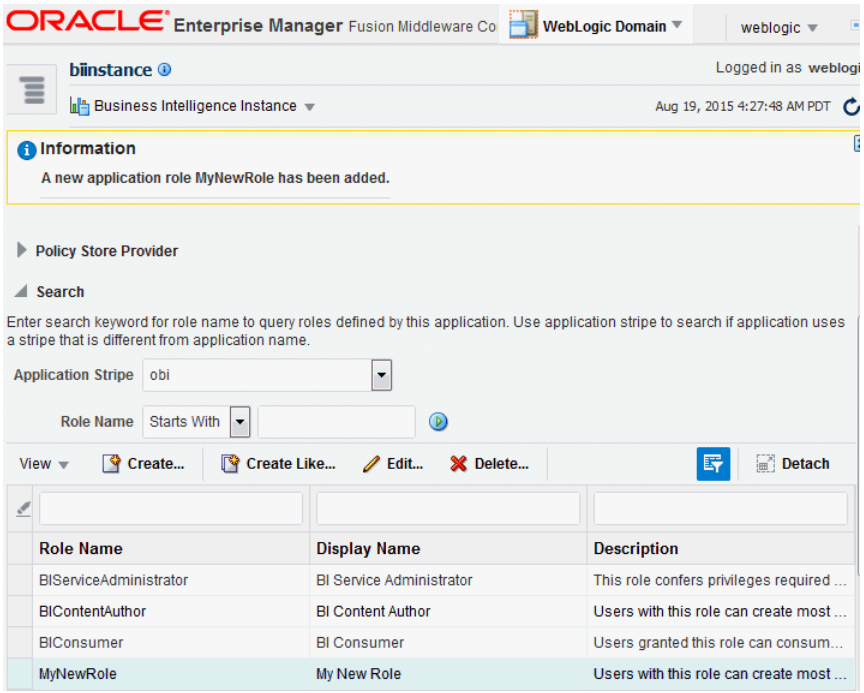
Figure 2–6 shows creation of the new application role **MyNewRole**, based upon the BIContentAuthor application role.

Figure 2–6 New Application Role Based on Existing Role



The newly-created application role displays in the table at the bottom of the page. Figure 2–7 shows the newly-created application role named **MyNewRole** based upon an existing application role.

Figure 2–7 Newly Created Application Role



7. Modify the members as appropriate and click **OK**.

2.4.2.3 Assigning a Group to an Application Role

You assign a group to an application role to provide users in that group with appropriate security privileges. For example, a group for marketing report consumers named BIMarketingGroup might require an application role called BIConsumerMarketing, in which case you assign the group named BIMarketingGroup to the application role named BIConsumerMarketing.

To assign a group to an application role:

1. Log in to Fusion Middleware Control, and display the **Application Roles** page.

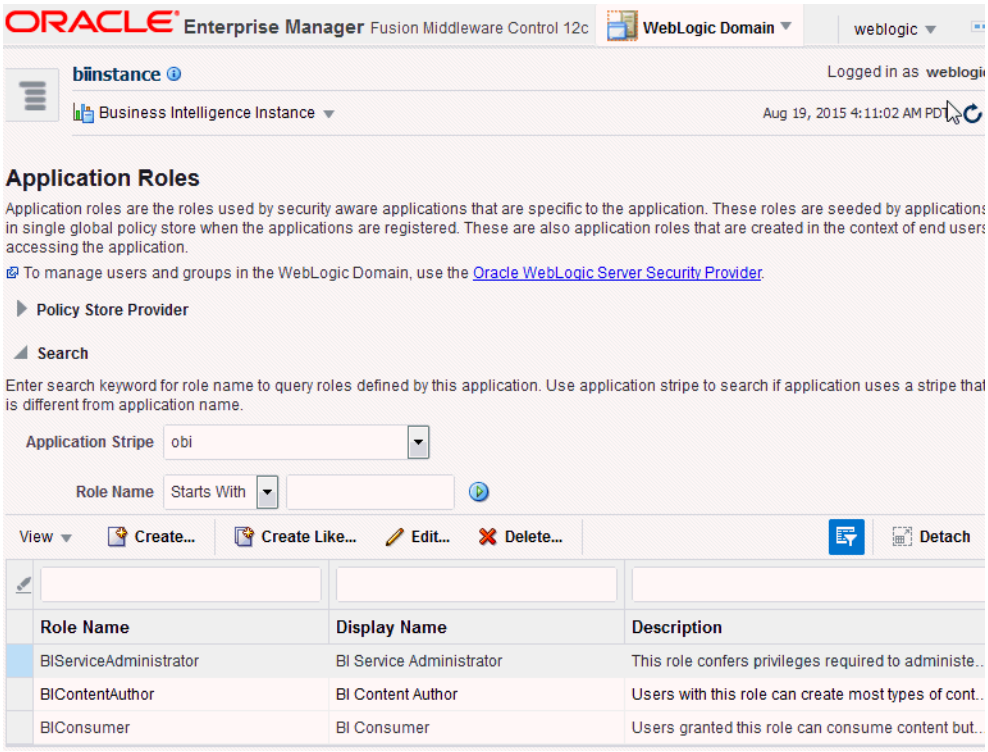
   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

   Whether or not the obi application stripe is pre-selected and the application policies are displayed depends upon the method used to navigate to the **Application Roles** page.

2. If necessary, select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.

   The Oracle Business Intelligence application roles display. Figure 2–8 shows the current application roles.

Figure 2–8 Application Roles Page



3. Select an application role in the list and click **Edit** to display the **Edit Application Role** dialog, and complete the fields as follows:

   In the **General** section:

   - **Role Name** - The name of the application role, this field is read only.
   - **Display Name** - The display name for the application role.
   - **Description** - A description for the application role.

4. In the **Members** section, click **Add** to add the group that you want to assign to the **Roles** list.

   For example, if a group for marketing report consumers named BIMarketingGroup require an application role called BIConsumerMarketing, then add the group named BIMarketingGroup to **Roles** list.

5. Click **OK** to return to the **Application Roles** page.

2.4.2.4 Deleting an Application Role

You must not delete an application role without first consulting your system administrator.

To delete an application role:

1. Log in to Fusion Middleware Control, and display the **Application Roles** page.

   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

2. Select the application role you want to delete.

3. Click **Delete**, then click **Yes**, to confirm deletion of the application role.

2.4.3 Creating Application Policies Using Fusion Middleware Control

You can create application roles based on the default application policies, or you can create your own application policies.

Application policies do not apply privileges to the metadata repository or Oracle BI Presentation Catalog objects and functionality.

All Oracle Business Intelligence permissions and permission sets are provided as part of the installation and you cannot create new permissions. The application policy is the mechanism that defines the permission set and permissions grants. Permission set and permissions grants are controlled in the Fusion Middleware Control **Application Policies** page. The permission set and permission grants are defined in an application policy. An application role, user, or group, is then assigned to an application policy. This process makes the application role a **grantee** of the application policy.

There are two methods for creating a new application policy:

- **Create New** - Create a new application policy and permissions are added to it.
- **Copy Existing** - Create new application policy by copying an existing application policy. The copy is named and existing permissions are removed or permissions are added.

Note: Oracle Business Intelligence 12*c* makes use of permission sets as well as permissions. A permission set is a collection of permissions. It is also known as an entitlement. All of the permissions available with BI 12*c* are grouped into permission sets. When the either the sample or starter application is imported into a service instance you will see the permission sets that have been assigned to the application roles. When an 11*g* upgrade bundle is imported into a service instance you will see the permissions from your 11*g* system, supplemented by new permission sets assigned to the migrated application roles

---

Note: Fusion Middleware Control only allows you to view permission set grants. It does not allow you to change the permission set grants against an application role. Fusion Middleware Control does allow you to modify permission grants against application roles. In 12*c*, if you need to update permission set grants against an application role you need to use the WLST command line (see "Managing Application Policies with WLST Commands" in *Oracle Fusion Middleware Application Security Guide*.

For more information about creating application policies, see "Managing Policies with Fusion Middleware Control" in *Oracle Fusion Middleware Application Security Guide*.

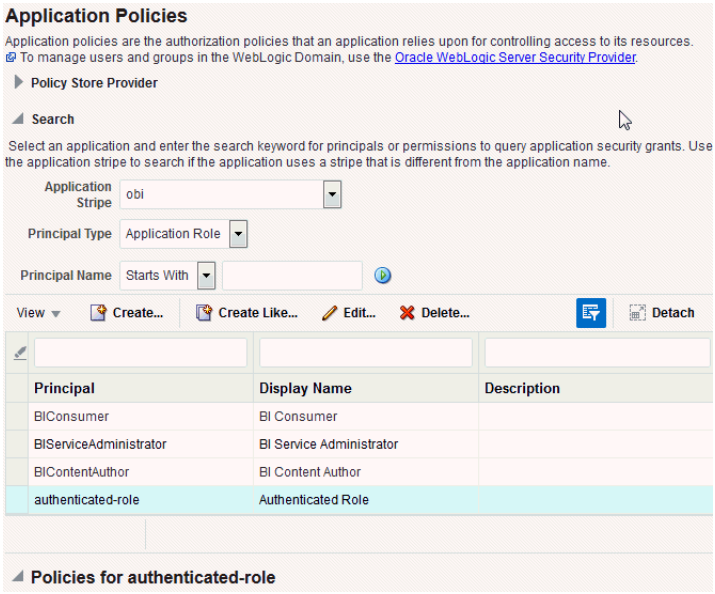
To create a new application policy:

1. Log in to Fusion Middleware Control, and display the **Application Policies** page.

   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

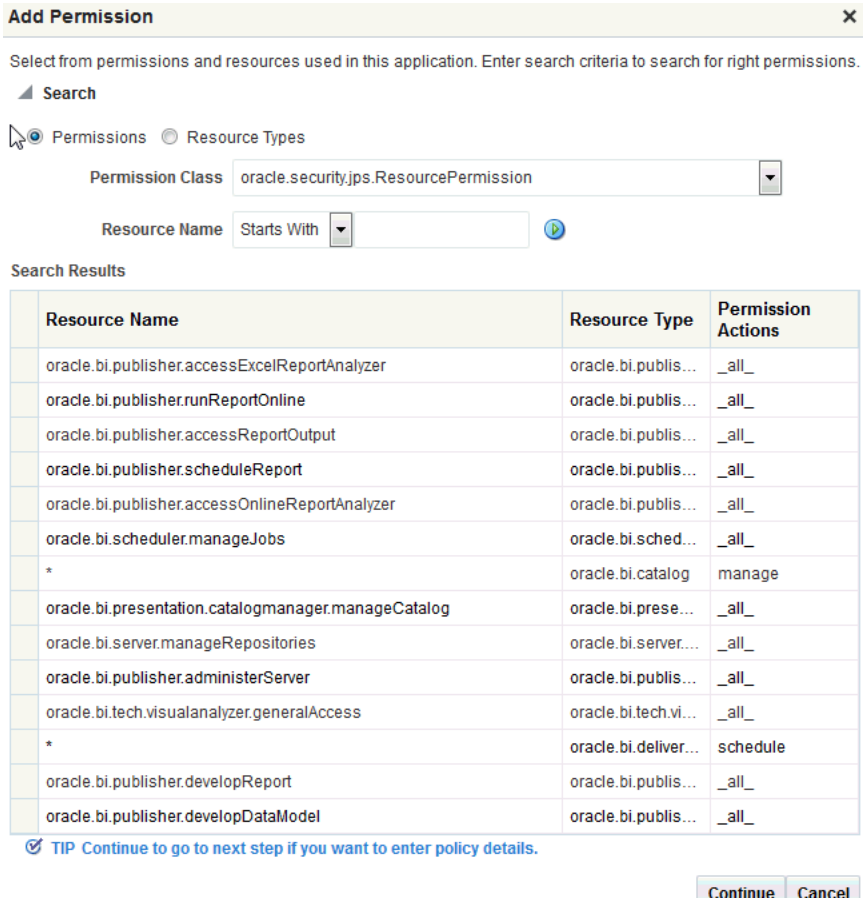
2. Select the **obi** from the **Application Stripe** list, then click the search icon next to **Name**.

   The Oracle Business Intelligence application policies are displayed. The **Principal** column displays the name of the policy grantee.



3. Click **Create** to display the **Create Application Grant** page.
4. To add permissions to the policy being created, click **Add** in the **Permissions** area to display the **Add Permission** dialog.
   - Complete the **Search** area and click the blue search button next to the **Resource Name** field.

     All permissions for the selected class are displayed.



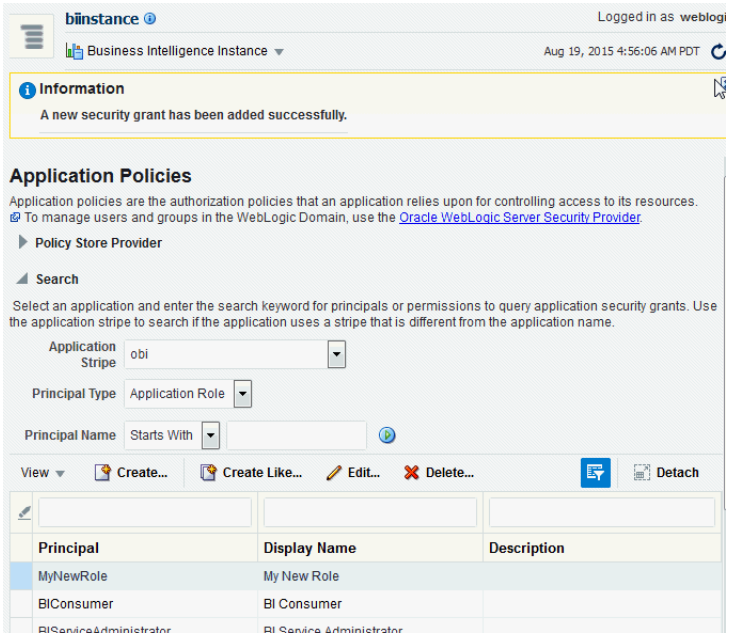
- Select the desired Oracle Business Intelligencer permission and click **Continue**.
- Modify permission details if required in the **Customize** page, then click **Select** to add the permission.

  You are returned to the **Create Application Grant** page. The selected permissions display in the **Permissions** area.
- Repeat until all desired permissions are selected.

  Selecting non-Oracle Business Intelligence permissions have no effect in the policy.
- To remove a permission, select it and click **Delete**.

5. To add an application role, group, or user to the policy being created, click **Add** in the **Grantee** area to display the **Add Principal** page.
   - Complete the **Search** area and click the blue search button next to the **Display Name** field.
   - Select a principal from the **Searched Principals** list.
   - Click **OK** to display the **Create Application Grant** page.
   - Click **OK**.

   You are returned to the **Application Policies** page. The Principal and Permissions of the policy created are displayed in the tables. The following figure shows the new application policy just created with MyNewRole application role as the grantee (**Principal**).



To create an application policy based on an existing one:

1. Log in to Fusion Middleware Control, and display the **Application Policies** page.

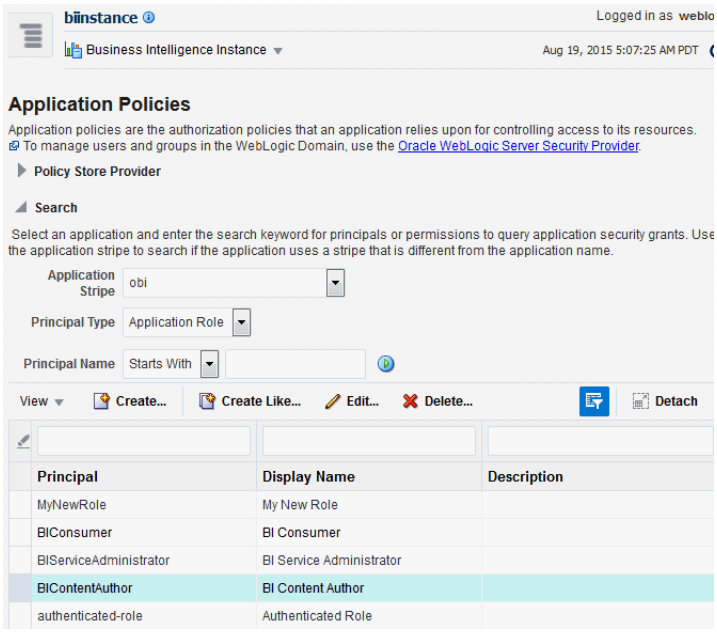
   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

2. Select **obi** from the **Application Stripe** list, then click the search icon next to **Name**.

   The Oracle Business Intelligence application policies are displayed. The **Principal** column displays the name of the policy grantee.

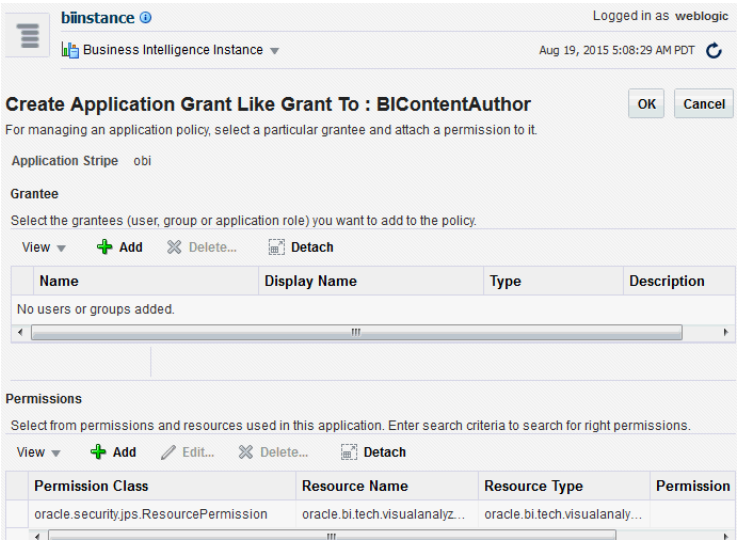
3. Select an existing policy from the table.

   The following figure shows the **BIContentAuthor** Principal selected with the **Create Like** button activated, which is used as an example in this procedure.



4. Click **Create Like** to display the **Create Application Grant Like** page. The Permissions table automatically displays permissions granted by the policy selected.

   The following figure shows the **Create Application Grant Like** dialog after the BIContentAuthor policy has been selected. Note that the **Permissions** section displays the permission grants for the BIContentAuthor policy.

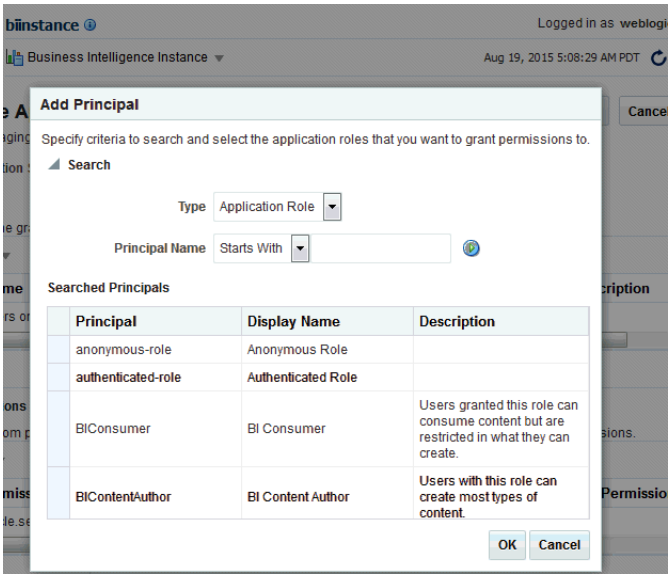


5. To remove any items, select it and click **Delete**.

6. To add application roles to the policy, click **Add Application Role** in the **Grantee** area to display the **Add Application Role** dialog.

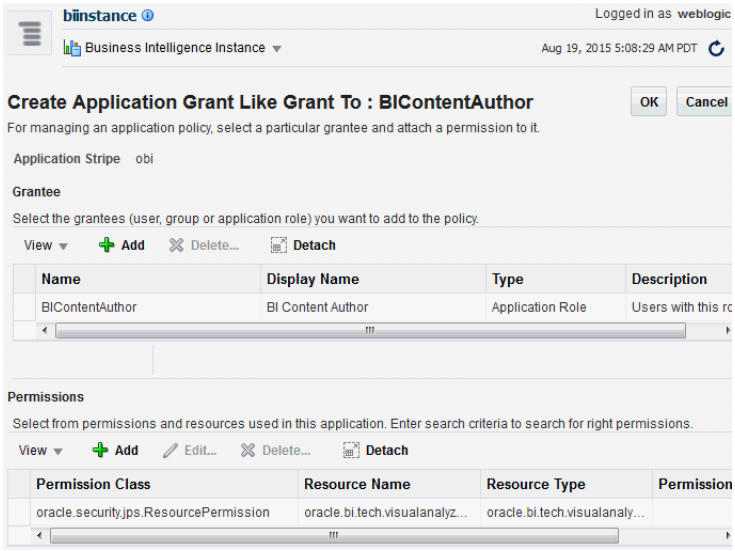
   The following figures use the **MyNewRole** application role as an example.

   - Complete the **Search** area and click the blue search button next to the **Display Name** field. The application roles matching the search are displayed.



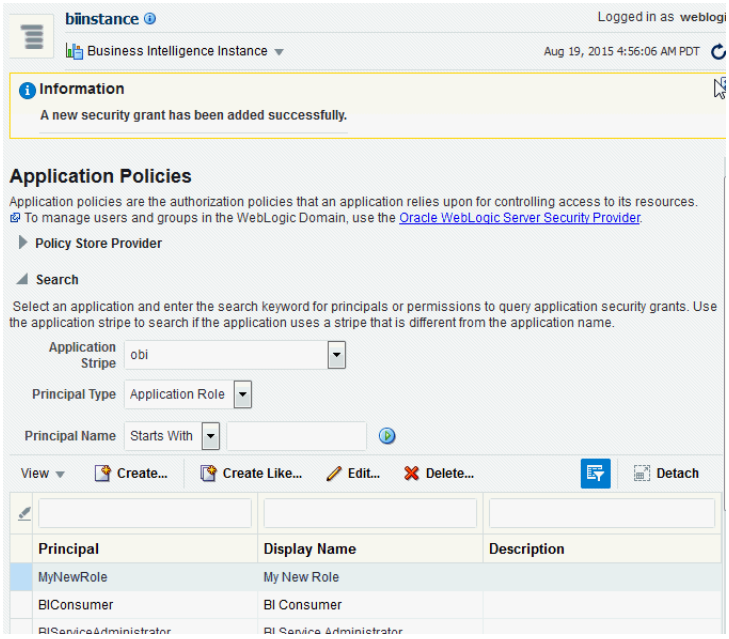
   - Select from the **Searched Principals** list and click **OK**.

     The **Create Application Grant Like** page displays with the selected application role added as **Grantee**.



- Click **OK** to return to the **Application Policies** page.

  The Principal and Permissions of the application policy just created are displayed in the table.



2.4.4 Modifying Application Roles Using Fusion Middleware Control

You can modify an application role by changing permission grants of the corresponding application policy (if the application role is a grantee of the application policy), or by changing its members, and by renaming or deleting the application role as follows:

- Section 2.4.4.1, "Adding or Removing Permission Grants from an Application Role"
- Section 2.4.4.2, "Adding or Removing Members from an Application Role"
- Section 2.4.4.3, "Renaming an Application Role"

For more information about managing application policies and application roles, see "Managing Policies with Fusion Middleware Control" in *Oracle Fusion Middleware Application Security Guide*.

2.4.4.1 Adding or Removing Permission Grants from an Application Role

Use this procedure if you want to change the permission grants for an application role. This is done by adding or removing the permission grants for the application policy which the application role is a grantee of.

To add or remove permission grants from an application policy:

1. Log in to Fusion Middleware Control, and display the **Application Policies** page.

   For more information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

   Whether or not the **obi** stripe is pre-selected and the application policies are displayed depends upon the method used to navigate to the **Application Policies** page.

2. If necessary, select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.

   The Oracle Business Intelligence application policies are displayed. The **Principal** column displays the name of the policy **grantee**.

3. Select the application role from the Principal column and click **Edit**.

4. Add or delete permissions from the **Edit Application Grant** view and click **OK** to save the changes.

2.4.4.2 Adding or Removing Members from an Application Role

Members can be added to or deleted from an application role using Fusion Middleware Control. You must perform these tasks in the WebLogic Domain where Oracle Business Intelligence is installed (for example, in bifoundation_domain). Valid members of an application role are users, groups, or other application roles. Being assigned to an application role is to become a member of an application role. Best practice is to assign groups instead of individual users to application roles.

Note: Be very careful when changing the permission grants and membership for the application role that is tagged as the administration application role, as changes to the permissions assigned to this application role could leave your system in an unusable state.

To add or remove members from an application role:

1. Log in to Fusion Middleware Control, and display the **Application Roles** page.

   For information, see Section 2.4.1, "Displaying Application Policies and Application Roles Using Fusion Middleware Control".

2. If not already displayed, select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.

   The Oracle Business Intelligence application roles are displayed.

3. Select the cell next to the application role name and click **Edit** to display the **Edit Application Role** page.

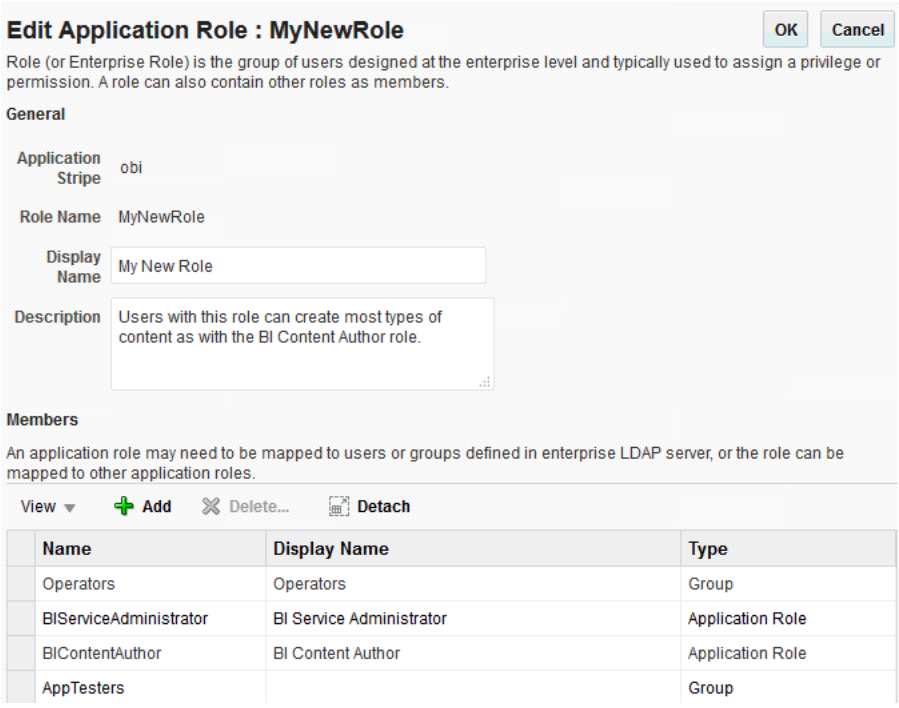
You can add or delete members from the **Edit Application Role** page. Valid members are application roles, groups, and users.

4. To delete a member, select the **Name** of the member to activate the **Delete** button, then click **Delete**.
5. To add a member click the **Add** button to display the **Add Principal** page.

   Search for members to assign to the current application role, as follows:

   - Select Application Role, Group, or Users from the **Type** field drop down list.
   - Optionally enter search details into **Principal Name** and **Display Name** fields.
   - Click the search button.
   - Select from the results returned in the **Searched Principals** box.
   - Click **OK** to return to the **Create Application Role** page.
   - Repeat the steps until all desired members are added to the application role.

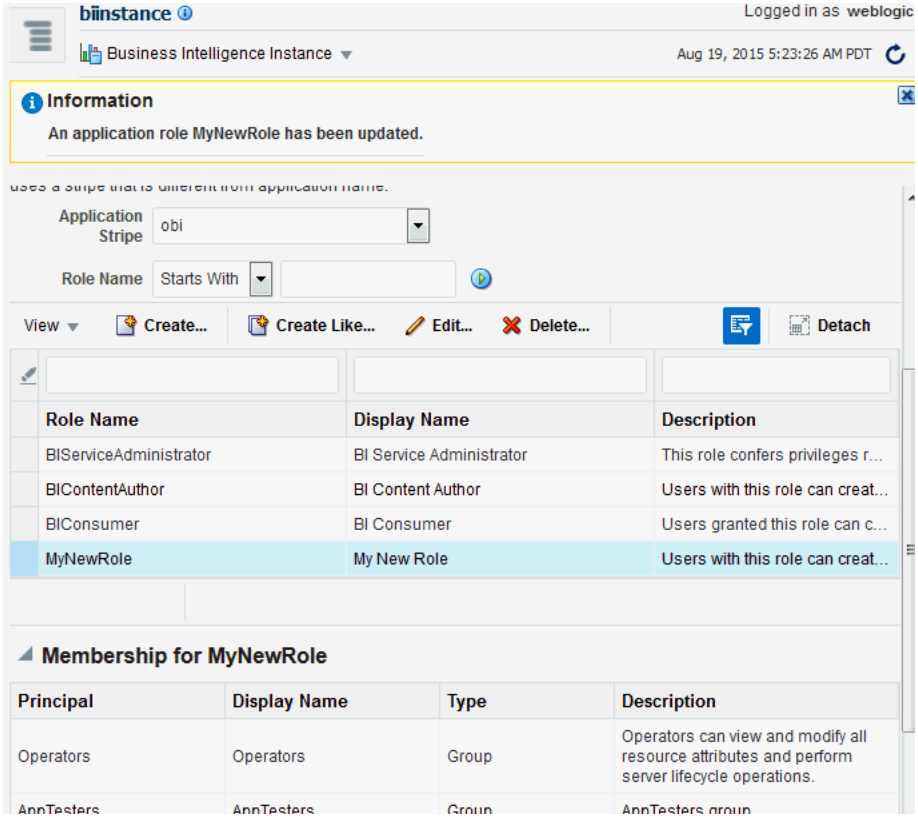
     The added member displays in the **Members** section corresponding to the application role modified in the **Application Roles** page. For example, the following figure shows the **Edit Application Role** page for the **MyNewRole** application role after the **Operators** group has been added.



6. Click **OK** in the **Edit Application Role** page to return to the **Application Roles** page.

   The members just added to the application role display in the **Membership for** section. If members were deleted, they no longer display.

   The following figure shows the **MyNewRole** application role with the recently added member **Operators** group displaying.



For additional information, see "Managing Application Roles" in *Oracle Fusion Middleware Application Security Guide*.

2.4.4.3 Renaming an Application Role

You cannot directly rename an existing application role; you can only update the display name. To rename an application role you must create a new application role (using the same application policies used for the deleted application role), and delete the old application role. When you create the new application role, you specify a new name. You must also update any references to the old application role with references to the new application role in both the Oracle BI Presentation Catalog and the metadata repository.

To rename an application role in the catalog and the metadata repository use the renameAppRoles command, as described in "Rename Application Role Command" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

2.5 Managing Metadata Repository Privileges Using the Oracle BI Administration Tool

This section explains how to use the Oracle BI Administration Tool to configure security in the Oracle BI repository, and contains the following topics:

- Section 2.5.1, "Overview"
- Section 2.5.2, "Setting Repository Privileges for an Application Role"
- Section 2.5.3, "Managing Application Roles in the Metadata Repository - Advanced Security Configuration Topic"

2.5.1 Overview

You use Identity Manager in the Oracle BI Administration Tool to manage permissions for application roles, and set access privileges for objects such as subject areas and tables. For an overview about using the Oracle BI Administration Tool to configure security, see Section 1.6.3, "Using Oracle BI Administration Tool".

> **Note:** Oracle Business Intelligence Applications customers should read this section to understand the basics about security and setting up authentication, and then refer to the security and configuration information provided in *Oracle Fusion Middleware Reference Guide for Oracle Business Intelligence Applications*.

2.5.2 Setting Repository Privileges for an Application Role

The data model for your service instance includes a security policy to define permissions for accessing different parts of the data model such as data columns and subject areas. The author of your data model uses the administration tool to maintain this security policy including assigning data model permissions to application roles. When you create a service instance or import a BI application archive file into a service instance, the security policy for the data model is imported from the BI application archive file.

> **Note:** In addition to setting repository privileges, you might assign Oracle BI Presentation Catalog privileges to a new application role. For more information, see Section 2.6.3, "Setting Presentation Services Privileges for Application Roles".

> **Note:** You can also set repository permissions programmatically using command line tools. For more information, see "Setting Permissions Using Command-Line Tools" in *Oracle Fusion Middleware XML Schema Reference for Oracle Business Intelligence Enterprise Edition*.

To set repository permissions for an application role:

1. Open the repository in the Oracle BI Administration Tool (in Online mode).

   For more information, see Section 1.6.3, "Using Oracle BI Administration Tool".

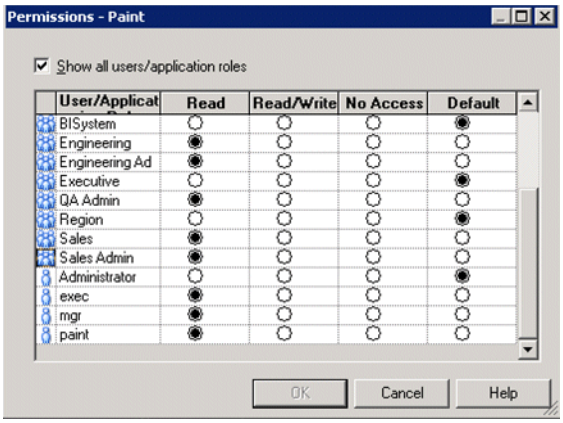
2. In the Presentation panel, navigate to the subject area or sub-folder for which you want to set permissions.

3. Right-click the subject area or sub-folder and select **Properties** to display the properties dialog.

   For example, to provide access to the Paint subject area, right-click **Paint**.

4. Click **Permissions** to display the Permissions <*Name*> dialog.

   > **Note:** Ensure that the **Show all users/application roles** check box is selected.



5. Use the Permissions <*Name*> dialog to change the security permissions for application roles in the **User/Application Role** list.

   For example, to enable users to create dashboards and reports, you might change the repository permissions for an application role named BISalesAnalysis from 'Read' to 'Read/Write'.

   Note: Best practice is to modify permissions for application roles, not modify permissions for individual users.

   To see all permissions for an object in the Presentation pane, right-click the object and choose **Permission Report** to display a list of users and application roles and what permissions that have for the selected object.

2.5.3 Managing Application Roles in the Metadata Repository - Advanced Security Configuration Topic

Application role definitions are maintained in the policy store and any changes must be made using the administrative interface. The repository maintains a *copy* of the policy store data to facilitate repository development. The Oracle BI Administration Tool displays application role data from the repository's copy; you are not viewing the policy store data in real time. Policy store changes made while you are working with an offline repository are not available in the Administration Tool until the policy store next synchronizes with the repository. The policy store synchronizes data with the repository copy whenever the BI Server restarts; if a mismatch in data is found, an error message is displayed.

While working with a repository in offline mode, you might discover that the available application roles do not satisfy the membership or permission grants needed at the time. A *placeholder for an Application Role* definition can be created in the Administration Tool to facilitate offline repository development. But this is just a placeholder visible in the Administration Tool and is not an actual application role. You cannot create an actual application role in the Administration Tool. You can create an application role only in the policy store, using the administrative interface available for managing the policy store.

An application role must be defined in the policy store for each application role placeholder created using the Administration Tool *before* bringing the repository back online. If a repository with role placeholders created while in offline mode is brought online before valid application roles are created in the policy store, then the application role placeholder disappears from the Administration Tool interface.

Always create a corresponding application role in the policy store before bringing the repository back online when using role placeholders in offline repository development.

For more information about how to create a placeholder for an application role during repository development, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

2.6 Managing Presentation Services Privileges Using Application Roles

This section explains how to manage Presentation Services privileges using application roles in Presentation Services Administration Manage Privileges page, and contains the following topics:

- Section 2.6.1, "Overview"
- Section 2.6.2, "About Presentation Services Privileges"
- Section 2.6.3, "Setting Presentation Services Privileges for Application Roles"
- Section 2.6.4, "Encrypting Credentials in BI Presentation Services - Advanced Security Configuration Topic"

2.6.1 Overview

The catalog for your service instance includes security policy for Presentation Service privileges. These privileges confer permissions for accessing specific Presentation Services functionality such as access to answers, access to dashboards as well as permissions on catalog objects such as folders and analyses. When you create a service instance or import a BI application archive file into a service instance, the security policy for the catalog (Presentation Services Privileges) is imported from the BI application archive file. The service administrator can modify the catalog security policy.

Systems upgraded from a previous release can continue to use Catalog groups to grant these privileges, but this is not considered a best practice (see Section D.2.2.1, "Migrating Catalog Groups to Application Roles"). Best practice is to use application roles to manage privileges, which streamlines the security management process. For example, using the same set of application roles throughout the system eliminates the need to manage a separate set of Catalog groups and member lists. For more information regarding how to continue using upgraded Catalog groups to manage Presentation Services privileges, see Section A.2.1, "Changes Affecting Security in Presentation Services".

Note: Assigning an application role to be a member of a Catalog group creates complex group inheritance and maintenance situations and is not considered a best practice.

When groups are assigned to application roles, the group members are automatically granted associated privileges in Presentation Services. This is in addition to the Oracle Business Intelligence permissions.

Tip: A list of application roles that a user is a member of is available from the **Roles and Groups** tab in the **My Account** dialog in Presentation Services.

2.6.2 About Presentation Services Privileges

Presentation Services privileges are maintained in the Presentation Services Administration Manage Privileges page, and they grant or deny access to Presentation Services features, such as the creation of analyses and dashboards. Presentation Services privileges have no effect in other Oracle Business Intelligence components.

Being a member of an application role that has been assigned Presentation Services privileges will grant those privileges to the user. The Presentation Services privileges assigned to application roles can be modified by adding or removing privilege grants using the **Manage Privileges** page in Presentation Services Administration.

Presentation Services privileges can be granted to users both explicitly and by inheritance. However, explicitly *denying* a Presentation Services privilege takes precedence over user access rights either granted or inherited as a result of group or application role hierarchy.

2.6.3 Setting Presentation Services Privileges for Application Roles

If you create an application role, you must set appropriate Presentation Services privileges to enable users with the application role to perform various functional tasks. For example, you might want users with an application role named BISalesAdministrator to be able to create Actions in Oracle Business Intelligence. In this case, you would grant them a privilege named Create Invoke Action.

Presentation Services privileges cannot be assigned using the administrative interfaces used to manage the policy store. If you create a new application role to grant Oracle Business Intelligence permissions, then you must set Presentation Services privileges for the new role in addition to any Oracle Business Intelligence permissions.

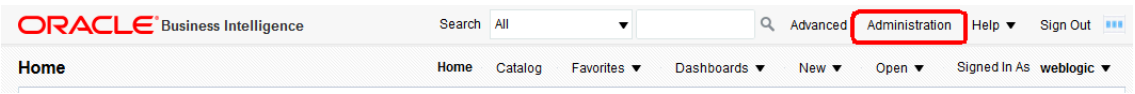
Note: Presentation Services privileges can be assigned to a new application role programmatically using SecurityService Service. For more information, see "SecurityService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

To set Presentation Services privileges for an application role:

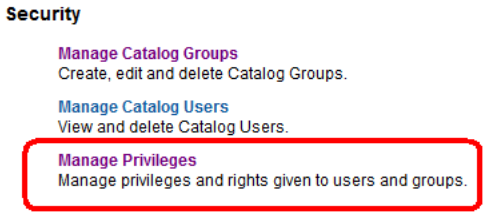
1. Log in to Oracle BI Presentation Services as a user with Administrator privileges.

   For more information, see Section 1.6.4, "Using Presentation Services Administration".

2. From the Home page in Presentation Services, select **Administration**.

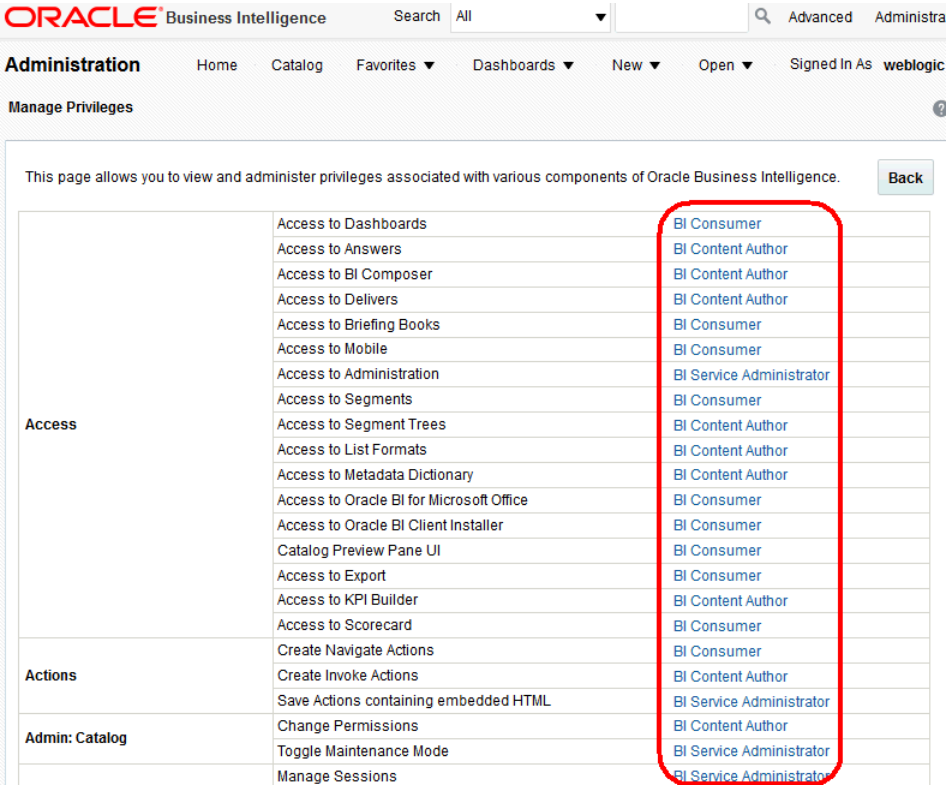


Note: If you log in as a user without Administrator privileges, the Administration option is not displayed.



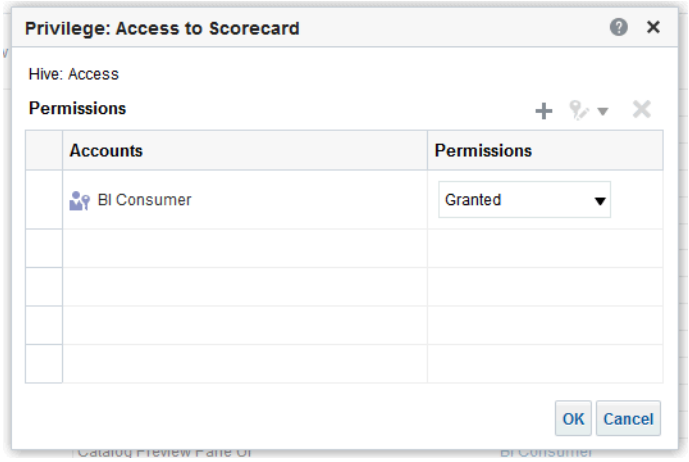
3. In the Security area, click **Manage Privileges** to display the Manage Privileges page.

   This page enables you to view application roles for Presentation Services privileges.



4. Click an application role next to the privilege that you want to administer.

   For example, to administer the privilege named Access to Scorecard for the application role named BIConsumer, you would click the **BIConsumer** link next to Access to Scorecard.



Use the Privilege <*privilege_name*> dialog to add application roles to the list of permissions, and grant and revoke permissions from application roles. For example, to grant the selected privilege to an application role, you must add the application role to the **Permissions** list.

5. Add an application role to the **Permissions** list, as follows:
   a. Click **Add Users/Roles**.
   b. Select **Application Roles** from the list and click **Search**.
   c. Select the application role from the results list.
   d. Use the shuttle controls to move the application role to the **Selected Members** list.
   e. Click **OK**.
6. Set the permission for the application role by selecting **Granted** or **Denied** in the **Permission** list.

   Note: Explicitly *denying* a Presentation Services permission takes precedence over user access rights either granted or inherited as a result of group or application role hierarchy.

7. Save your changes.

   Note: Existing Catalog groups are migrated during the upgrade process. Moving an existing Oracle BI Presentation Catalog security configuration to the role-based Oracle Fusion Middleware security model based requires that each Catalog group be replaced with a corresponding application role. To duplicate an existing Presentation Services configuration, replace each Catalog group with a corresponding application role that grants the same Oracle BI Presentation Catalog privileges. You can then delete the original Catalog group from Presentation Services.

2.6.4 Encrypting Credentials in BI Presentation Services - Advanced Security Configuration Topic

The BI Server and Presentation Services client support industry-standard security for login and password encryption. When an end user enters a user name and password in the web browser, the BI Server uses the Hypertext Transport Protocol Secure (HTTPS) standard to send the information to a secure Oracle BI Presentation Services port. From Oracle BI Presentation Services, the information is passed through ODBC to the BI Server, using Triple DES (Data Encryption Standard). This provides a high level of security (168 bit), preventing unauthorized users from accessing data or Oracle Business Intelligence metadata.

At the database level, Oracle Business Intelligence administrative users can implement database security and authentication. Finally, a proprietary key-based encryption provides security to prevent unauthorized users from accessing the metadata repository.

2.7 Managing Data Source Access Permissions Using Oracle BI Publisher

This section discusses managing the data source access permissions that are stored in Oracle BI Publisher, using the Oracle BI Publisher Administration pages. Data source access permissions control application role access to data sources. A user must be assigned to an application role which is granted specific data source access permissions to enable the user to perform the following tasks:

- Create a data model against the data source.
- Edit a data model against a data source.
- View a report created with a data model built from the data source.

For more information regarding data source security in published reporting, see "Granting Access to Data Sources" in the *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*.

2.8 Enabling High Availability of the Default Embedded Oracle WebLogic Server LDAP Identity Store

This section is only applicable if using the default Weblogic LDAP in a HA environment.

To enable high availability of the default embedded Oracle WebLogic Server LDAP identity store in a clustered environment, you configure the virtualize attribute. When you set the virtualize attribute value to true, BI processes will look to their local Managed Server where they can authenticate and perform lookups against a local copy of the embedded default Oracle WebLogic Server LDAP identity store.

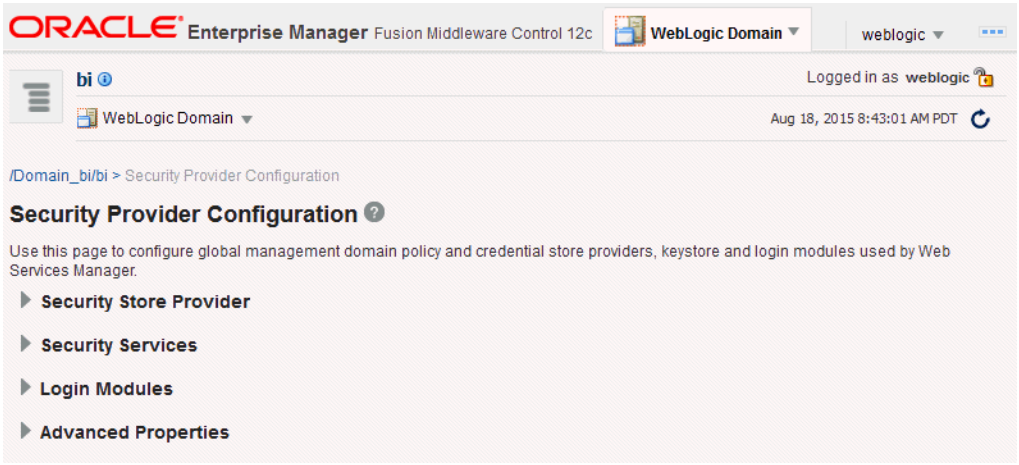
To enable high availability of the default embedded Oracle WebLogic Server LDAP identity store:

1. Log in to Fusion Middleware Control.

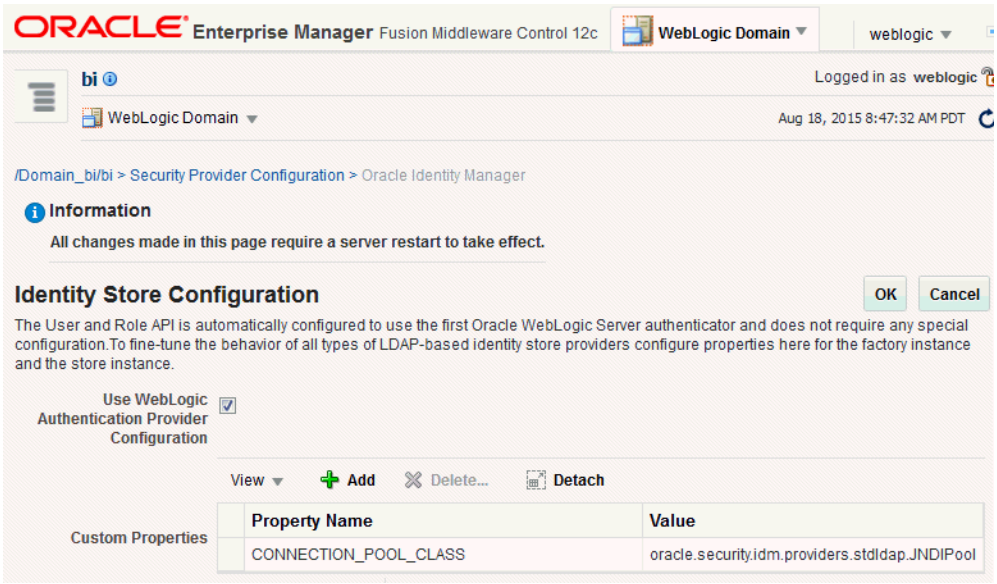
   For more information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".

2. From the navigation pane expand the **WebLogic Domain** folder and select **bi**.

3. Right-click **bi** and select Security, then Security Provider Configuration to display the **Security Provider Configuration** page.



4. Expand Security Store Provider, and Identity Store Provider area, and click **Configure** to display the Identity Store Configuration page.



5. In the Custom Properties area, use the **Add** option to add the following custom properties:

   - Property Name=`virtualize`

     Value=`true`

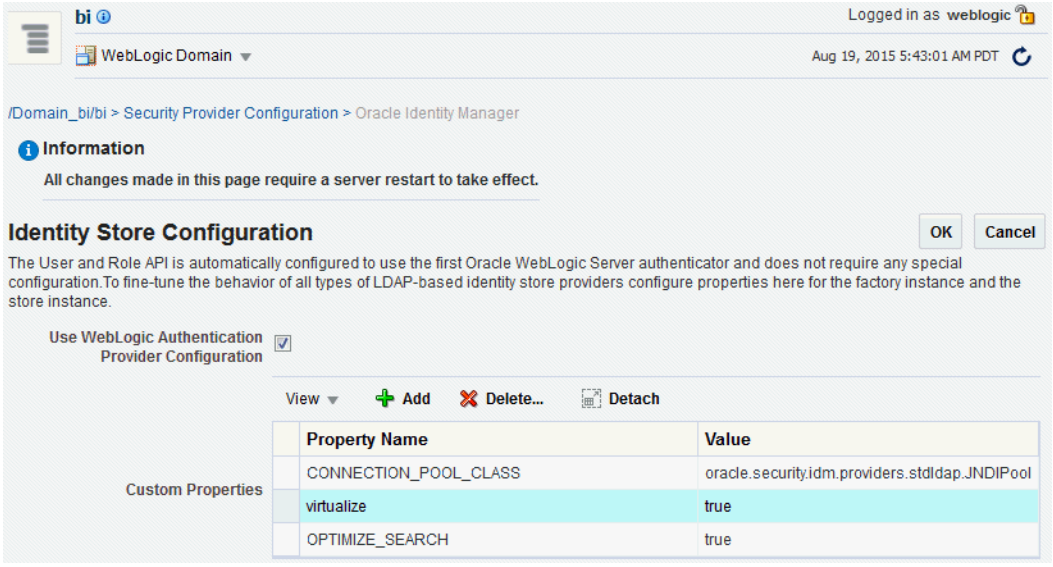
   - Property Name=`OPTIMIZE_SEARCH`

     Value=`true`

   Note: The Property Name `virtualize` must be lowercase, and OPTIMIZE_SEARCH must be uppercase.

   Figure 2–9 shows an example set of Custom Properties including a new property called virtualize with its value set to true.

Figure 2–9 Identity Store Configuration Page Showing New Custom Property



6. Click **OK** to save the changes.
7. Restart the Administration Server, any Managed Servers, and Oracle BI EE components.

2.9 Deleting a User

When a user is no longer required you must completely remove their user ID from the system to prevent an identical, newly-created user from inheriting the old user's access permissions. This situation can occur because authentication and access permissions are associated with user ID.

You delete a user by removing them from the policy store, the Oracle BI Presentation Catalog, the metadata repository, and the identity store.

To delete a user:

1. Delete the user from the policy store.

   If you have assigned the user directly to any application roles, you must remove all references to that user.

2. Delete the user from the Oracle BI Presentation Catalog, and the metadata repository using the command line utility.

   - **Delete Users command**

     To delete a user from the catalog and the metadata repository use the deleteusers command.

     For more information, see "Delete Users Command" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

3. If you are using Oracle WebLogic Server LDAP as your identity store, complete the following steps to delete a user:

   a. Log in to the Oracle WebLogic Server Administration Console.

      For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

b. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**.

c. Select **Users and Groups** tab, then **Users**.

d. Select a user. Click **Delete**.

e. In the **Delete Users** page click **Yes**.

f. Click **OK**.

The user name is removed from the User table in the embedded WebLogic LDAP server.

4. If you are using an identity store other than Oracle WebLogic Server LDAP, follow the appropriate instructions for your identity store.

2.10 Using the runcat Command Line Interface to Manage Security-Related Tasks in the Oracle BI Presentation Catalog

The runcat command line interface enables you to manage some security-related tasks in the Oracle BI Presentation Catalog.

You can invoke the command line utility on supported platforms for Oracle Business Intelligence such as Windows, Linux, IBM-AIX, Sun Solaris, and HP-UX. Enter a command such as the following one on Linux for assistance in using the command line utility:

```
./runcat.sh -help
```

Use the following syntax to convert a permission for a catalog group into a permission for an application role.

```
runcat.cmd/runcat.sh -cmd replaceAccountInPermissions -old <catalog_group_
name> -oldType group -new <application_role_name> -newType role -offline
<catalog_path>
```

For more information see "Opening an Oracle BI Presentation Catalog" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Reporting on Users Privileges for a Set of Oracle BI Presentation Catalog Items

Use the following syntax to report on all privileges in the Oracle BI Presentation Catalog, and who has those privileges. For example:

```
runcat.cmd/runcat.sh -cmd report -online
http://localhost:8080/analytics/saw.dll -credentials
c:/oracle/catmancredentials.properties -outputFile c:/temp/report.txt
-delimiter "\t" -folder "/system/privs" -mustHavePrivilege -type "Security
ACL" -fields "Path:Accounts"       "Must Have Privilege"
```

For help use the following command:

```
runcat.sh -cmd report -help
```

Renaming an Application Role

For more information, see Section 2.4.4.3, "Renaming an Application Role".

3

Using Alternative Authentication Providers

This chapter explains how to configure Oracle Business Intelligence to use alternative directory servers for authentication instead of using the default Oracle WebLogic Server LDAP directory. This chapter explains how to set up Oracle Business Intelligence to use Oracle Internet Directory, Active Directory, and other authentication providers, and also explains how to use OID LDAP, or a database as a policy store, and credential store.

> **Note:** For a detailed list of security setup steps, see Section 1.7, "Detailed List of Steps for Setting Up Security in Oracle Business Intelligence".

This chapter contains the following sections:

3.1 Introduction

When you use an alternative authentication provider, you will typically use administrative tools provided by your provider vendor to set up your users and groups. You can then assign these users and groups to the application roles defined in your BI Service Instance. For more information about assigning users and groups to application roles, see Section 2.4, "Managing Application Roles and Application Policies Using Fusion Middleware Control".

You continue to use the other Oracle Business Intelligence tools (such as, the Oracle BI Administration Tool, Fusion Middleware Control, and the Presentation Services Administration Page) to manage the other areas of the security model.

For a current list of supported authentication providers and directory servers to use with Oracle Business Intelligence, you select the authentication provider from the **Type** list in the **Create a New Authentication Provider** page. For more information, see System Requirements and Certification.

You can configure one or more supported authentication providers. For more information, see Section 3.4, "Configuring Oracle Business Intelligence to Use

Alternative Authentication Providers".

If you use a directory server other than the default WebLogic LDAP Server, you can view the users and groups from the other directory server in Oracle WebLogic Server Administration Console. However, you must manage the users and groups in the interface for the directory server being used. For example, if you are using Oracle Internet Directory (OID LDAP), you must use OID Console to create and edit users and groups.

3.2 High-Level Steps for Configuring an Alternative Authentication Provider

To configure an alternative authentication provider:

1. Ensure your external Identity Store has all the users and groups setup for use with Oracle Business Intelligence.

   For more information, see Section 3.3, "Setting Up Groups and Users in the Alternative Authentication Provider".

2. Configure the necessary authentication provider(s) as described in Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers".

3. Go to the **myrealm\Users and Groups** tab to verify that the users and groups from the alternative authentication provider are displayed correctly. If the users and groups are displayed correctly, then proceed to the next step. Otherwise, reset your configuration settings and retry.

4. Assign application roles to corresponding groups (enterprise roles) of the new identity store, using Fusion Middleware Control.

   For more information, see Section 2.4.4.2, "Adding or Removing Members from an Application Role".

3.3 Setting Up Groups and Users in the Alternative Authentication Provider

Before you use an alternative authentication provider, you must configure suitable groups and users. You then associate them with the application roles within your BI Service Instance. Oracle Business Intelligence does not require or mandate any specific users or groups, and in a production environment your corporate Identity Store, for example Oracle Internet Directory (OID), would typically already contain users and groups relevant to you organization. However, for an example of how you might set up a simple system based on the Sample App Lite or Starter Applications see Section 2.2, "An Example Security Setup of Users, Groups, and Application Roles".

To set up users and groups in an alternative authentication provider:

1. Create groups in the alternative authentication provider similar to the application roles from your BI Service Instance. For example (using the Sample Application):

   BIServiceAdministrators, BIContentAuthors, BIConsumers

2. Create users in the alternative authentication provider, corresponding to the groups from Step 1. For example:

   BISERVICEADMIN, BICONTENTAUTHOR, BICONSUMER

3. Assign the users to respective groups n the alternative authentication provider.

For example, assign BISERVICEADMIN user to the BIServiceAdministrators group.

4. Make the BIContentAuthors group part of the BIConsumers group in the alternative authentication provider.

   This grouping enables BIContentAuthors to inherit permissions and privileges of BIConsumers.

3.4 Configuring Oracle Business Intelligence to Use Alternative Authentication Providers

This section describes how to configure Oracle Business Intelligence to use one or more authentication providers instead of the default Oracle WebLogic Server LDAP directory, and contains the following topics:

- Section 3.4.1, "Reconfiguring Oracle Internet Directory as an Authentication Provider"
- Section 3.4.2, "Reconfiguring Microsoft Active Directory as the Authentication Provider"
- Section 3.4.3, "Configuring User and Group Name Attributes in the Identity Store"
- Section 3.4.4, "Configuring LDAP as the Authentication Provider and Storing Groups in a Database"
- Section 3.4.5, "Configuring a Database as the Authentication Provider"
- Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control"
- Section 3.4.7, "Configuring Multiple Authentication Providers so that When One Fails, Users from Others can Still Log In to Oracle Business Intelligence"
- Section 3.4.8, "Setting the JAAS Control Flag Option"
- Section 3.4.9, "Configuring a Single LDAP Authentication Provider as the Authenticator"

Note: Storing users and groups in a single LDAP Identity Store may be sufficient. However, for more advanced installations, you may need your users in multiple LDAP identity stores, or in a database Identity Store. You enable these using a mechanism called 'Identity Store Virtualization' (see Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control").

Note: This section shows settings for specific authentication providers. However, you can also use the instructions as a general guide for configuring other authentication providers.

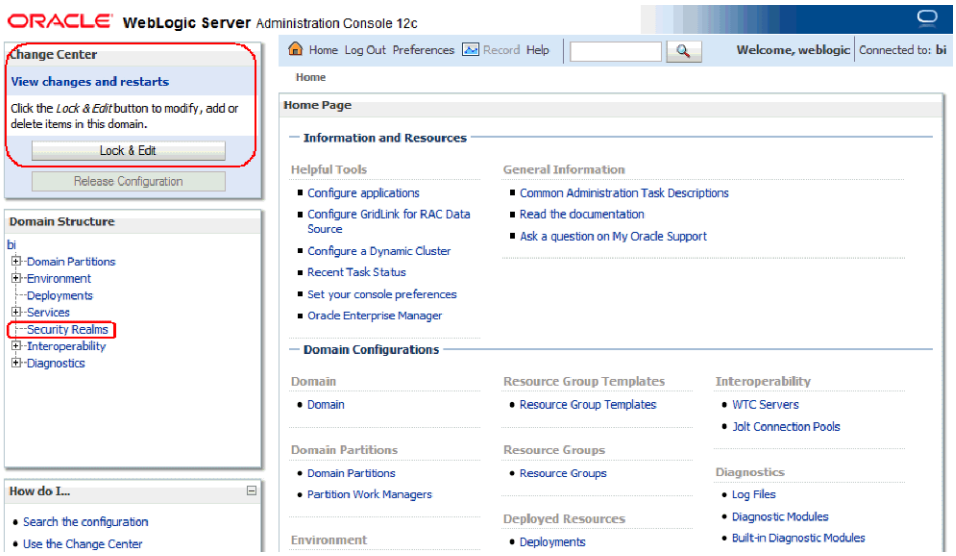
3.4.1 Reconfiguring Oracle Internet Directory as an Authentication Provider

This procedure illustrates how to reconfigure your Oracle Business Intelligence installation to use Oracle Internet Directory(OID LDAP).

To reconfigure OID LDAP as the authentication provider:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

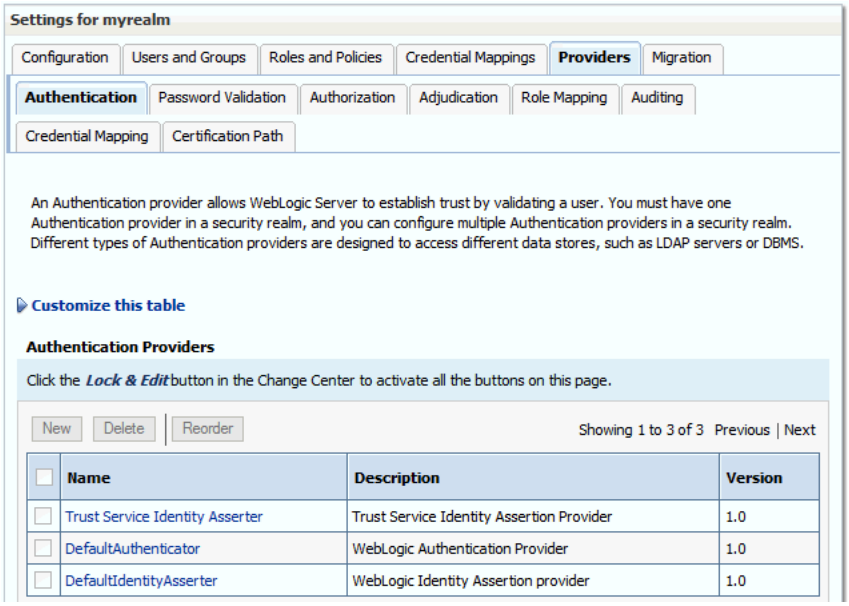
   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".



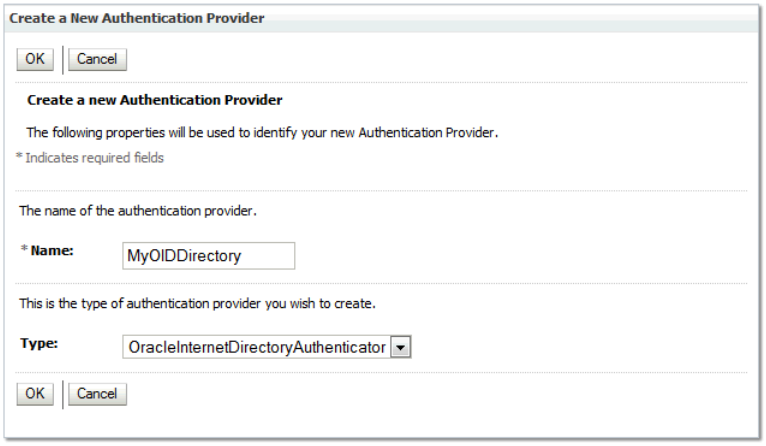
2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

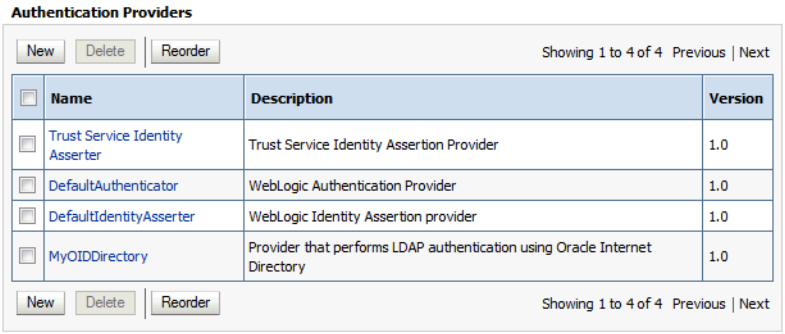
3. Display the **Providers** tab, then display the **Authentication** sub-tab.



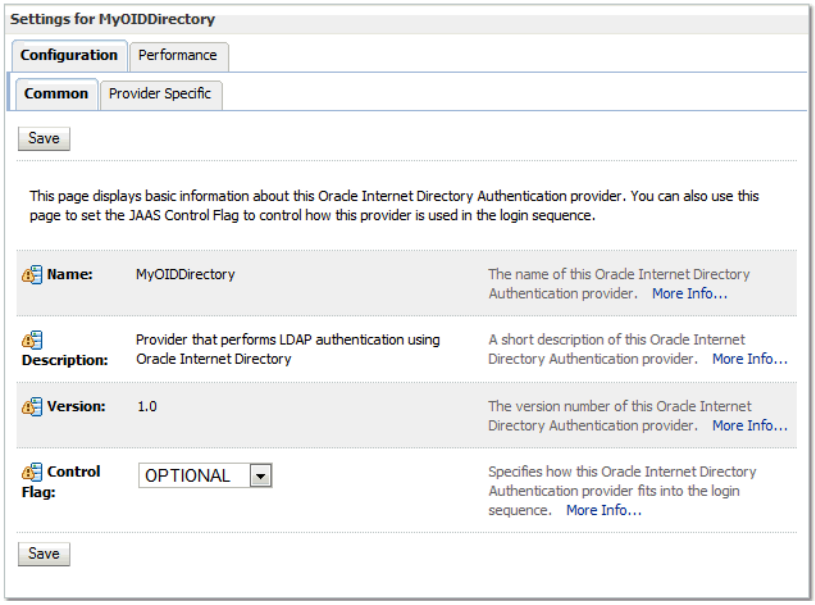
4. Click **New** to launch the **Create a New Authentication Provider** page.



5. Enter values in the **Create a New Authentication Provider** page as follows:
   - **Name**: Enter a name for the authentication provider. For example, MyOIDDirectory.
   - **Type**: Select OracleInternetDirectoryAuthenticator from the list.
   - Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.

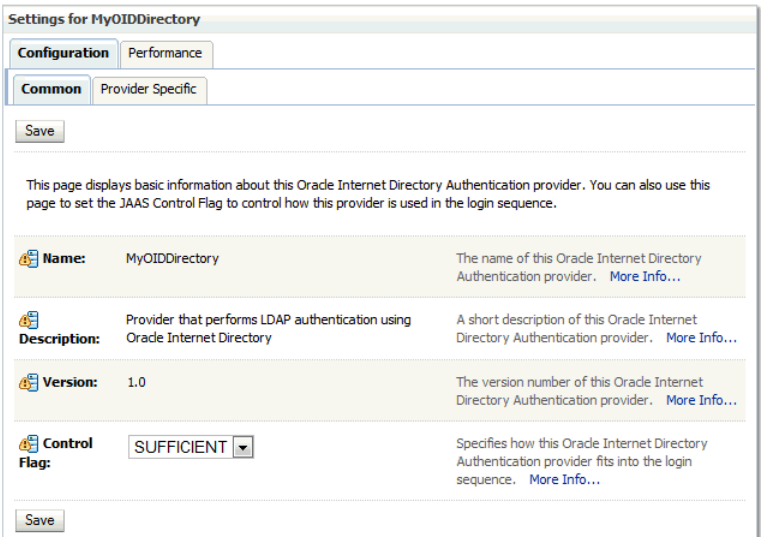


6. Click MyOIDDirectory in the **Name** column of the **Authentication Providers** table to display the **Settings** page.

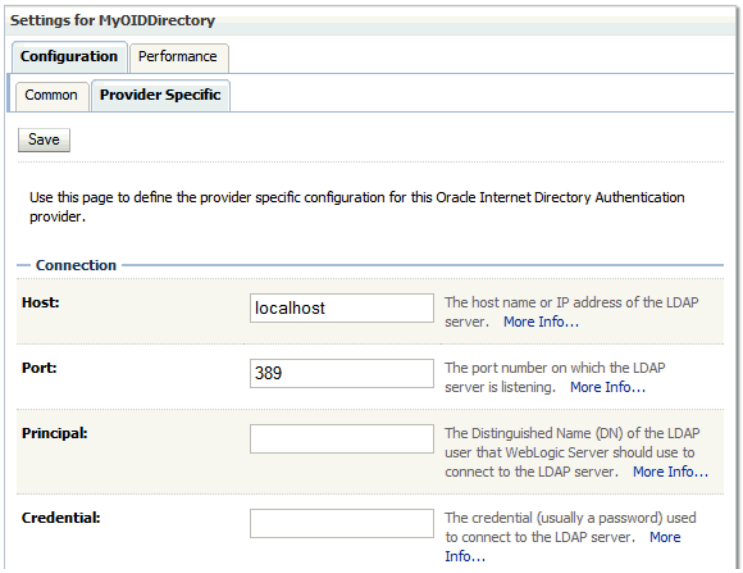


7. Display the **Configuration****Common** tab, and use the **Control Flag** list to select 'SUFFICIENT', then click **Save**.

   For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".



8. Display the **Provider Specific** tab.



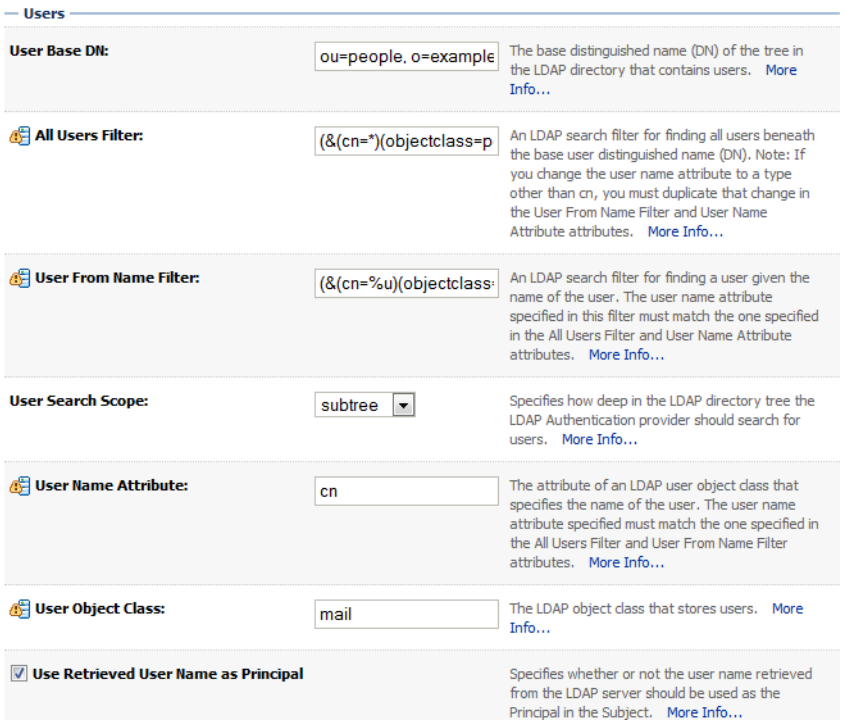
9. Use the Provider Specific tab to specify the following details:

Section Name	Field Name	Description
Connection	Host	The host name of the Oracle Internet Directory server.
Connection	Port	The port number on which the Oracle Internet Directory server is listening.
Connection	Principal	The distinguished name (DN) of the Oracle Internet Directory user to be used to connect to the Oracle Internet Directory server. For example: cn=OIDUser,cn=users,dc=us,dc=mycompany,dc=com.
Connection	Credential	The Password for the Oracle Internet Directory user entered as the Principal.
Groups	Group Base DN	The base distinguished name (DN) of the Oracle Internet Directory server tree that contains groups.
Users	User Base DN	The base distinguished name (DN) of the Oracle Internet Directory server tree that contains users.
Users	All Users Filter	The LDAP search filter. Click More Info... for details. Leave this blank, as this is the default value for the Active Directory authenticator. Note that any filter that you add to the All Users Filter is appended to all user searches.
Users	User From Name Filter	The LDAP search filter. Click More Info... for details.

Section Name	Field Name	Description
Users	User Name Attribute	The attribute that you want to use to authenticate (for example, cn, uid, or mail). For example, to authenticate using a user's email address you set this value to `mail`. **Note**: The value that you specify here must match the User Name Attribute that you are using in the authentication provider, as described in Section 3.4.3.1, "Configuring User Name Attributes".

Figure 3–1 shows the Users area of the Provider Specific tab.

Figure 3–1 Provider Specific Tab - Users Area



For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

10. (Optional) If the User Name attribute, or the Group Name attribute is configured to a value other than 'cn' in Oracle Internet Directory, you must change corresponding values in Oracle WebLogic Server Administration Console.

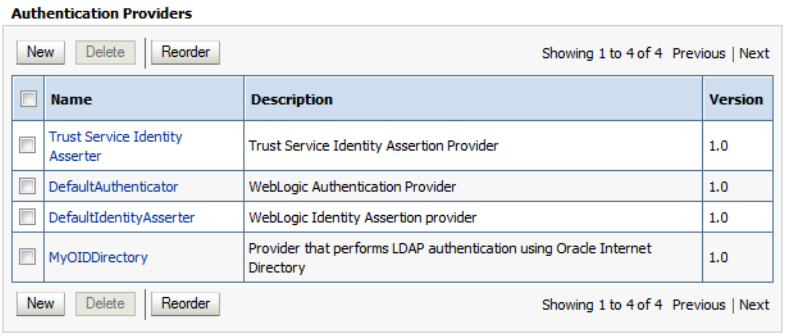
    For more information, see Section 3.4.3, "Configuring User and Group Name Attributes in the Identity Store".

Note: The LDAP authenticators provided by WebLogic (including OracleInternetDirectoryAuthenticator and ActiveDirectoryAuthenticator), typically default to using 'cn' as the user name and group name attributes. It is often necessary to use alternative attributes for the user name, for example 'uid' or 'mail', although it is less common to need to use different group name attributes.

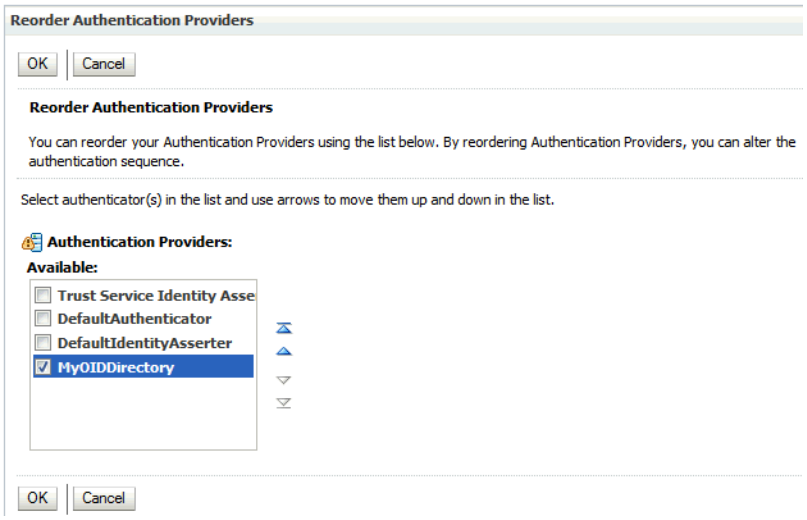
---

11. Click **Save**.
12. Perform the following steps to set up the DefaultAuthenticator **Control Flag** setting:
    a. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab, then select **DefaultAuthenticator** to display its configuration page.
    b. Display the **Configuration\Common** tab and select 'SUFFICIENT' from the **Control Flag** list.

       For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".
    c. Click **Save**.
13. Perform the following steps to reorder Providers:
    a. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab.

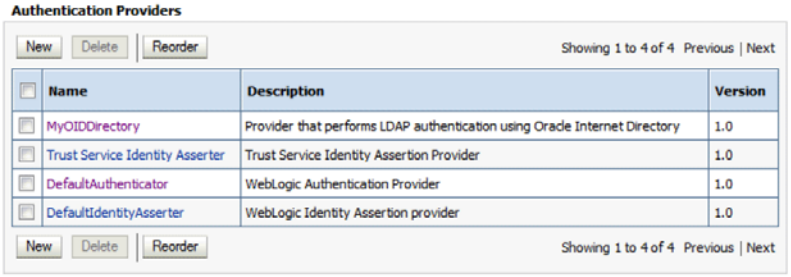


    b. Click **Reorder** to display the **Reorder Authentication Providers** page
    c. Select MyOIDDirectory and use the arrow buttons to move it into the first position in the list, then click **OK**.



d. Click **OK** to save your changes.

The authentication providers are displayed in the re-ordered sequence.



14. Click **Save**.
15. In the Change Center, click **Activate Changes**.
16. Restart Oracle WebLogic Server.

3.4.2 Reconfiguring Microsoft Active Directory as the Authentication Provider

This procedure illustrates how to reconfigure your Oracle Business Intelligence installation to use Microsoft Active Directory.

The example data in this section uses a fictional company called XYZ Corporation that wants to set up SSO for Oracle Business Intelligence for their internal users.

This example uses the following information:

- Active Directory domain

  The XYZ Corporation has an Active Directory domain, called xyzcorp.com, which authenticates all the internal users. When users log in to the corporate network, the log in to the Active Directory domain. The domain controller is addc.xyzcorp.com, which controls the Active Directory domain.

- Oracle BI EE WebLogic domain

  The XYZ Corporation has a WebLogic domain called bi (default name) installed on a network server domain called bieesvr1.xyz2.com.

- System Administrator and Test user

The following system administrator and domain user test the configuration:

- System Administrator user

  Jo Smith (login=jsmith, hostname=xyz1.xyzcorp.com)

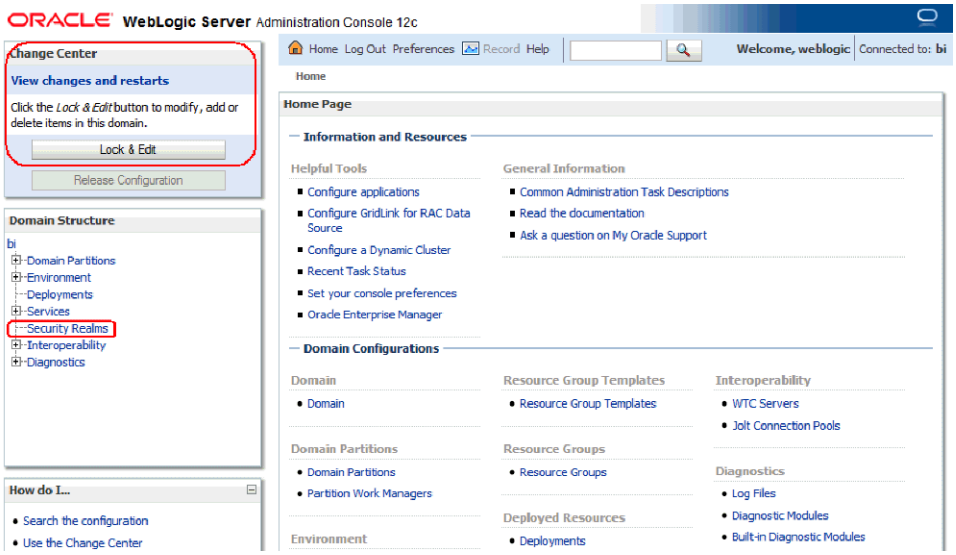
- Domain user

  Bob Jones (login=bjones hostname=xyz47.xyzcorp.com)

To reconfigure Active Directory as the Authentication Provider:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

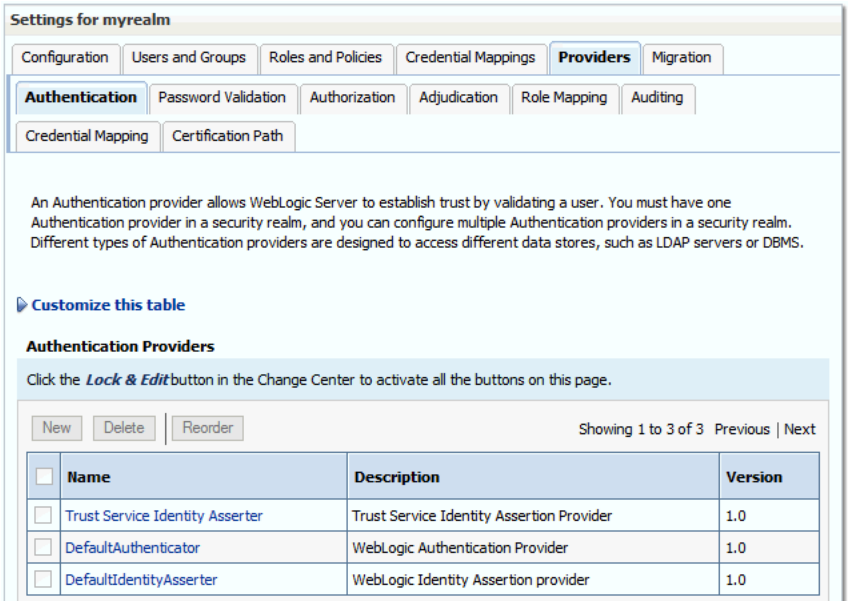
   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".



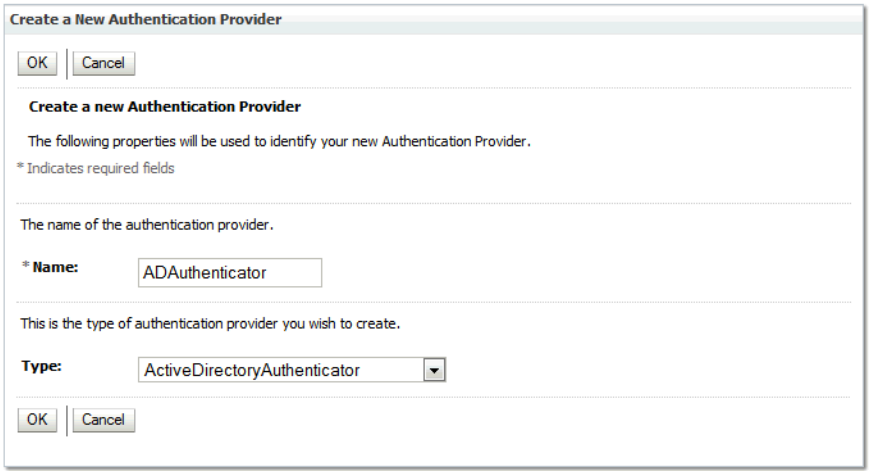
2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

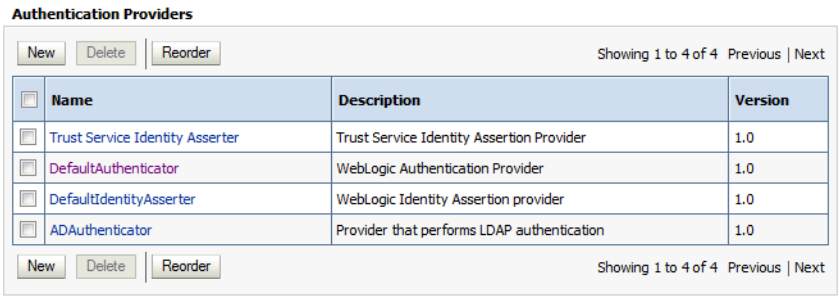
3. Display the **Providers** tab, then display the **Authentication** sub-tab.



4. Click **New** to launch the **Create a New Authentication Provider** page.

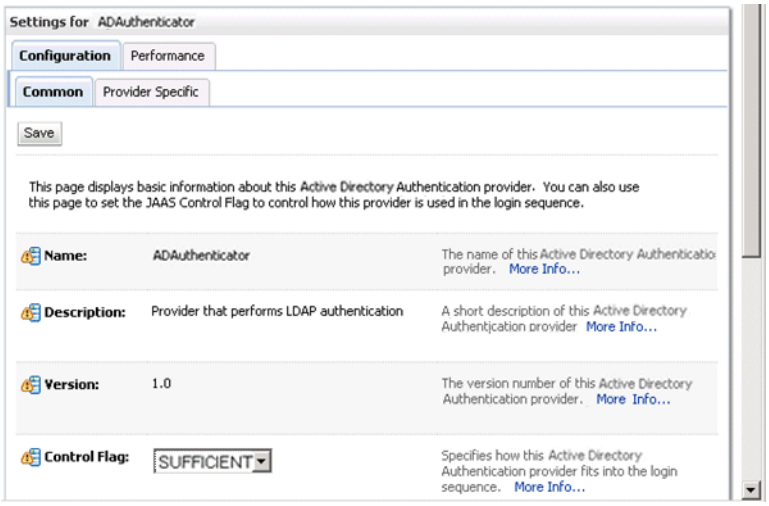


5. Enter values in the **Create a New Authentication Provider** page as follows:
   - **Name**: Enter a name for the authentication provider. For example, ADAuthenticator.
   - **Type**: Select ActiveDirectoryAuthenticator from the list.
   - Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.



6. Click DefaultAuthenticator in the **Name** column to display the Settings page.
7. In the Common Authentication Provider Settings page, change the **Control Flag** from REQUIRED to SUFFICIENT and click **Save**.

   For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".
8. In the authentication providers table, click ADDirectory in the **Name** column to display the Settings page.
9. Display the **Configuration****Common** tab, and use the **Control Flag** list to select 'SUFFICIENT', then click **Save**.



10. Display the **Provider Specific** tab to access the options which apply specifically to connecting to an Active Directory LDAP authentication store.
11. Use the Provider Specific tab to specify the following details:

Section Name	Field Name	Description
Connection	Host	The name of the Active Directory server addc.xyzcorp.com.
Connection	Port	The port number on which the Active Directory server is listening (389).
Connection	Principal	The LDAP DN for the user that connects to Active Directory when retrieving information about LDAP users. For example: cn=jsmith,cn=users,dc=us,dc=xyzcorp,dc=com.
Connection	Credential/Confirm Credential	Password for the specified Principal (for example welcome1).
Groups	Group Base DN	The LDAP query used to find groups in AD. **Note:** Only groups defined under this path will be visible to WebLogic. (CN=Builtin,DC=xyzcorp,DC=com).
Users	User Base DN	The LDAP query used to find users in AD. CN=Users,DC=xyzcorp,DC=com

Section Name	Field Name	Description
Users	User Name Attribute	Attribute used to specify user name in AD. Default value is cn. Do not change this value unless you know your Active Directory is configured to use a different attribute for user name. If you do change it, see, Section 3.4.3.1, "Configuring User Name Attributes".
Users	All Users Filter	LDAP search filter. Click More Info... for details.
Users	User From Name Filter	LDAP search filter. Blank by default in AD. Click More Info... for details.
Users	User Object class	The name of the user.
Users	Use Retrieved User Name as Principal	Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. Click More Info... for details. Oracle recommends that you select this check box as it helps to enforce consistent case usage. For example, if your LDAP user name is JSmith, but you logged in as jsmith (lower case) the Principal is still JSmith (mixed case). This means that any application role memberships granted directly to users, instead of indirectly through groups, are consistently applied at authentication time.

For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

12. (Optional) If the User Name attribute, or the Group Name attribute is configured to a value other than 'cn' in Microsoft Active Directory, you must change corresponding values in Oracle WebLogic Server Administration Console.

    For more information, see Section 3.4.3, "Configuring User and Group Name Attributes in the Identity Store".

    Note: The LDAP authenticators provided by WebLogic (including OracleInternetDirectoryAuthenticator and ActiveDirectoryAuthenticator), typically default to using 'cn' as the user name and group name attributes. It is often necessary to use alternative attributes for the user name, for example 'uid' or 'mail', although it is less common to need to use different group name attributes.

13. Click **Save**.
14. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab.
15. Click **Reorder** to display the Reorder Authentication Providers page.

16. Select ADDirectory and use the arrow buttons to move it into the first position in the list, then click OK.
17. In the Change Center, click **Activate Changes**.
18. Restart Oracle WebLogic Server.

3.4.3 Configuring User and Group Name Attributes in the Identity Store

The LDAP authenticators provided by WebLogic, including OracleInternetDirectoryAuthenticator and ActiveDirectoryAuthenticator, typically default to using 'cn' as the user name and group name attributes. It is often necessary to use alternative attributes for the user name, for example 'uid' or 'mail', although it is less common to need to use different group name attributes. This section explains how to reconfigure both.

This topic contains the following sections:

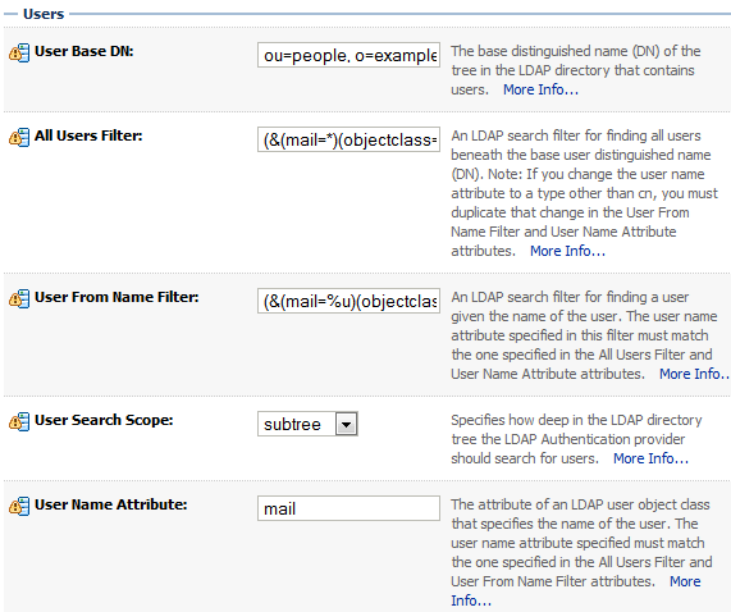
- Section 3.4.3.1, "Configuring User Name Attributes"
- Section 3.4.3.2, "Configuring Group Name Attributes"

3.4.3.1 Configuring User Name Attributes

This section describes how to reconfigure the OracleInternetDirectoryAuthenticator, for example, to use mail as the User Name Attribute.

Figure 3–2 shows the **User Name Attribute** configured with the value mail.

Figure 3–2 Example: Provider Specific Tab - User Attributes



The UserNameAttribute in the alternative authentication provider is usually set to the value "cn"; if it is not, you must make sure the settings for AllUsersFilter and UserFromNameFilter are configured correctly as shown in Table 3–1. Table 3–1 illustrates the default setting (using the value cn), and a required new setting (using a new value in the attribute AnOtherUserAttribute).

Table 3–1 Changing User Name Attribute

Attribute Name	Default Setting	Required New Setting
UserNameAttribute	cn	**AnOtherUserAttribute**
AllUsersFilter	(&(cn=*)(objectclass=person))	(&(**AnOtherUserAttribute** =*)(objectclass=person))
UserFromNameFilter	(&(cn=%u)(objectclass=person))	(&(**AnOtherUserAttribute** =%u)(objectclass=person))

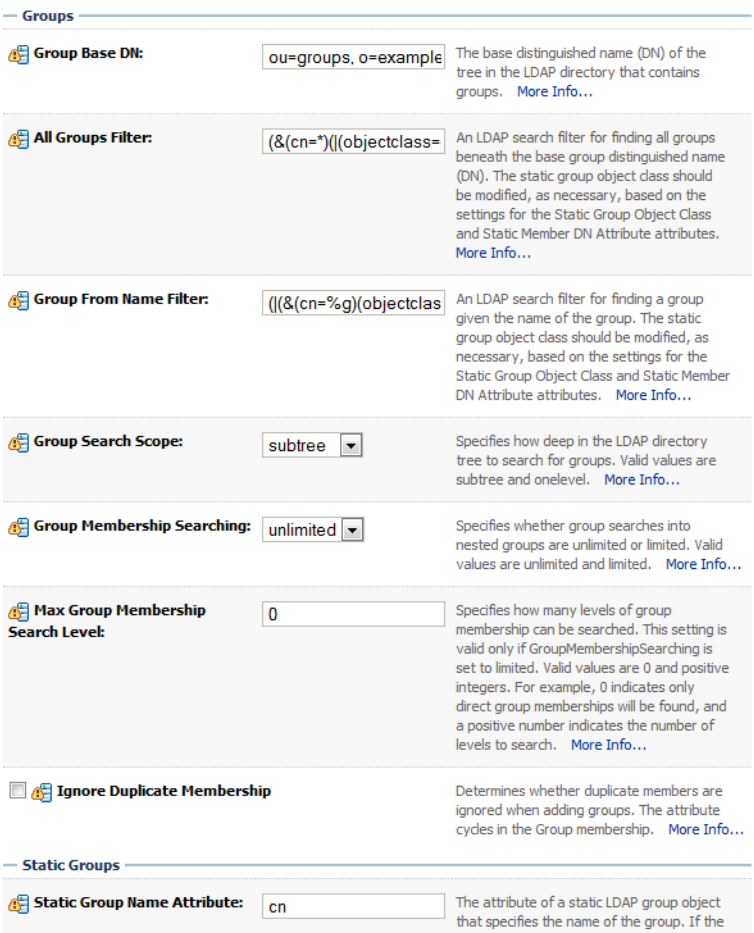
Make the changes in the Provider Specific tab, using Table 3–1 (substitute the AnOtherGroupAttribute setting with your own value). For more information about how to display the Provider Specific tab, see Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers".

3.4.3.2 Configuring Group Name Attributes

This section describes how to reconfigure the ActiveDirectoryAuthenticator, to use a group name other than cn.

Figure 3–3 shows group settings.

Figure 3–3 Example: Provider Specific Tab - Group Attributes



If the group name, for example, for Active Directory server is set to anything other than the default value "cn", you must change it. If you change the value, you must also

change the values of AllGroupsFilter and GroupFromNameFilter as shown in Table 3–2 (the example shows a group name stored in an attribute called AnOtherGroupAttribute).

Table 3–2 Changing Group Name Attributes

Attribute Name	Default Setting	Required New Setting
StaticGroupNameAttribute/DynamicGroupNameAttribute	cn	**AnOtherGroupAttribute**
AllGroupsFilter	(&(cn=*)(objectclass=person))	(&(**AnOtherGroupAttribute**=*)(objectclass=person))
GroupFromNameFilter	(&(cn=%u)(objectclass=person))	(&(**AnOtherGroupAttribute**=%u)(objectclass=person))

Make the changes in the Provider Specific tab, using Table 3–2 (substitute the AnOtherGroupAttribute setting with your own value). For more information about how to display the Provider Specific tab, see Section 3.4.2, "Reconfiguring Microsoft Active Directory as the Authentication Provider".

3.4.4 Configuring LDAP as the Authentication Provider and Storing Groups in a Database

This section describes how to configure Oracle Business Intelligence to authenticate against an LDAP Identity Store, and store group information in a database. The examples provided in this section use Oracle Internet Directory (OID LDAP), and a sample database schema. However, you do not have to use OID LDAP as your LDAP identity store and your database schema does not have to be identical to the sample provided.

Oracle Business Intelligence provides an authentication provider for WebLogic Server called BISQLGroupProvider that enables you to use this method. This authentication provider does not authenticate end user credentials but enables external group memberships held in a database table to contribute to an authenticated user's identity.

This section contains the following topics:

- Section 3.4.4.1, "Prerequisites"
- Section 3.4.4.2, "Creating a Sample Schema for Groups and Group Members"
- Section 3.4.4.3, "Configuring a Data Source and the BISQLGroupProvider Using Oracle WebLogic Server Administration Console"
- Section 3.4.4.4, "Configuring the Virtualized Identity Store"
- Section 3.4.4.5, "Testing the Configuration by Adding a Database Group to an Application Role"
- Section 3.4.4.6, "Correcting Errors in the Adaptors"

3.4.4.1 Prerequisites

The following prerequisites must be satisfied before you attempt to configure LDAP authentication as described in this section:

- Oracle Business Intelligence Enterprise Edition Release 12.2.1.0 (or higher) must be installed and running.
- You must apply all relevant patches to the Oracle BI EE 12.2.1.0 system.

- A suitable database schema containing at least one table with the required groups in it, and a mapping table which maps those groups to the names of users authenticated by LDAP must be running and accessible from the WebLogic Server on which Oracle BI EE is running.
- The configuration must include a supported LDAP server to use as the identity store that contains users.
- If you need Oracle Business Intelligence to deliver content to members of an application role the following restrictions apply:
  - You can only pair a single LDAP authenticator with a single BISQLGroupProvider.

    When you configure multiple LDAP authenticators and want to retrieve group membership from the BISQLGroupProvider, content cannot be delivered to all members of an application role. In this configuration Oracle BI Delivers cannot resolve application role membership based on users and group membership.
  - You cannot define the same group in more than one identity store.

    You cannot have a group with the same name in both LDAP and database groups table. If you do, the security code invoked by Oracle BI Delivers cannot resolve application role membership.

3.4.4.2 Creating a Sample Schema for Groups and Group Members

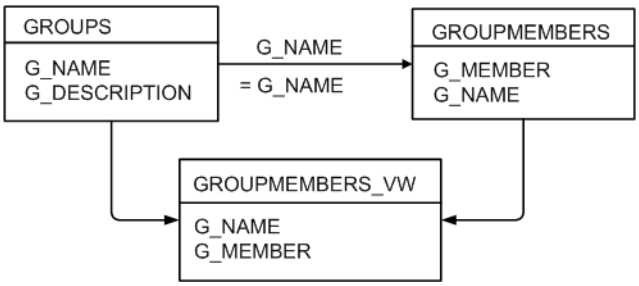
The sample schema described here is deliberately simplistic, and is intended only to illustrate how to configure Oracle Business Intelligence to use the schema.

The sample schema is called ACME_BI_GROUPS and contains two tables and a view: the GROUPS table defines the list of external groups, the GROUPMEMBERS table, and GROUPMEMBERS_VW view which describe group membership for users that exist in your primary identity store.

The advantage of defining tables (or views) identical to Figure 3–4 is that the configuration of the BISQLGroupProvider can use the default SQL outlined in Table 3–3.

Figure 3–4 has the tables GROUPS, GROUPMEMBERS, and the view GROUPMEMBERS_VW.

Figure 3–4 Sample Schema for Groups and Group Members



You must map the users in your LDAP store to Groups in your database table by login name. In Figure 3–4, the value of G_MEMBER in the GROUPMEMBERS table must match the value of the LDAP attribute used for login (for example, uid, cn or mail), as specified in the LDAP authenticator. For example, you should not map the database groups by uid if the login attribute is mail. Create a GROUPMEMBERS_VW view with an outer join between GROUPMEMBERS and GROUPS tables.

3.4.4.3 Configuring a Data Source and the BISQLGroupProvider Using Oracle WebLogic Server Administration Console

You configure a data source and the BISQLGroupProvider using Oracle WebLogic Server Administration Console as follows:

- Section 3.4.4.3.1, "Configuring Oracle Internet Directory as the Primary Identity Store for Authentication Using Oracle WebLogic Server"
- Section 3.4.4.3.2, "Installing the BISQLGroupProvider"
- Section 3.4.4.3.3, "Configuring the Data Source Using Oracle WebLogic Server Administration Console"
- Section 3.4.4.3.4, "Configuring the BISQLGroupProvider SQL Authenticator Using Oracle WebLogic Server Administration Console"

3.4.4.3.1 Configuring Oracle Internet Directory as the Primary Identity Store for Authentication Using Oracle WebLogic Server Follow the link to instructions that will enable you to configure WebLogic to authenticate your user population against OID LDAP.

For more information, see Section 3.4.1, "Reconfiguring Oracle Internet Directory as an Authentication Provider".

> **Note:** When following the steps of this task, make a note of the value of the **User Base DN** and **User Name Attribute** in the Provider Specific configuration page for your OID LDAP authenticator, which will be needed later. For more information, see Section 3.4.4.4.3, "Configuring a Database Adaptor to Retrieve Group Information".

3.4.4.3.2 Installing the BISQLGroupProvider Before you can configure a BISQLGroupProvider authenticator, you must first install the JAR file bi-sql-group-provider.jar, which contains the authenticator. The file is available in the following location:

ORACLE_HOME/bi/plugins/security/bi-sql-group-provider.jar

You must copy the file to the following location:

ORACLE_HOME/wlserver/server/lib/mbeantypes

After copying the file into the specified location you must restart the Administration Server to enable the new provider to appear in the list of available authenticators.

> **Note:** If you perform an Enterprise Install to create a clustered environment, then the installation cannot start the scaled-out Managed server because the bi-sql-group-provider.jar file is not available. When this situation occurs during installation, copy the Jar file to the correct location and click **Retry** in the installer.

3.4.4.3.3 Configuring the Data Source Using Oracle WebLogic Server Administration Console

To configure the data source using Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. Click **Services** in the left pane and click **Data Sources**.
3. In the Summary of Data Sources page, click **New**, and select **Generic Data Source**.
4. In the JDBC Data Sources Properties page, enter or select values for the following properties:
   - **Name** - For example, enter: `BIDatabaseGroupDS`

     The name used in the underlying configuration file (config.xml) and throughout the Oracle WebLogic Server Administration Console whenever referring to this data source.
   - **JNDI Name** - For example, enter: `jdbc/BIDatabaseGroupDS`

     The JNDI path to which this JDBC data source will be bound.
   - **Database Type** - For example, select: Oracle

     The DBMS of the database that you want to connect to.
5. Click **Next**.
6. Select a database driver from the **Database Driver** drop down list.

   For example, select: Oracle's Driver (Thin) for Service Connections; Versions:9.0.1 and later.

   Note: If using an Oracle database, select 'Oracle's Driver (Thin) for Service Connections; Releases:9.0.1 and later'.
7. Click **Next**.
8. Click **Next**.
9. On the Connection Properties page, enter values for the following properties:
   - **Database Name** - For example, enter: `ora11g`

     The name of the database that you want to connect to.
   - **Host Name** - For example, enter: `mymachine.example.com`

     The DNS name or IP address of the server that hosts the database.

     Note: Do not use localhost if you intend to use a cluster.
   - **Port** - For example, enter: `1521`

     The port on which the database server listens for connections requests.
   - **Database User Name**

     Typically the schema owner of the tables defined in Section 3.4.4.2.

     For example, enter `MYUSER`.
   - **Password/Confirm Password**

     The password for the **Database User Name**.

     For example, enter `mypassword`.
10. Click **Next**.
11. Check the details on the page are correct, and click **Test Configuration**.

12. Click **Next**.
13. In the Select Targets page select the servers or clusters for your data source to be deployed to.

    You should select the Administration Server and Managed Servers as your targets, for example:

    - In the Servers pane

      Select the **AdminServer** option.

    - In the Clusters pane

      Select the **bi_server1** check box to deploy to the cluster (this does not apply to a Simple Install).

14. Click **Finish**.
15. In the Change Center, click **Activate Changes**.

> **Note:** In this example, the data source is called BIDatabaseGroupDS.

3.4.4.3.4 Configuring the BISQLGroupProvider SQL Authenticator Using Oracle WebLogic Server Administration Console

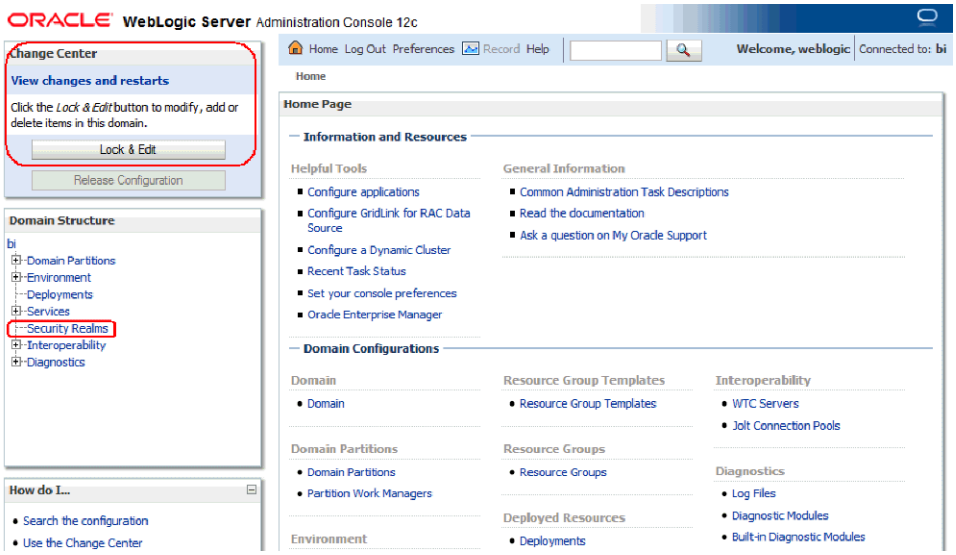
This task explains how to create a BISQLGroupProvider against the BIDatabaseGroupDS data source using the example table structure outlined in Section 3.4.4.2, "Creating a Sample Schema for Groups and Group Members". You may need to modify the SQL statements used (table or column names) if your structure differs from the example.

> **Note:** There is no authentication against the database, as it just stores the groups to be associated with users. Authentication occurs against LDAP and the database is exposed when the BISQLGroupProvider assigns groups to application roles in Oracle WebLogic Server Administration Console.

To configure the BISQLGroupProvider SQL authenticator using Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console as a WebLogic administrator, and click **Lock & Edit** in the Change Center.

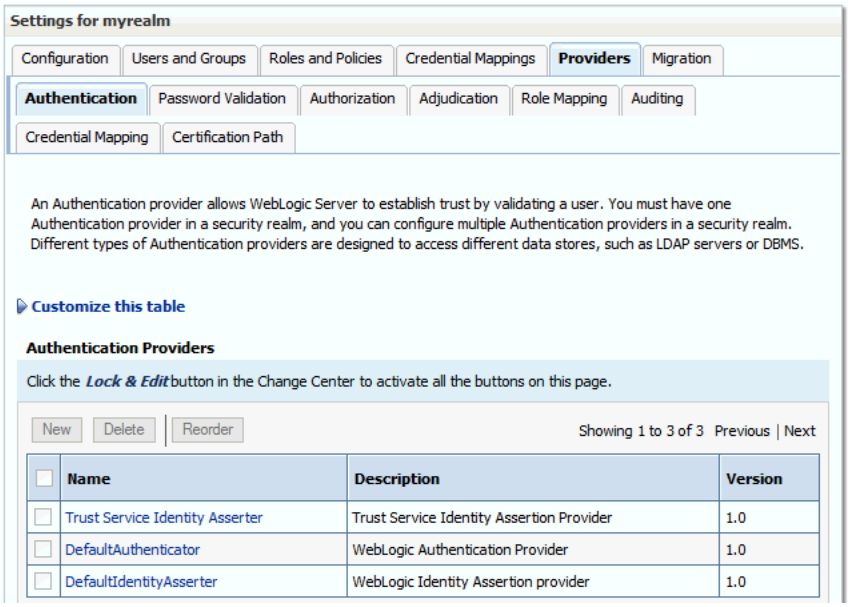
   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".



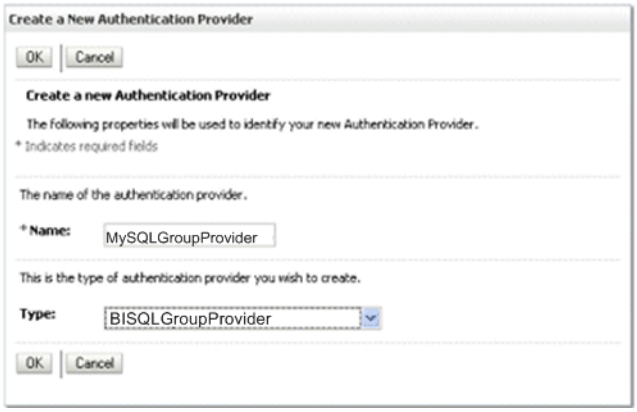
2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

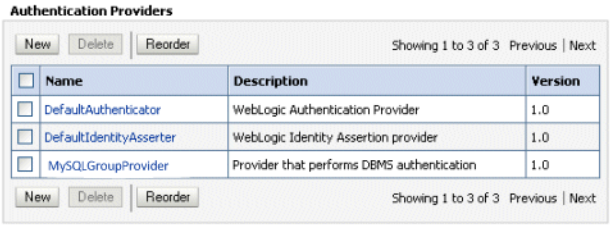
3. Display the **Providers** tab, then display the **Authentication** sub-tab.



4. Click **New** to launch the **Create a New Authentication Provider** page.



5. Enter values in the **Create a New Authentication Provider** page as follows:
   - **Name**: Enter a name for the authentication provider. For example, MySQLGroupProvider.
   - **Type**: Select BISQLGroupProvider from the list.
   - Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.



6. In the authentication providers table, click MySQLGroupProvider in the **Name** column to display the Settings page.
7. Display the **Provider Specific** tab to specify the SQL statements used to query and authenticate against your database tables.
8. Specify the **DataSource Name**. This should be the JNDI name rather than the data source name. For example: `jdbc/BIDatabaseGroupDS`.

   Table 3–3 shows SQL statements for the sample schema outlined in Section 3.4.4.2

Table 3–3 SQL Statements for the Sample Schema

Query	SQL	Notes
SQL List Groups	SELECT G_NAME FROM GROUPS WHERE G_NAME LIKE ?	The SQL statement used to retrieve group names that match a wildcard. The SQL statement requires a single parameter for the group name and must return a resultSet containing matching groups.
SQL Group Exists	SELECT G_NAME FROM GROUPS WHERE G_NAME = ?	The SQL statement used to look up a group. The SQL statement requires a single parameter for the group name and must return a resultSet containing at most a single record containing the group.

Table 3–3 (Cont.) SQL Statements for the Sample Schema

Query	SQL	Notes
SQL Is Member	SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_ NAME = ? AND G_MEMBER = ?	The SQL statement used to look up members of a group. The SQL statement requires two parameters: a group name and a member or group name. It must return a resultSet containing the group names that matched.
SQL List Member Groups	SELECT G_NAME FROM GROUPMEMBERS WHERE G_ MEMBER = ?	The SQL statement used to look up the groups a user or group is a member of. The SQL statement requires a single parameter for the username or group name and returns a resultSet containing the names of the groups that matched.
SQL Get Group Description (if description supported enabled)	SELECT G_DESCRIPTION FROM GROUPS WHERE G_ NAME = ?	The SQL statement used to retrieve the description of a group. Only valid if Descriptions Supported is enabled. The SQL statement requires a single parameter for the group name and must return a resultSet containing at most a single record containing the group description.

Note: If you are using a different table structure, you might need to adapt these SQL statements (table or column names) to your own schema. Also, you should leave the question mark (?) as a runtime query placeholder (rather than hardcode a user or group name).

For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

9. Enter all of the SQL statements appropriate to your authenticator.

   The SQL is case sensitive.

10. Click **Save**.

11. Perform the following steps to reorder the authentication providers:

    a. Display the **Providers** tab.

    b. Click **Reorder** to display the **Reorder Authentication Providers** page

    c. Select **BISQLGroupProvider** and use the arrow buttons to move it into the first position in the list.

    d. Click **OK** to save your changes.

12. Perform the following steps to configure the **Control Flag** setting of **BISQLGroupProvider**:

    a. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab, then select **BISQLGroupProvider** to display its configuration page.

    b. Display the **Configuration\Common** tab and select 'OPTIONAL' from the **Control Flag** list.

For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".

c. Click **Save**.

13. In the Change Center, click **Activate Changes**.

14. Restart the Oracle Business Intelligence components (use Fusion Middleware Control once the Administration Server has been restarted), Oracle WebLogic Server, and Managed servers.

Note: Check the **Users and Groups** tab to confirm that the database users and groups appear there.

3.4.4.4 Configuring the Virtualized Identity Store

You configure the virtualized identity store as follows:

- Section 3.4.4.4.1, "Enabling Virtualization by Configuring the Identity Store"
- Section 3.4.4.4.2, "Configuring SSL Against LDAP"
- Section 3.4.4.4.3, "Configuring a Database Adaptor to Retrieve Group Information"

3.4.4.4.1 Enabling Virtualization by Configuring the Identity Store You configure the identity store to enable virtualization so that more than one identity store can be used with the identity store service, and therefore user profile information can be split across different authentication providers (identity stores).

For more information, see Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control".

3.4.4.4.2 Configuring SSL Against LDAP If you have configured an LDAP Authenticator to communicate over SSL (one-way SSL only), you must put the corresponding LDAP server's route certificate in an additional keystore used by the virtualization (libOVD) functionality.

For more information, see Section 5.14.2, "Configuring SSL when Using Multiple Authenticators".

3.4.4.4.3 Configuring a Database Adaptor to Retrieve Group Information You configure a database adaptor to make it appear like an LDAP server, which enables the virtualized identity store provider to retrieve group information from a database using the database adapter.

To configure a database adaptor to retrieve group information:

This task shows how to edit and apply adapter templates that specify how to use your database tables as an identity store to map groups.

1. Create a file named bi_sql_groups_adapter_template.xml.

   This file describes the mapping of the GROUPMEMBERS_VW view to a virtual LDAP store. The view uses an outer join to ensure that fields from more than one table can be referenced by the database adaptor.

2. Make sure that the file contains the following contents:

Note: You must adapt the sections of **bold** text below to match your table and column attributes against LDAP server attributes. The example shown here is of the sample schema that is used throughout Section 3.4.4.

Note: For the element:<param name="ReplaceAttribute" value="uniquemember={cn=%uniquemember%,cn=users,dc=oracle,dc=com}"/>

This must match the user attribute and root User DN of the main authenticator. For example, for the default authenticator:

uid=%uniquemember%,ou=people,ou=myrealm,dc=bifoundation_domain

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<adapters schvers="303" version="1"
xmlns="http://www.octetstring.com/schemas/Adapters"
xmlns:adapters="http://www.w3.org/2001/XMLSchema-instance">
   <dataBase id="directoryType" version="0">
      <root>%ROOT%</root>
      <active>true</active>
      <serverType>directoryType</serverType>
      <routing>
         <critical>true</critical>
         <priority>50</priority>
         <inclusionFilter/>
         <exclusionFilter/>
         <plugin/>
         <retrieve/>
         <store/>
         <visible>Yes</visible>
         <levels>-1</levels>
         <bind>true</bind>
         <bind-adapters/>
         <views/>
         <dnpattern/>
      </routing>
      <pluginChains
xmlns="http://xmlns.oracle.com/iam/management/ovd/config/plugins">
         <plugins>
            <plugin>
               <name>VirtualAttribute</name>

<class>oracle.ods.virtualization.engine.chain.plugins.virtualattr.VirtualAttrib
utePlugin</class>
               <initParams>
                  <param name="ReplaceAttribute"
value="uniquemember={cn=%uniquemember%,cn=users,dc=oracle,dc=com}"/>
               </initParams>
            </plugin>
         </plugins>
         <default>
            <plugin name="VirtualAttribute"/>
         </default>
         <add/>
         <bind/>
```

```
         <delete/>
         <get/>
         <modify/>
         <rename/>
      </pluginChains>
      <driver>oracle.jdbc.driver.OracleDriver</driver>
      <url>%URL%</url>
      <user>%USER%</user>
      <password>%PASSWORD%</password>
      <ignoreObjectClassOnModify>false</ignoreObjectClassOnModify>
      <includeInheritedObjectClasses>true</includeInheritedObjectClasses>
      <maxConnections>10</maxConnections>
      <mapping>
         <joins/>
         <objectClass name="groupofuniquenames" rdn="cn">
            <attribute ldap="cn" table="GROUPMEMBERS_VW" field="G_NAME"
type=""/>
            <attribute ldap="description" table="GROUPMEMBERS_VW" field="G_
NAME" type=""/>
            <attribute ldap="uniquemember" table="GROUPMEMBERS_VW" field="G_
MEMBER" type=""/>
         </objectClass>
      </mapping>
      <useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
      <connectionWaitTimeout>10</connectionWaitTimeout>
      <oracleNetConnectTimeout>0</oracleNetConnectTimeout>
      <validateConnection>false</validateConnection>
   </dataBase>
</adapters>
```

3. Customize appropriate sections highlighted in bold, for the following elements:

   - ReplaceAttribute

     Specifies how to define the unique member for a group (the %uniquemember% is a placeholder for a value which will be passed in at runtime when looking up whether a user is a member of a group)

     The only aspect of this element you may want to change is the specification of the root for your users. While this is notional, by default it must match whatever you specify as the root of your user population when you run the libovdadapterconfig script in Step 10.

   - groupofuniquenenames

     Specifies how group attributes are mapped to database fields.

     You must map the following attributes:

     – **cn** (map to a unique name for your group)

     – **uniquemember** (map to the unique name for your user in the user/group mapping table in your database schema

     Mapping the following attribute is optional:

     – **description** is optional (although clearly helpful)

     No other attributes are user-configurable.

4. Copy the adapter file into the following folder:

   ORACLE_HOME/oracle_common/modules/oracle.ovd/templates/

5. Open a command prompt/terminal at:

ORACLE_HOME/oracle_common/bin

6. Ensure the following environment variables are set, for example:
   - ORACLE_HOME=oraclehome
   - WL_HOME=*ORACLE_HOME*/wlserver/
   - JAVA_HOME=*ORACLE_HOME*/jdk/jre
7. Run the libovdadapterconfig script to create a database adapter from the template file. The syntax is:

```
libovdadapterconfig -adapterName <name of adapter> -adapterTemplate <name (NOT
including path) of template file which defines adapater> -host localhost -port
<Admin Server port> -userName <user id of account which has administrative
privileges in the domain> -domainPath <path to the BI domain> -dataStore DB
-root <nominal specification of a pseudo-LDAP query to treat as the "root" of
this adapter - must match that specified in template for adapter 2 above>
-contextName default -dataSourceJNDIName <JNDI name for DataSource which points
at the database being mapped>
```

For example:

```
./libovdadapterconfig.sh -adapterName biSQLGroupAdapter -adapterTemplate bi_
sql_groups_adapter_template.xml -host localhost -port 7001 -userName weblogic
-domainPath /opt/oracle_bi/user_projects/domains/bifoundation_domain/
-dataStore DB -root cn=users,dc=oracle,dc=com -contextName default
-dataSourceJNDIName jdbc/BIDatabaseGroupDS
```

Note: The dataSourceJNDIName must be the JNDI name and not just the DS name.

Note: The root parameter value should match the root dn specified in the <param name="replaceattribute" element in the adaptor template. For example, if user is specified in the default authenticator, the root would normally be set to ou=people, ou=myrealm, dc=bifoundation_domain.

The script should exit without error.

8. Restart WebLogic Administration Server and Managed servers.

Note: When you start WebLogic you will see the following warning which you can ignore:

Warning: BISQLGroupsProvider: Connection pool not usable.

You should now be able to log in to WebLogic and Oracle Business Intelligence using credentials stored in the database.

3.4.4.5 Testing the Configuration by Adding a Database Group to an Application Role

To test the configuration by adding a database group to an application role:

1. Log in to Fusion Middleware Control, and open WebLogic domain and bifoundation_domain in the navigation menu on the left of the page.

   For more information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".

2. Right-click bifoundation_domain and select **Security**, then **Application Roles** to display the Application Role Configuration page.

3. Add a database group which contains an LDAP user to one of the application roles (for example, BIServiceAdministrator) which that user does not currently have access to.

4. Log in to Oracle Business Intelligence as a user that is a member of the group that was newly added to the application role.

   In the top right of the page, you will see the text "Logged in as <*user id*>".

5. Click the user id to display a drop down menu.

6. Select **My Account** from the menu.

7. Display the **Roles and Catalog Groups** tab and verify the user now has the new application role.

3.4.4.6 Correcting Errors in the Adaptors

You cannot modify an existing database adapter, so if you make an error in either the libovdadapter command, or the templates you use to create the adapters, you must delete then recreate the adapter.

For more information, see Section 3.4.5.6, "Correcting Database Adapter Errors by Deleting and Recreating the Adapter".

3.4.5 Configuring a Database as the Authentication Provider

This section describes how to configure Oracle Business Intelligence to use a database as the authentication provider by using a SQLAuthenticator and a virtualized identity store database adapter, and contains the following topics:

- Section 3.4.5.1, "Introduction and Prerequisites"
- Section 3.4.5.2, "Creating a Sample Schema for Users and Groups"
- Section 3.4.5.3, "Configuring a Data Source and SQL Authenticator Using the Oracle WebLogic Server Administration Console"
- Section 3.4.5.4, "Configuring the Virtualized Identity Store"
- Section 3.4.5.5, "Troubleshooting the SQL Authenticator"
- Section 3.4.5.6, "Correcting Database Adapter Errors by Deleting and Recreating the Adapter"

3.4.5.1 Introduction and Prerequisites

User role and profile information can be stored in a database with the help of an adapter that enables the database to appear like an LDAP server. A virtualized identity store provider can retrieve user profile information from a database through a database adapter.

The method of database authentication described here is only possible in Release 11.1.1.5 (or higher), because earlier releases require the use of initialization blocks.

This topic explains how to configure Oracle Business Intelligence with a SQLAuthenticator and a virtualized identity store provider (including a database adapter), both running against a suitable database schema. The examples given are illustrative only, and your database schema need not be identical to the sample described here.

Use this procedure when you need to authenticate users against a database schema. The preferred identity store for authentication purposes is an LDAP directory service, such as Oracle Internet Directory (OID LDAP).

The approach to database authentication described here requires two database columns, one containing users and another containing passwords. This method is not based on database user accounts.

Oracle Business Intelligence Enterprise Edition Releases 11.1.1.5, 11.1.1.6, and 11.1.1.7 (or higher) must be installed and running. However, for Releases 11.1.1.5 and 11.1.1.6, you must also apply Oracle Fusion Middleware patch 13826887. For more information, see "Patching Oracle Business Intelligence Systems" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*).

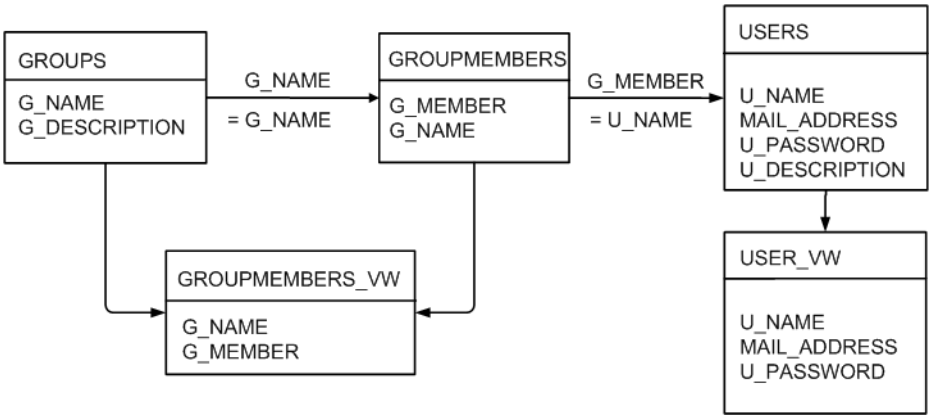
3.4.5.2 Creating a Sample Schema for Users and Groups

In practice, you will have your own schemas, which you are using in an earlier installation of Oracle BI EE. The sample schema described here is deliberately simplistic, and is intended only to illustrate how to configure the system to use the schema.

> **Note:** A suitable database schema containing the users, credentials and groups required for authentication, must be accessible from the WebLogic Server on which Oracle BI EE is running.

Figure 3–5 has tables, USERS, USER_VW, GROUPMEMBERS, GROUPS, and GROUPMEMBERS_VW, where USER_VW is a view on the USERS table, and GROUPMEMBERS_VW is a view joining the GROUPMEMBERS and GROUPS tables.

Figure 3–5 Sample Schema for Users and Groups



If either user or group information exists in more than one table, remove USER_VW must create a view over the tables of each type of information.

Create a view on the GROUPMEMBERS and GROUPS tables (for example, GROUPMEMBERS_VW) with an outer join on the GROUPS table and an inner join on the GROUPMEMBERS table, which enables you to see groups in Fusion Middleware

Control even when they have no user assigned to them. To present the view shown in Figure 3–5 to the database adapter, you would need to follow the configuration shown in Section 3.4.5.4.2, "Configuring a Database Adaptor".

3.4.5.3 Configuring a Data Source and SQL Authenticator Using the Oracle WebLogic Server Administration Console

You configure a data source and SQL authenticator using the Oracle WebLogic Server Administration Console as follows:

- Section 3.4.5.3.1, "Configuring a Data Source Using the Oracle WebLogic Server Administration Console"
- Section 3.4.5.3.2, "Configuring a SQL Authenticator Using the Oracle WebLogic Server Administration Console"

3.4.5.3.1 Configuring a Data Source Using the Oracle WebLogic Server Administration Console

To configure a data source using the Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".
2. Click **Services** in the left pane and click **Data Sources**.
3. In the Summary of Data Sources page, click **New**, and select **Generic Data Source**.
4. In the JDBC Data Sources Properties page, enter or select values for the following properties:
   - **Name** - For example, enter: UserGroupDS

     The name used in the underlying configuration file (config.xml) and throughout the Administration Console whenever referring to this data source.
   - **JNDI Name** - For example, enter: `jdbc/UserGroupDS`

     The JNDI path to which this JDBC data source will be bound.
   - **Database Type** - For example, select: Oracle

     The DBMS of the database that you want to connect to.
5. Click **Next**.
6. Select a database driver from the **Database Driver** drop down list.

   For example, select: Oracle's Driver (Thin) for Service Connections; Releases:9.0.1 and later
7. Click **Next**.
8. Click **Next**.
9. On the Connection Properties page, enter values for the following properties:
   - **Database Name** - For example, enter: `ora12c`

     The name of the database that you want to connect to.
   - **Host Name** - For example, enter: `mymachine.example.com`

     The DNS name or IP address of the server that hosts the database.

- **Port** - For example, enter: `1521`

  The port on which the database server listens for connections requests.

- **Database User Name**

  Typically the schema owner of the tables defined in Section 3.4.5.2

- **Password/Confirm Password**

  The password for the **Database User Name**.

10. Click **Next**.
11. Check the details on the page are correct, and click **Test Configuration**.
12. Click **Next**.
13. In the Select Targets page select the servers or clusters for deploying the data source.

    You should select the Administration Server and Managed server as your targets, for example:

    - In the Servers pane

      Select the **AdminServer** check box.

    - In the Clusters pane

      Select the **bi_server1** option.

14. Click **Finish**.
15. In the Change Center, click **Activate Changes**.
16. Restart the system.

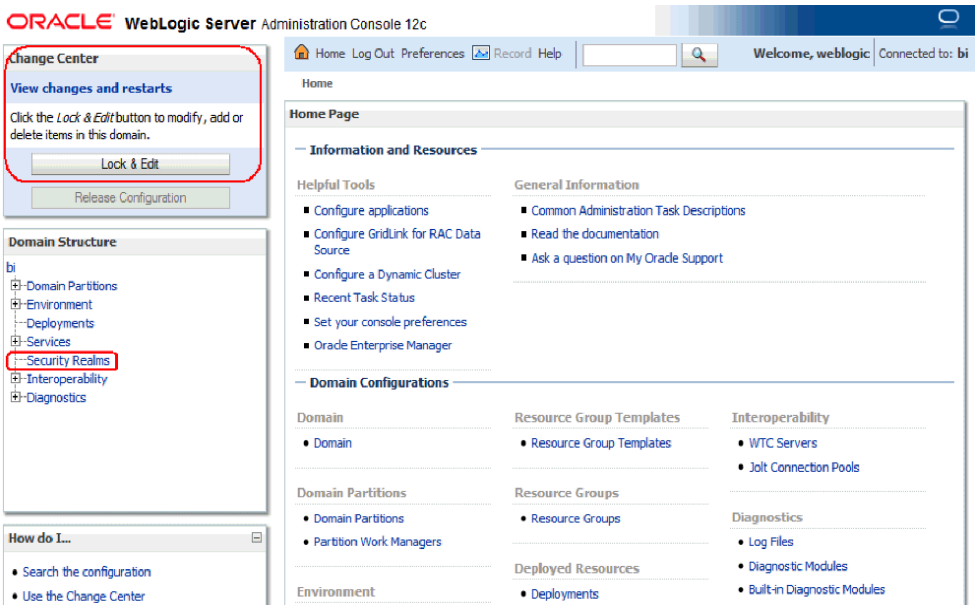
3.4.5.3.2 Configuring a SQL Authenticator Using the Oracle WebLogic Server Administration Console

This task enables a suitably privileged user to log in to the Oracle WebLogic Server Administration Console using the WebLogic database authenticator.

To configure a SQL authenticator using the Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

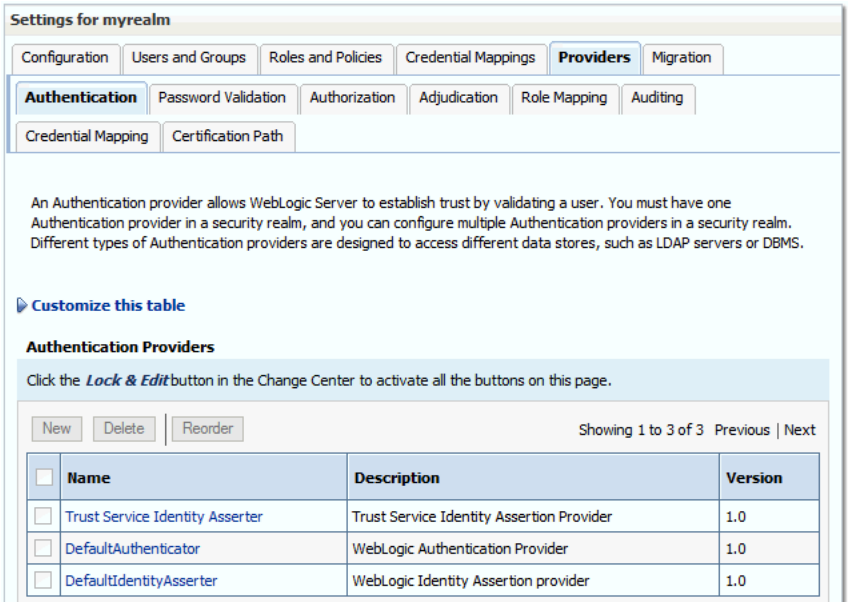
   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".



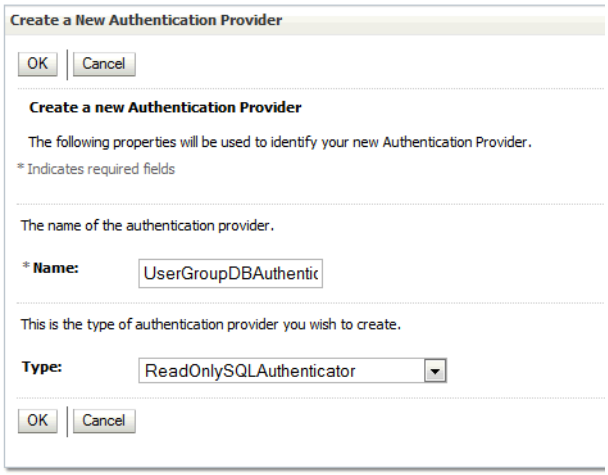
2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

3. Display the **Providers** tab, then display the **Authentication** sub-tab.

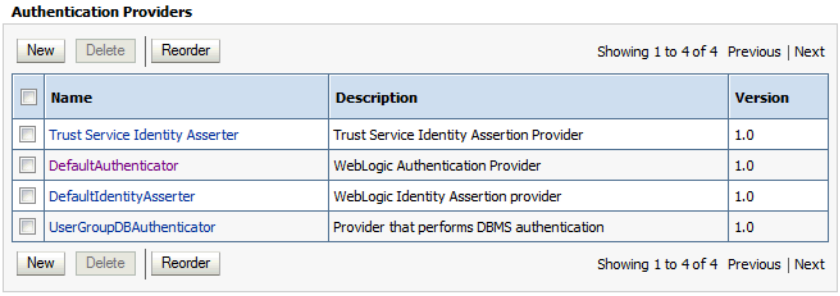


4. Click **New** to launch the **Create a New Authentication Provider** page.



5. Enter values in the **Create a New Authentication Provider** page as follows:
   - **Name**: Enter a name for the authentication provider. For example, UserGroupDBAuthenticator.
   - **Type**: Select ReadOnlySQLAuthenticator from the list.

     This creates a read-only SQL Authenticator, and WebLogic does not write back to the database.
   - Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.



6. In the authentication providers table, click UserGroupDBAuthenticator in the **Name** column to display the Settings page.
7. Display the **Provider Specific** tab, and enter in the **Data Source Name** field, the name of the data source that you created in Section 3.4.5.3.1.

   For example, `UserGroupDS`.
8. In the **Provider Specific** tab you specify the SQL statements used to query, and authenticate against, your database tables.

   Table 3–4 shows SQL statements for the sample schema outlined in Section 3.4.5.2

Table 3–4 SQL Statements for the Sample Schema

Query	SQL	Notes
SQL Get Users Password (used to authenticate)	SELECT U_PASSWORD FROM USERS WHERE U_NAME = ?	The SQL statement used to look up a user's password. The SQL statement requires a single parameter for the username and must return a resultSet containing at most a single record containing the password.
SQL User Exists	SELECT U_NAME FROM USERS WHERE U_NAME = ?	The SQL statement used to look up a user. The SQL statement requires a single parameter for the username and must return a resultSet containing at most a single record containing the user.
SQL List Users	SELECT U_NAME FROM USERS WHERE U_NAME LIKE ?	The SQL statement used to retrieve users that match a particular wildcard search. The SQL statement requires a single parameter for the usernames and returns a resultSet containing matching usernames.
SQL List Groups	SELECT G_NAME FROM GROUPS WHERE G_NAME LIKE ?	The SQL statement used to retrieve group names that match a wildcard. The SQL statement requires a single parameter for the group name and returns a resultSet containing matching groups.
SQL Group Exists	SELECT G_NAME FROM GROUPS WHERE G_NAME = ?	The SQL statement used to look up a group. The SQL statement requires a single parameter for the group name and must return a resultSet containing at most a single record containing the group.
SQL Is Member	SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME=? AND G_MEMBER LIKE ?	The SQL statement used to look up members of a group. The SQL statement requires two parameters: a group name and a member or group name. It must return a resultSet.
SQL List Member Groups	SELECT G_NAME FROM GROUPMEMBERS WHERE G_MEMBER = ?	The SQL statement used to look up the groups a user or group is a member of. The SQL statement requires a single parameter for the username or group name and returns a resultSet containing the names of the groups that matched.
SQL Get User Description (if description supported enabled)	SELECT U_DESCRIPTION FROM USERS WHERE U_NAME = ?	The SQL statement used to retrieve the description of a specific user. The SQL statement requires a single parameter for the username and must return a resultSet containing at most a single record containing the user description.

Table 3–4 (Cont.) SQL Statements for the Sample Schema

Query	SQL	Notes
SQL Get Group Description (if description supported enabled)	SELECT G_DESCRIPTION FROM GROUPS WHERE G_NAME = ?	The SQL statement used to retrieve the description of a group. It is valid only if Descriptions Supported is enabled. The SQL statement requires a single parameter for the group name and must return a resultSet containing at most a single record containing the group description.

Note: If you are using a different table structure, you might need to adapt these SQL statements (table or column names) to your own schema. Also, you should leave the question mark (?) as a runtime query placeholder (rather than hardcode a user or group name).

For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

9. Enter all of the SQL statements appropriate to your Authenticator.

   The SQL is case sensitive.

10. If your password column is in plain text (that is, if the result of the query supplied for the **SQL Get Users Password** column is not hashed or encrypted), select the **Plaintext Password Enabled** option.

    If the **Plaintext Password Enabled** option is cleared, the SQLAuthenticator expects passwords to have been hashed using SHA-1 (default encryption algorithm). For more information on the supported encryption algorithms, see the documentation for the base SQLAuthenticator Mbean PasswordAlgorithm attribute.

11. Click **Save**.

12. Perform the following steps to configure default authenticator **Control Flag** setting:

    a. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab, then select **DefaultAuthenticator** to display its configuration page.

    b. Display the **Configuration\Common** tab and select 'SUFFICIENT' from the **Control Flag** list.

       For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".

    c. Click **Save**.

13. Perform the following steps to reorder the Authentication Providers:

    a. Display the **Providers** tab.

    b. Click **Reorder** to display the **Reorder Authentication Providers** page

    c. Select UserGroupDBAuthenticator and use the arrow buttons to move it into the first position in the list.

    d. Click **OK** to save your changes.

14. In the Change Center, click **Activate Changes**.

15. Restart the Oracle Business Intelligence components (use Fusion Middleware Control once the Administration Server has been restarted), Oracle WebLogic Server, and Managed servers.
16. Follow the steps described in Section 3.5, "Resetting the BI System User Credential" to ensure there is a trusted system user in your database, by replacing the credentials in the Credential store to point to this user's credentials.

    The credentials must be of a suitable user account specified in the database tables that you are trying to configure authentication against.

> **Note:** The screenshot of the Oracle WebLogic Server Administration Console in Section 3.5, shows users in the domain that you will not see until you complete the database configuration steps.

> **Note:** Check the **Users and Groups** tab to confirm that the database users and groups appear there.

3.4.5.4 Configuring the Virtualized Identity Store

Configure the virtualized identity store as follows:

- Section 3.4.5.4.1, "Enabling Virtualization by Configuring the Identity Store"
- Section 3.4.5.4.2, "Configuring a Database Adaptor"

3.4.5.4.1 Enabling Virtualization by Configuring the Identity Store You must configure the identity store to enable virtualization so that more than one Identity Store can be used with the identity store service, and therefore user profile information can be split across different authentication providers (identity stores).

For more information, see Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control".

3.4.5.4.2 Configuring a Database Adaptor You configure a database adaptor to make the database appear like an LDAP server, which enables the virtualized identity store provider to retrieve user profile information from a database using the database adapter.

To configure a database adaptor:

This task shows how to edit and apply adapter templates that specify how to use your database tables as an identity store.

1. Create a file named adapter_template_usergroup1.xml.

   This file describes the mapping of the user table to a virtual LDAP store.
2. Make sure that the file contains the following contents:

> **Note:** You must adapt the section shown in bold, to match the columns in your own table with attributes in the LDAP server. The example given here is for the sample schema that is used throughout Section 3.4.5.

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<adapters schvers="303" version="1"
```

```
xmlns="http://www.octetstring.com/schemas/Adapters"
xmlns:adapters="http://www.w3.org/2001/XMLSchema-instance">
   <dataBase id="directoryType" version="0">
      <root>%ROOT%</root>
      <active>true</active>
      <serverType>directoryType</serverType>
      <routing>
         <critical>true</critical>
         <priority>50</priority>
         <inclusionFilter/>
         <exclusionFilter/>
         <plugin/>
         <retrieve/>
         <store/>
         <visible>Yes</visible>
         <levels>-1</levels>
         <bind>true</bind>
         <bind-adapters/>
         <views/>
         <dnpattern/>
      </routing>
      <pluginChains
xmlns="http://xmlns.oracle.com/iam/management/ovd/config/plugins">
         <plugins>
            <plugin>
               <name>DBGUID</name>

<class>oracle.ods.virtualization.engine.chain.plugins.dbguid.DBGuidPlugin</clas
s>
               <initParams>
                  <param name="guidAtribute" value="orclguid"/>
               </initParams>
            </plugin>
         </plugins>
         <default>
            <plugin name="DBGUID"/>
         </default>
         <add/>
         <bind/>
         <delete/>
         <get/>
         <modify/>
         <rename/>
      </pluginChains>
      <driver>oracle.jdbc.driver.OracleDriver</driver>
      <url>%URL%</url>
      <user>%USER%</user>
      <password>%PASSWORD%</password>
      <ignoreObjectClassOnModify>false</ignoreObjectClassOnModify>
      <includeInheritedObjectClasses>true</includeInheritedObjectClasses>
      <maxConnections>10</maxConnections>
      <mapping>
         <joins/>
         <objectClass name="person" rdn="cn">
            <attribute ldap="cn" table="USER_VW" field="U_NAME" type=""/>
            <attribute ldap="uid" table="USER_VW" field="U_NAME" type=""/>
            <attribute ldap="usernameattr" table="USER_VW" field="U_NAME"
type=""/>
            <attribute ldap="loginid" table="USER_VW" field="U_NAME" type=""/>
            <attribute ldap="description" table="USER_VW" field="U_NAME"
```

```
type=""/>
            <attribute ldap="orclguid" table="USER_VW" field="orclguid"
type=""/>
         </objectClass>
      </mapping>
      <useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
      <connectionWaitTimeout>10</connectionWaitTimeout>
      <oracleNetConnectTimeout>0</oracleNetConnectTimeout>
      <validateConnection>false</validateConnection>
   </dataBase>
</adapters>
```

In this example the section highlighted in bold should be the only section that needs customizing, but the elements should be mapped by matching the attributes/classes used in a virtual LDAP schema with the columns in your database which correspond to them. The virtual schema is the same as that of WebLogic Embedded LDAP, so you can map database columns to any of the attributes shown in Table 3–5.

Table 3–5 Examples of Attributes to Map to Database Columns

Attribute	Example
description	John Doe
cn	john.doe
uid	john.doe
sn	Doe
userpassword	welcome1
displayName	John Doe
employeeNumber	12345
employeeType	Regular
givenName	John
homePhone	650-555-1212
mail	john.doe@example.com
title	Manager
manager	uid=mary.jones,ou=people,ou=myrealm,dc=wc_domain
preferredLanguage	en
departmentNumber	tools
facsimiletelephonenumber	650-555-1200
mobile	650-500-1200
pager	650-400-1200
telephoneNumber	650-506-1212
postaladdress	200 Oracle Parkway
l	Redwood Shores
homepostaladdress	123 Main St., Anytown 12345

3. Use the first, outer element (**<objectClass name="person" rdn="cn">**) to declare mapping of the LDAP objectclass person.

   The cn attribute is used as its RDN (Relative Distinguished Name). The sub-elements then declare which LDAP attributes map to which tables and columns in the database. For example, the line **<attribute ldap="uid" table="USERS" field="USER_ID" type=""/>** maps the USER_ID field of the USER_VW table to the standard LDAP attribute uid (that is, a unique user id for each user).

   Next, you map groups using the same method.

4. Create a file named adapter_template_usergroup2.xml.

   This file describes the mapping of the group table to a virtual LDAP store.

5. Add the following contents to the file:

   You must customize the section shown in bold to match the columns in your own table. The sample content shown here is to match the sample schema that is used throughout this example.

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<adapters schvers="303" version="1"
xmlns="http://www.octetstring.com/schemas/Adapters"
xmlns:adapters="http://www.w3.org/2001/XMLSchema-instance">
    <dataBase id="directoryType" version="0">
      <root>%ROOT%</root>
      <active>true</active>
      <serverType>directoryType</serverType>
      <routing>
         <critical>true</critical>
         <priority>50</priority>
         <inclusionFilter/>
         <exclusionFilter/>
         <plugin/>
         <retrieve/>
         <store/>
         <visible>Yes</visible>
         <levels>-1</levels>
         <bind>true</bind>
         <bind-adapters/>
         <views/>
         <dnpattern/>
      </routing>
      <pluginChains
xmlns="http://xmlns.oracle.com/iam/management/ovd/config/plugins">
         <plugins>
            <plugin>
               <name>VirtualAttribute</name>

<class>oracle.ods.virtualization.engine.chain.plugins.virtualattr.VirtualAttrib
utePlugin</class>
               <initParams>
                  <param name="ReplaceAttribute"
value="uniquemember={cn=%uniquemember%,cn=users,dc=oracle,dc=com}"/>
               </initParams>
            </plugin>
         </plugins>
         <default>
            <plugin name="VirtualAttribute"/>
         </default>
```

```
            <add/>
            <bind/>
            <delete/>
            <get/>
            <modify/>
            <rename/>
         </pluginChains>
         <driver>oracle.jdbc.driver.OracleDriver</driver>
         <url>%URL%</url>
         <user>%USER%</user>
         <password>%PASSWORD%</password>
         <ignoreObjectClassOnModify>false</ignoreObjectClassOnModify>
         <includeInheritedObjectClasses>true</includeInheritedObjectClasses>
         <maxConnections>10</maxConnections>
         <mapping>
            <joins/>
            <objectClass name="groupofuniquenames" rdn="cn">
               <attribute ldap="cn" table="GROUPMEMBERS_VW" field="G_NAME"
type=""/>
              <attribute ldap="description" table="GROUPMEMBERS_VW" field="G_NAME
type=""/>
               <attribute ldap="uniquemember" table="GROUPMEMBERS_VW" field="G_
MEMBER" type=""/>
               <attribute ldap="orclguid" table="GROUPMEMBERS_VW" field="G_NAME"
type=""/>
            </objectClass>
         </mapping>
         <useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
         <connectionWaitTimeout>10</connectionWaitTimeout>
         <oracleNetConnectTimeout>0</oracleNetConnectTimeout>
         <validateConnection>false</validateConnection>
      </dataBase>
</adapters>
```

6. Customize appropriate sections highlighted in bold, for the following elements:

   - ReplaceAttribute

     Specifies how to define the unique member for a group (the %uniquemember% is a placeholder for a value which will be passed in at runtime when looking up whether a user is a member of a group)

     The only aspect of this element you may want to change is the specification of the root for your users. While this is notional, by default it must match whatever you specify as the root of your user population when you run the libovdadapterconfig script in Step 10.

   - groupofuniquenames

     Specifies how group attributes are mapped to database fields and as with the user, the attributes correspond to the defaults in Weblogic Embedded LDAP.

     You must map the following attributes:

     – **cn** (map to a unique name for your group)

     – **uniquemember** (map to the unique name for your user in the user/group mapping table in your database schema)

     – **orclguid** (maps to a unique id, if available in your database schema)

     Mapping the following attributes is optional:

– **description** is optional (although clearly helpful)

No other attributes are user-configurable.

7. Copy the two adapter files into the following folder:

   ORACLE_HOME/oracle_common/modules/oracle.ovd/templates/

8. Open a command prompt/terminal at:

   ORACLE_HOME/oracle_common/bin

9. Ensure the following environment variables are set, for example:
   - ORACLE_HOME=*ORACLE_HOME*/oraclehome
   - WL_HOME=*ORACLE_HOME*/wlserver
   - JAVA_HOME=*ORACLE_HOME*/jdk/jre

10. Run the libovdadapterconfig script to create each of the two adapters from the template files. The syntax is:

```
libovdadapterconfig -adapterName <name of adapter> -adapterTemplate <name (NOT
including path) of template file which defines adapter> -host localhost -port
<Admin Server port> -userName <user id of account which has administrative
privileges in the domain> -domainPath <path to the BI domain> -dataStore DB
-root <nominal specification of a pseudo-LDAP query to treat as the "root" of
this adapter - must match that specified in template for adapter 2 above>
-contextName default -dataSourceJNDIName <JNDI name for DataSource which points
at the database being mapped>
```

For example:

```
./libovdadapterconfig.sh -adapterName userGroupAdapter1 -adapterTemplate
adapter_template_usergroup1.xml -host localhost -port 7001 -userName weblogic
-domainPath /opt/oracle_bi/user_projects/domains/bifoundation_domain/
-dataStore DB -root cn=users,dc=oracle,dc=com -contextName default
-dataSourceJNDIName jdbc/UserGroupDS

./libovdadapterconfig.sh -adapterName userGroupAdapter2 -adapterTemplate
adapter_template_usergroup2.xml -host localhost -port 7001 -userName weblogic
-domainPath /opt/oracle_bi/user_projects/domains/bifoundation_domain/
-dataStore DB -root cn=users,dc=oracle,dc=com -contextName default
-dataSourceJNDIName jdbc/UserGroupDS
```

The scripts should exit without error.

11. Restart WebLogic Administration Server and Managed servers.

    You should now be able to log in to WebLogic and Oracle Business Intelligence using credentials stored in the database

3.4.5.5 Troubleshooting the SQL Authenticator

This section provides troubleshooting information on the SQL authenticator, and contains the following topics:

- Section 3.4.5.5.1, "Adding a User to the Global Admin Role Using the Oracle WebLogic Server Administration Console"
- Section 3.4.5.5.2, "An Incorrect Data Source Name is Specified for the SQLAuthenticator"
- Section 3.4.5.5.3, "Incorrect SQL Queries"

3.4.5.5.1 Adding a User to the Global Admin Role Using the Oracle WebLogic Server Administration Console

If you cannot log in to Oracle Business Intelligence using a database user, a useful diagnostic test is to see whether your user can log in to WebLogic at all. If you do not have other applications on the WebLogic Server which take advantage of WebLogic container authentication, you can add your user (temporarily) to the WebLogic Global Admin role and see if the user can log in to the Oracle WebLogic Server Administration Console to test whether the SQLAuthenticator is working at all.

To add a user to the global admin role using the Oracle WebLogic Server Administration Console:

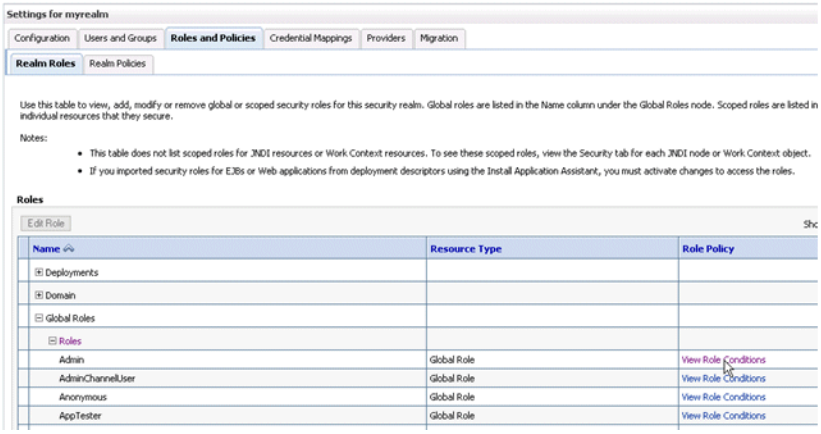
1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

3. Display the **Roles and Policies** tab, then display the **Realm Roles** sub-tab.



4. In the list of roles, click on the plus sign to expand **Global Roles**, then **Roles**, then click the **View Role Conditions** link for the Admin role.

5. Ensure the conditions specified will match your user, either directly, or by belonging to a group.

   For example, a condition may be User=myadminaccount or Group=Administrators.

6. If you have made any changes, click **Save**.

   Changes are applied immediately.

7. You should now be able to check whether the user in question can log in to the Oracle WebLogic Server Administration Console at http://*<bi server address>*:*<AdminServer Port>*/console (for example, http://example.com:9500/console).

   If the user can log in to the console, but cannot log in to Oracle Business Intelligence, the SQLAuthenticator is working correctly, but there may be issues in the identity store service. Check that you have specified the virtualize=true, and OPTIMIZE_SEARCH=true properties in Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control" and that your DBAdapter

templates are correct in Section 3.4.5.4.2, "Configuring a Database Adaptor".

3.4.5.5.2 An Incorrect Data Source Name is Specified for the SQLAuthenticator If you specify the wrong name for the data source field of the SQLAuthenticator, then errors such as the following are included in the log files for Administration Server and Managed Servers:

```
Caused by: javax.security.auth.login.FailedLoginException:
[Security:090761]Authentication failed for user jsmith java.sql.SQLException:
[Security:090788]"Problem with DataSource/ConnectionPool configuration, verify
DataSource name wrongdsname is correct and Pool configurations are correct"
      at weblogic.security.providers.authentication.shared.DBMSAtnLoginModuleI
mpl.login(DBMSAtnLoginModuleImpl.java:318)
```

Use the data source name as in the example shown in Section 3.4.5.3.1, "Configuring a Data Source Using the Oracle WebLogic Server Administration Console".

3.4.5.5.3 Incorrect SQL Queries Ensure that the SQL queries that you specify when configuring the SQLAuthenticator are syntactically correct and refer to the correct tables. For example, the following error occurs in the Administration Server.log file when the wrong table name is specified for the password query:

```
####<Jul 7, 2011 4:03:27 PM BST> <Error> <Security> <gbr20020> <AdminServer>
<[ACTIVE] ExecuteThread: '8' for queue: 'weblogic.kernel.Default (self-tuning)'>
<<WLS Kernel>> <> <de7dd0dc53f3d0ed:e0ce69e:131007c1afe:-8000-00000000000007fa>
<1310051007798> <BEA-000000> <[Security:090759]A SQLException occurred while
retrieving password information
java.sql.SQLSyntaxErrorException: ORA-00942: table or view does not exist
     at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:457)
     at oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:405)
     at oracle.jdbc.driver.T4C8Oall.processError(T4C8Oall.java:889)
     at oracle.jdbc.driver.T4CTTIfun.receive(T4CTTIfun.java:476)
```

3.4.5.6 Correcting Database Adapter Errors by Deleting and Recreating the Adapter

You cannot modify an existing database adapter, so if you make an error in either the libovdadapter command, or the templates you use to create the adapters, you must delete then recreate the adapter using the following procedure.

To correct database adapter errors by deleting and recreating the adapter:

1. Log in to the WLS console by running the WLST script.

   For example:

   ORACLE_HOME/oracle_common/common/bin/wlst.sh (UNIX)

   ORACLE_HOME\oracle_common\common\bin\wlst.cmd (Windows)

2. Connect to your Administration Server using the following syntax:

   connect ('<*WLS admin user name*>','<*WLS admin password*>','t3://<*admin server host*>:<*admin server port*>')

   For example:

   ```
   connect('weblogic','weblogic','t3://myserver:9500')
   ```

3. Delete the misconfigured adapter using the following syntax:

   deleteAdapter(adapterName='<*AdapterName*>')

For example:

```
deleteAdapter(adapterName='userGroupAdapter2')
```

4. Exit the WLST console using the command exit() and recreate the adapter with the correct settings by following the steps outlined in Section 3.4.5.4.2, "Configuring a Database Adaptor".

3.4.6 Configuring Identity Store Virtualization Using Fusion Middleware Control

This section describes how to configure Oracle Business Intelligence to use Identity Store Virtualization using Fusion Middleware Control.

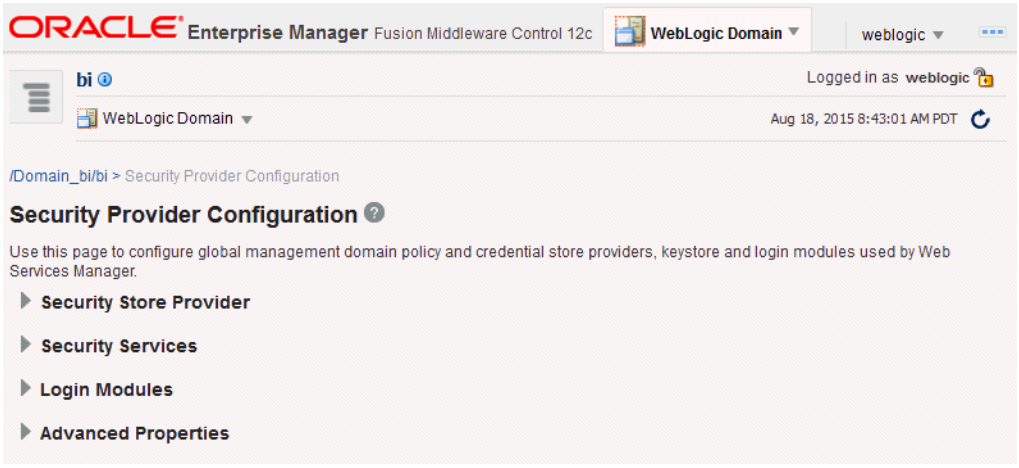
To configure identity store virtualization using Fusion Middleware Control:

If you are communicating with LDAP over SSL (one-way SSL only), see Section 5.14.2, "Configuring SSL when Using Multiple Authenticators".

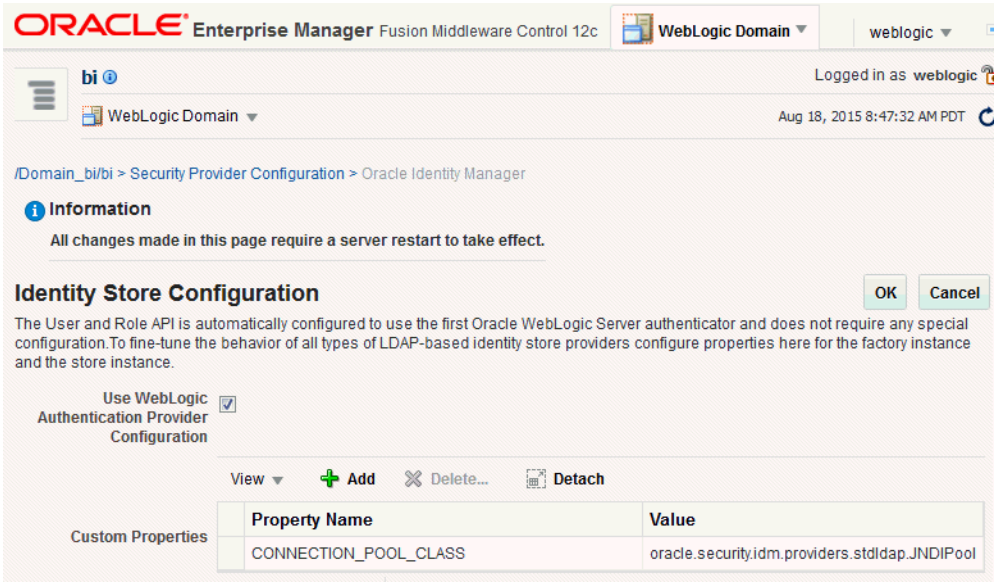
For more information, see .

1. (Optional) If not already done, configure supported authentication providers as described in Section 3.4.
2. Log in to Fusion Middleware Control.

   For more information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".
3. From the navigation pane expand the **WebLogic Domain** folder and select **bi**.
4. Right-click bi and select Security, then Security Provider Configuration to display the Security Provider Configuration page.



5. Expand Security Store Provider and Identity Store Provider, and click **Configure** to display the Identity Store Configuration page.



6. In the Custom Properties area, use the **Add** option to add the following custom properties:

   - Property Name=`virtualize`

     Value=`true`

   - Property Name=`OPTIMIZE_SEARCH`

     Value=`true`

   Note: The Property Name `virtualize` must be lowercase, and OPTIMIZE_SEARCH must be uppercase.

   Note: If you are using multiple authentication providers, go to Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers" and configure the **Control Flag** setting as follows:

   - If each user appears in only one authentication provider.

     Set the value of **Control Flag** for all authentication providers to SUFFICIENT.

   - If users appear in more than one authentication provider.

     Set the value of **Control Flag** for all authentication providers to OPTIONAL.

     For example, if a user's group membership is spread across more than one authentication provider

7. Click **OK** to save the changes.
8. Restart the Administration Server and Managed Servers.

3.4.7 Configuring Multiple Authentication Providers so that When One Fails, Users from Others can Still Log In to Oracle Business Intelligence

If you configure Oracle Business Intelligence to use multiple authentication providers, and one authentication provider becomes unavailable, users from the other authentication providers cannot log in to Oracle Business Intelligence. This section explains how to configure an authentication provider so that when it fails, users from other authentication providers can still log in to Oracle Business Intelligence. For more information, see Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control").

When you cannot log in due to an authentication provider becoming unavailable, the following error message is displayed:

```
Unable to Sign In
An error occurred during authentication.
Try again later or contact your system administrator
```

If there is a possibility that one authenticator (from multiple configured authenticators) might become unavailable, and is not critical, use the following procedure to enable users from other authenticators to log in to Oracle Business Intelligence.

To configure multiple authentication providers so that when one fails, users from other authentication providers can still log in to Oracle Business Intelligence:

1. Open the file adapters.os_xml for editing.

   For example, on Windows, the file is located in:

   ORACLE_HOME\user_projects\domains\bi\config\fmwconfig\ovd\default

2. Locate the following element in the file:

   ```
   <critical>true</critical>>
   ```

   Change the value of the <critical> element to `false` in the adapters.os_xml file for each authenticator provider that is not critical, as follows:

   ```
   <critical>false</critical>
   ```

3. Save and close the file.

4. Restart WebLogic Administration Server and Managed Servers.

3.4.8 Setting the JAAS Control Flag Option

When you configure multiple authentication providers, use the JAAS Control Flag for each provider to control how the authentication providers are used in the login sequence. You can set the JAAS Control Flag in the Oracle WebLogic Server Administration Console. For more information, See "Set the JAAS control flag" in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*. You can also use the WebLogic Scripting Tool or Java Management Extensions (JMX) APIs to set the JAAS Control Flag for an authentication provider.

Setting the Control Flag attribute for the authenticator provider determines the ordered execution of the authentication providers. The possible values for the Control Flag attribute are:

- REQUIRED - This LoginModule must succeed. Even if it fails, authentication proceeds down the list of LoginModules for the configured Authentication providers. This setting is the default.

- REQUISITE - This LoginModule must succeed. If other Authentication providers are configured and this LoginModule succeeds, authentication proceeds down the list of LoginModules. Otherwise, control is returned to the application.
- SUFFICIENT - This LoginModule need not succeed. If it does succeed, return control to the application. If it fails and other Authentication providers are configured, authentication proceeds down the LoginModule list.
- OPTIONAL - This LoginModule can succeed or fail. However, if all Authentication providers configured in a security realm have the JAAS Control Flag set to OPTIONAL, the user must pass the authentication test of one of the configured providers.

When additional Authentication providers are added to an existing security realm, by default the Control Flag is set to OPTIONAL. If necessary, change the setting of the Control Flag and the order of Authentication providers so that each Authentication provider works properly in the authentication sequence.

3.4.9 Configuring a Single LDAP Authentication Provider as the Authenticator

This topic explains how to reconfigure Oracle Business Intelligence to use a single LDAP authentication provider, by disabling the default WebLogic Server LDAP authenticator.

When you install Oracle Business Intelligence, the system is automatically configured to use WebLogic Server LDAP as the default authenticator. The install process will automatically generate the required users and groups in WebLogic Server LDAP. However, you may have your own LDAP directory (for example Oracle Internet Directory) that you may want to use as the default authenticator, and disable the WebLogic Server default authenticator. Having a single source authentication provider prevents user names and passwords being derived from multiple authentication sources, which could lead to multiple points of attack, or entry from unauthorizeed users.

This topic contains the following sections:

3.4.9.1 Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator

The examples shown in this section are for configuring Oracle Internet Directory (OID LDAP) but could easily apply to other LDAP authentication providers by using minor changes.

To configure Oracle Internet Directory LDAP authentication as the only authenticator:

- "Task 1 - Enable Backup and Recovery"
- "Task 2 - Configure the System to use WebLogic Server and an Alternative Authentication Provider"
- "Task 3 - Identify or Create Essential Users Required in OID LDAP"
- "Task 4 - Associate OID LDAP Groups with Global Roles in the WebLogic Console"
- "Task 5 - Set User to Group Membership in OID LDAP"

- "Task 6 - Remove the Default Authenticator"
- "Task 7 - Restart the BI Services"
- "Task 8 - Remove WebLogic Server Roles"
- "Task 9 - Stop Alternative Methods of Authentication"

3.4.9.1.1 Task 1 - Enable Backup and Recovery Before you begin the process of disabling the WebLogic Server LDAP default method of authentication it is strongly recommended that you back up the system first. Otherwise, if you make an error during configuration you may find that you become locked out of the system or cannot restart it.

To enable backup and recovery, during the re-configuration phase, take a copy of the config.xml file in *ORACLE_HOME*\user_projects\domains\bi\config directory.

As you make changes it is advised that you keep copies of this file.

3.4.9.1.2 Task 2 - Configure the System to use WebLogic Server and an Alternative Authentication Provider To remove the default WebLogic Server authenticators and use an alternative LDAP source (for example, OID LDAP), you must configure the system to use both WebLogic Server and the alternative method. For more information, see Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers". Your starting point should be that the WebLogic Server LDAP users (default authenticator) and the new alternative LDAP users are both configured to allow access to Oracle Business Intelligence.

When you have configured the system to enable you to log on as either a WebLogic Server LDAP user or an OID LDAP user, you can then proceed to follow the steps to remove the WebLogic Server default authenticator, as described in these tasks.

3.4.9.1.3 Task 3 - Identify or Create Essential Users Required in OID LDAP You must ensure that the essential users shown in Table 3–6 are migrated from WebLogic Server LDAP to OID LDAP.

Table 3–6 Essential Users Required in OID LDAP

Standard WebLogic Server Users	New Users Required in OID LDAP
LCMManager,User	OID_LCMManagerUser (this can be any existing OID LDAP user)
For example, weblogic	OID_Weblogic (this can be any existing OID LDAP user)
OracleSystemUser	OracleSystemUser (this user must exist with this name in OID LDAP, which is a fixed requirement of OWSM)

Three users are created during install:

- weblogic (or whatever is specified during install or upgrade, so can be different).

  This administrator user is created during the install (sometimes called weblogic, but can have any name). You need to identify or create an equivalent user in OID LDAP but this user can have any name, which needs to be part of a group called Administrators.

- OracleSystemUser

This user is specifically required (by Oracle Web Services Manager - OWSM) for the Global Roles mapping, and you must create this user in OID LDAP using this exact name.

3.4.9.1.4 Task 4 - Associate OID LDAP Groups with Global Roles in the WebLogic Console The global role mappings shown in Table 3–7 must be configured in OID LDAP.

Table 3–7 Global Role Mapping in WebLogic Admin Console

Global Roles	Current WebLogic Server Groups	New OID LDAP Groups Required
Admin	Administrators	OID_Administrators
AdminChannelUsers	AdminChannelUsers	OID_AdminChannelUsers
AppTester	AppTesters	OID_AppTesters
CrossDomainConnector	CrossDomainConnectors	OID_CrossDomainConnectors
Deployer	Deployers	OID_Deployers
Monitor	Monitors	OID_Monitors
Operator	Operators	OID_Operators
OracleSystemRole	OracleSystemGroup	OracleSystemGroup (fixed requirement)

You must associate the global roles from Table 3–7 (displayed in the WebLogic Server Admin Console) with your replacement OID LDAP groups, before you can disable the default WebLogic Server authenticator.

To associate OID LDAP groups with global roles in Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.

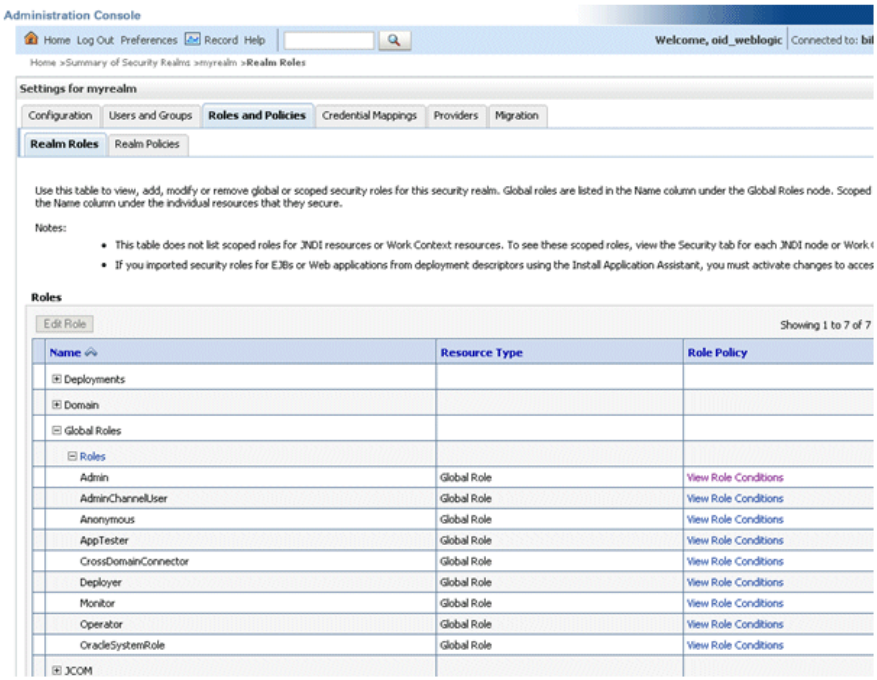
   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

3. Click **Realm Roles**.

4. Click **Global Roles** and expand **Roles**.



5. Add a new condition for each Role as follows:

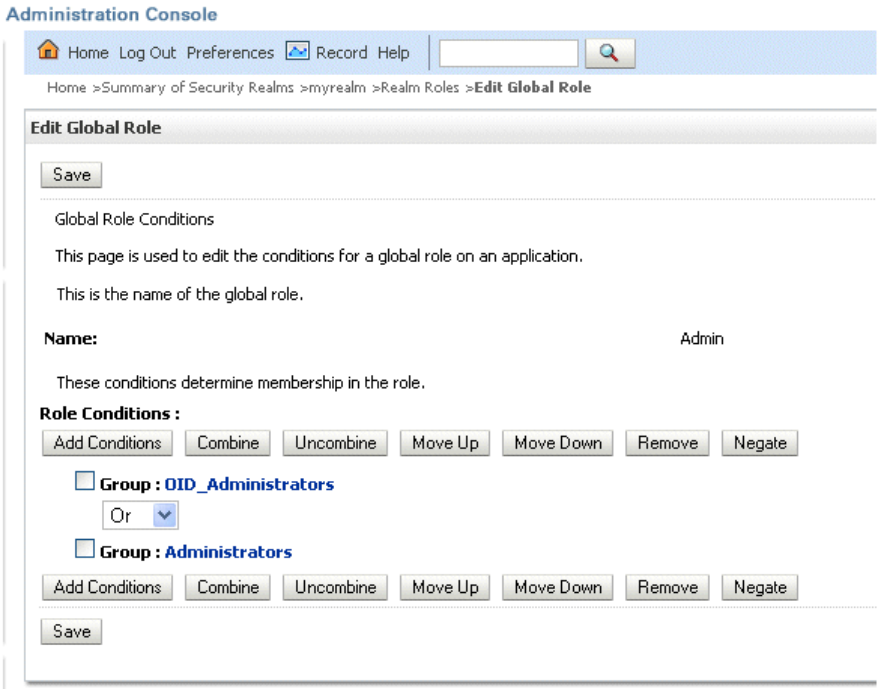
> **Note:** Do not do add a new condition for the Anonymous and Oracle System roles, which can both remain unchanged.

   a. Click View Role Conditions.

   b. Select group from the **Predicate List** drop down.

   c. Enter your newly-associated OID LDAP group from Table 3–7.

      For example, assign the Admin role to the OID_Administrators role.



Note: Once you have successfully disable the Default WebLogic Server Authentication you can return here and remove the old WebLogic Server groups (for example, here you would remove Group: Administrators). For more information, see Task 8 - Remove WebLogic Server Roles.

d. Save your changes.

3.4.9.1.5 Task 5 - Set User to Group Membership in OID LDAP Now that you have created new users and groups in OID LDAP to replicate the users and groups automatically created in WebLogic Server LDAP you must ensure that these users and groups also have the correct group membership in OID LDAP as shown in Table 3–8.

Table 3–8 User to Group Membership Required in OID LDAP

New OID LDAP User	Is A Member Of These New OID LDAP Groups
OID_Weblogic	OID_Administrators OID_BIServiceAdministrators
OracleSystemUser **Note:** A user with this exact name must exist in OID LDAP.	OracleSystemGroup **Note:** A group with this exact name must exist in OID LDAP

Note: In order to achieve the user and group membership shown in Table 3–8 you must have suitable access to update your OID LDAP server, or someone else must be able to update group membership on your behalf.

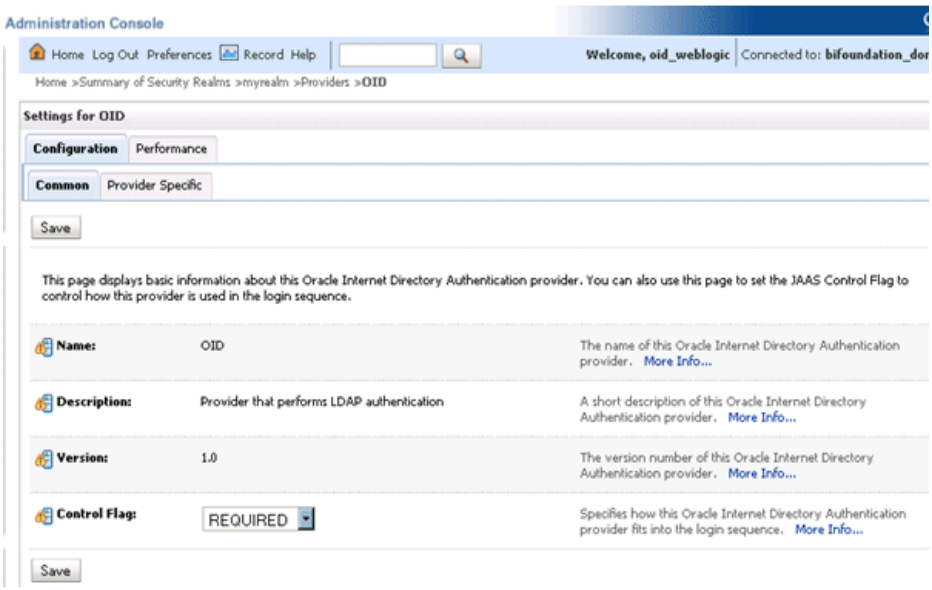
3.4.9.1.6 Task 6 - Remove the Default Authenticator You are now ready to remove the Default Authenticators.

To remove the default authenticators:

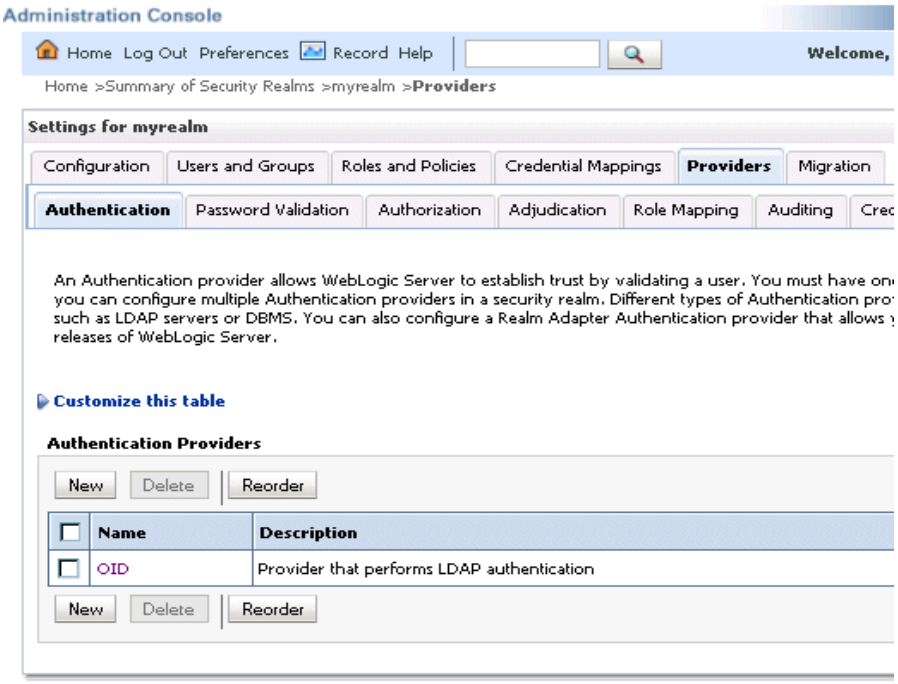
You must have first created an LDAP authenticator that maps to your LDAP source (for more information, see Task 2 - Configure the System to use WebLogic Server and an Alternative Authentication Provider).

1. Change the **Control Flag** from SUFFICIENT to REQUIRED in the Oracle WebLogic Server Administration Console.

   For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".



2. Save the changes.
3. Delete any other authenticators so that your OID LDAP authenticator is the single source.



3.4.9.1.7 Task 7 - Restart the BI Services Now you are ready to restart the BI services. You must use the new OID administrator user (for example, OID_Weblogic), because the WebLogic Server administration user created during installation was removed, and users now exist in the single OID source. The OID administration user must have sufficient privileges (granted by the Global Admin role) to start WebLogic.

> **Note:** When you log in to the Administration Tool online you must now provide the OID LDAP user and password (for example, OID_Weblogic) along with the repository password.

3.4.9.1.8 Task 8 - Remove WebLogic Server Roles Complete this task if everything is working correctly.

> **Note:** Back up your config.xml, now, before performing this step (see Task 1 - Enable Backup and Recovery)

To remove all automatically created WebLogic server roles from the OR clause:

1. Edit global roles.

   For more information, see Task 4 - Associate OID LDAP Groups with Global Roles in the WebLogic Console.

2. Remove all WebLogic Server roles that were automatically created, from the OR clause.

   For example:

   - Admin
   - AdminChannelUsers
   - AppTester

- CrossDomainConnector
- Deployer
- Monitor
- Operator

3. Save your changes.

3.4.9.1.9 Task 9 - Stop Alternative Methods of Authentication

Oracle Business Intelligence allows various forms of authentication methods to be applied at once. While some can see this as a desirable feature it also comes with security risks. To implement a single source of authentication, you must remove the authentication methods that use initialization blocks from the Metadata Repository.

To stop all initialization block authentication access:

You stop access through initialization blocks using the Oracle BI Administration Tool. Successful authentication requires a user name, and initialization blocks populate user names using the special system session variable called USER.

1. Remove the USER System Variable from the Metadata Repository.
2. Ensure that initialization blocks in the Metadata Repository have the **Required for authentication** check box cleared.
3. Check that initialization blocks in the Metadata Repository that set the system session variables PROXY and PROXYLEVEL do not allow users to bypass security.

   The system variables PROXY and PROXYLEVEL allow connected users to impersonate other users with their security profile. This method is acceptable when the impersonated user account has less privileges, but if the account has more privileges it can be a security issue.

Caution: If you disable an initialization block, then any dependent initialization blocks will also be disabled.

You can now be sure that any attempted access using initialization block authentication cannot be successful. However, you must check all of your initialization blocks.

3.4.9.2 Troubleshooting

You might receive the following error after you have configured Oracle Internet Directory LDAP authentication as the single source:

```
<Critical> <WebLogicServer> <BEA-000386> <Server subsystem failed.

Reason: weblogic.security.SecurityInitializationException: User
<oidweblogic> is not permitted to boot the server. The server policy may
have changed in such a way that the user is no longer able to boot the
server. Reboot the server with the administrative user account or contact
the system administrator to update the server policy definitions.
```

Solution

If when you restart the system as the new WebLogic OID LDAP administrator (oidweblogic), you are locked out, and the message is displayed, it is because the oidweblogic user has insufficient privileges. The oidweblogic user requires the Admin global role to enable it to belong to an OID LDAP Administrator group. You resolve this issue by adding the BIServiceAdministrators group (or an OID LDAP equivalent) to the Admin global role.

Note: To restore a previously working configuration, you must replace the latest updated version of the config.xml file with a backup version that you have made before changing the configuration (for more information, see Task 1 - Enable Backup and Recovery).

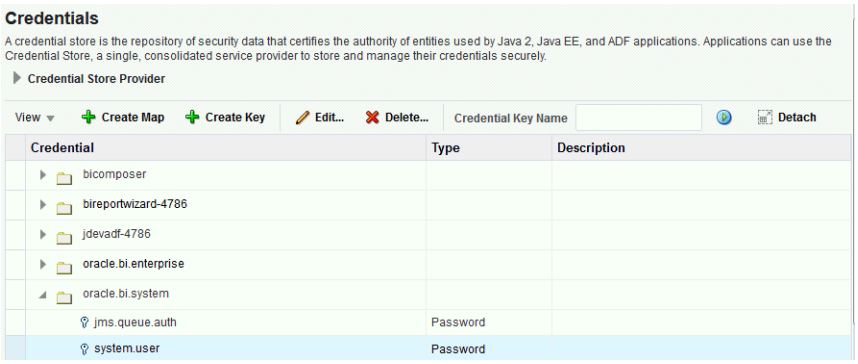
To complete the restoration of the backup config.xml file, restart Oracle Business Intelligence as the original WebLogic administrator user, instead of as the OID LDAP user.

3.5 Resetting the BI System User Credential

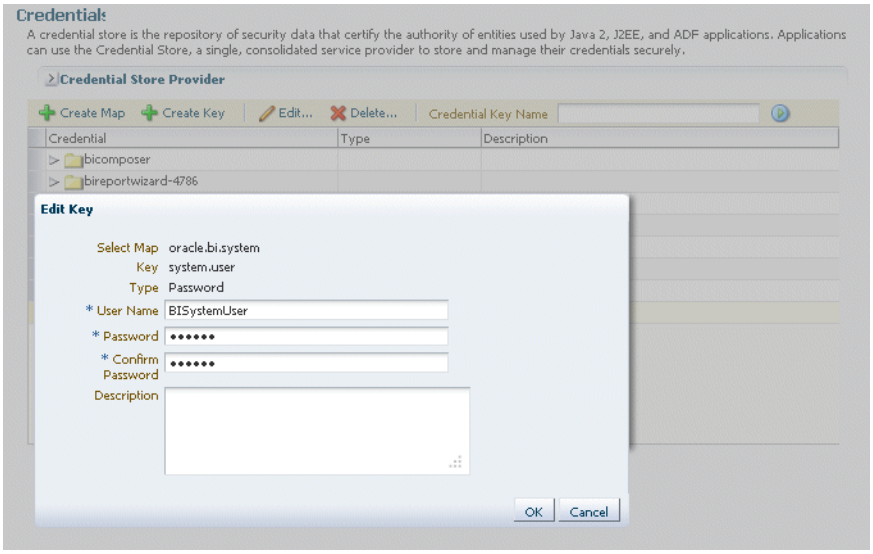
In 11*g* a user called BISystemUser was created in the embedded WebLogic LDAP, but in 12*c* this user no longer exists and has been replaced with a single credential. This credential is populated with securely-generated random values at BI domain creation time and is stored in the Credential Store. If at any time you need to reset the user name or password of this credential, follow these steps.

To reset the BI System User credential:

1. From the Fusion Middleware Control target navigation pane, expand the farm, then expand **WebLogic Domain**, and select **bi**.
   - From the WebLogic Domain menu, select **Security**, then **Credentials**.
   - Open the **oracle.bi.system** credential map, select **system.user** and click **Edit**.



   - In the **Edit Key** dialog, update the user name or password as required. Ensure that these values do not match the credentials of a user in your Identity Store.



- Click **OK**.

2. Restart the system

4

Enabling SSO Authentication

This chapter provides some general guidelines for configuring single sign-on (SSO) authentication for Oracle Business Intelligence.

> **Note:** For a detailed list of security setup steps, see Section 1.7, "Detailed List of Steps for Setting Up Security in Oracle Business Intelligence".

This chapter contains the following topics:

- SSO Configuration Tasks for Oracle Business Intelligence
- Understanding SSO Authentication and Oracle Business Intelligence
- SSO Implementation Considerations
- Configuring SSO in an Oracle Access Manager Environment
- Configuring Custom SSO Environments
- Configuring SSO With SmartView
- Enabling Oracle Business Intelligence to Use SSO Authentication
- Enabling the Online Catalog Manager to Connect

> **Note:** Oracle recommends using Oracle Access Manager as an enterprise-level SSO authentication provider with Oracle Fusion Middleware. Section 4.2, Section 4.3, and Section 4.4 assume that Oracle Access Manager is the SSO authentication provider. Section 4.5 references alternative authentication providers in custom SSO environment solutions.
>
> For more information about configuring and managing Oracle Access Manager with Oracle Fusion Middleware, see "Introduction to Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Application Security Guide*.
>
> For more information about supported SSO providers, see "System Requirements and Certification".

4.1 SSO Configuration Tasks for Oracle Business Intelligence

Table 4–1 contains SSO authentication configuration tasks and provides links for obtaining more information.

Table 4–1 Task Map: Configuring SSO Authentication for Oracle Business Intelligence

Task	Description	For More Information
Configure Oracle Access Manager as the SSO authentication provider.	Configure Oracle Access Manager to protect the Oracle Business Intelligence URL entry points.	Section 4.4, "Configuring SSO in an Oracle Access Manager Environment" "Configuring Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Application Security Guide*
Configure the HTTP proxy.	Configure the web proxy to forward requests from Presentation Services to the SSO provider.	"Configuring Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Application Security Guide*
Configure a new authenticator for Oracle WebLogic Server.	Configure the Oracle WebLogic Server domain in which Oracle Business Intelligence is installed to use the new identity store.	Section 4.4.1, "Configuring a New Authenticator for Oracle WebLogic Server" Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers" *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*
Configure a new identity asserter for Oracle WebLogic Server.	Configure the Oracle WebLogic Server domain in which Oracle Business Intelligence is installed to use the SSO provider as an asserter.	Section 4.4.2, "Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server" Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers" *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*
Configure custom SSO solutions.	Configure alternative custom SSO solutions to protect the Oracle Business Intelligence URL entry points.	Section 4.5, "Configuring Custom SSO Environments"
Enable Oracle Business Intelligence to accept SSO authentication.	Enable the SSO provider configured to work with Oracle Business Intelligence.	Section 4.7, "Enabling Oracle Business Intelligence to Use SSO Authentication"

Note: For an example of an Oracle Business Intelligence SSO installation scenario, see *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

4.2 Understanding SSO Authentication and Oracle Business Intelligence

Integrating a single sign-on (SSO) solution enables a user to log on (sign-on) and be authenticated once. Thereafter, the authenticated user is given access to system components or resources according to the permissions and privileges granted to that user. Oracle Business Intelligence can be configured to trust incoming HTTP requests

authenticated by a SSO solution that is configured for use with Oracle Fusion Middleware and Oracle WebLogic Server. For more information about configuring SSO for Oracle Fusion Middleware, see "Configuring Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Application Security Guide*.

When Oracle Business Intelligence is configured to use SSO authentication, it accepts authenticated users from whatever SSO solution Oracle Fusion Middleware is configured to use. If SSO is not enabled, then Oracle Business Intelligence challenges each user for authentication credentials. When Oracle Business Intelligence is configured to use SSO, a user is first redirected to the SSO solution's login page for authentication. After the user is authenticated the SSO solution forwards the user name to Presentation Services where this name is extracted. Next a session with the BI Server is established using the impersonation feature (a connection string between the Oracle BI Presentation Server and the BI Server using credentials that act on behalf of a user being impersonated).

After successfully logging in using SSO, users are still required to have the oracle.bi.server.manageRepositories permission to log in to the Administration Tool using a valid user name and password combination. After installation, the oracle.bi.server.manageRepositories permission is granted by being a member of the default BIAdministration application role.

Configuring Oracle Business Intelligence to work with SSO authentication requires minimally that the following be done:

- Oracle Fusion Middleware and Oracle WebLogic Server are configured to accept SSO authentication. Oracle Access Manager is recommended in production environments.
- Oracle BI Presentation Services is configured to trust incoming messages.
- The HTTP header information required for identity propagation with SSO configurations (namely, user identity and SSO cookie) is specified and configured.

4.2.1 How an Identity Asserter Works

This section describes how Oracle Access Manager authentication provider works with Oracle WebLogic Server using Identity Asserter for single sign-on, providing the following features:

- **Identity Asserter for Single Sign-on**

  This feature uses the Oracle Access Manager authentication services and validates already-authenticated Oracle Access Manager users through a suitable token and creates a WebLogic-authenticated session. It also provides single sign-on between WebGate and portals. WebGate is a plug-in that intercepts web resource (HTTP) requests and forwards them to the Access Server for authentication and authorization.

- **Authenticator**

  This feature uses Oracle Access Manager authentication services to authenticate users who access an application deployed in Oracle WebLogic Server. Users are authenticated based on their credentials, for example a user name and password.

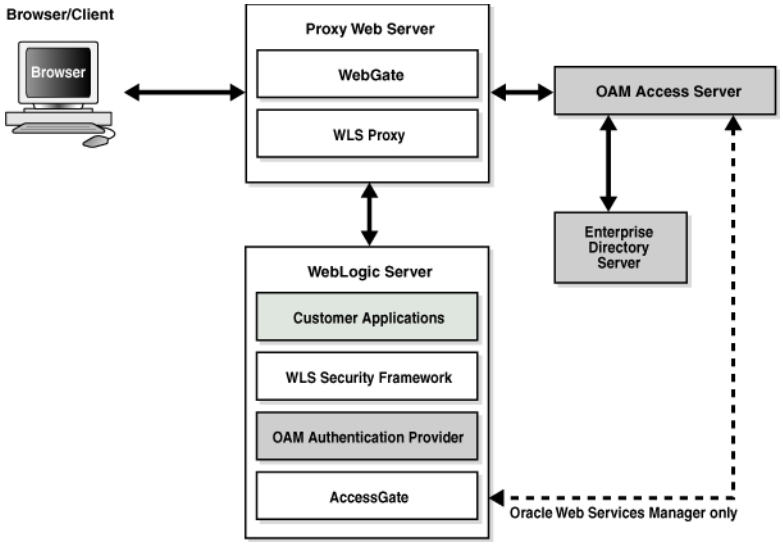
After the authentication provider for Oracle Access Manager is configured as the Identity Asserter for single sign-on, the web resources are protected. Perimeter authentication is performed by WebGate on the web tier and by the appropriate token to assert the identity of users who attempt access to the protected WebLogic resources.

All access requests are routed to a reverse proxy web server. These requests are in turn intercepted by WebGate. The user is challenged for credentials based on the authentication scheme configured within Oracle Access Manager (form-based login recommended).

After successful authentication, WebGate generates a token and the web server forwards the request to Oracle WebLogic Server, which in turn invokes Oracle Access Manager Identity Asserter for single sign-on validation. Oracle Access Manager is able to pass various types of heading token, the simplest being an HTTP header called OAM_REMOTE_USER containing the user ID that has been authenticated by Oracle Access Manager. The WebLogic Security Service invokes Oracle Access Manager Identity Asserter for single sign-on, which next gets the token from the incoming request and populates the subject with the WLSUserImpl principal. The Identity Asserter for single sign-on adds the WLSGroupImpl principal corresponding to the groups the user is a member of. Oracle Access Manager then validates the cookie.

Figure 4–1 depicts the distribution of components and the flow of information when the Oracle Access Manager Authentication Provider is configured as an Identity Asserter for SSO with Oracle Fusion Middleware.

Figure 4–1 Oracle Access Manager Single Sign-On Solution for Web Resources Only



4.2.2 How Oracle Business Intelligence Operates with SSO Authentication

After SSO authorization has been implemented, Presentation Services operates as if the incoming web request is from a user authenticated by the SSO solution. Presentation Services next creates a connection to the BI Server using the impersonation feature and establishes the connection to the BI Server on behalf of the user. User personalization and access controls such as data-level security are maintained in this environment.

4.3 SSO Implementation Considerations

When implementing a SSO solution with Oracle Business Intelligence you should consider the following:

- When accepting trusted information from the HTTP server or servlet container, it is essential to secure the machines that communicate directly with Presentation Services. This can be done by setting the Listener\Firewall node in the

instanceconfig.xml file with the list of HTTP Server or servlet container IP addresses. Additionally, the Firewall node must include the IP addresses of all Oracle Business Intelligence Scheduler instances, Oracle BI Presentation Services Plug-in instances, and Oracle Business Intelligence JavaHost instances. If any of these components are co-located with Oracle BI Presentation Services, then address 127.0.0.1 must be added in this list as well. This setting does not control end-user browser IP addresses.

- When using mutually-authenticated SSL, you must specify the Distinguished Names (DNs) of all trusted hosts in the Listener\TrustedPeers node.

4.4 Configuring SSO in an Oracle Access Manager Environment

For information about how to configure Oracle Access Manager as the SSO authentication provider for Oracle Fusion Middleware with WebLogic Server, see "Configuring Single Sign-On in Oracle Fusion Middleware" in *Oracle Fusion Middleware Application Security Guide*. For more information about managing Oracle Access Manager, see *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager*.

For information about how to configure Oracle BI Publisher to use Oracle Access Manager as the SSO authentication provider, see "Configuring BI Publisher to Use Oracle Access Manager (OAM) Single Sign-On" in *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*.

After the Oracle Fusion Middleware environment is configured, in general the following must be done to configure Oracle Business Intelligence:

- Configure the SSO provider to protect the Oracle Business Intelligence URL entry points.
- Configure the web server to forward requests from Presentation Services to the SSO provider.
- Configure the new identity store as the main authentication source for the Oracle WebLogic Server domain in which Oracle Business Intelligence has been installed. For more information, see Section 4.4.1, "Configuring a New Authenticator for Oracle WebLogic Server".
- Configure the Oracle WebLogic Server domain in which Oracle Business Intelligence is installed to use an Oracle Access Manager asserter. For more information, see Section 4.4.2, "Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server".
- After configuration of the SSO environment is complete, enable SSO authentication for Oracle Business Intelligence. For more information, see Section 4.7.2, "Enabling SSO Authentication Using Fusion Middleware Control".

4.4.1 Configuring a New Authenticator for Oracle WebLogic Server

After installing Oracle Business Intelligence, the Oracle WebLogic Server embedded LDAP server is the default authentication source (identity store). To use a new identity store (for example, OID), as the main authentication source, you must configure the Oracle WebLogic Server domain (where Oracle Business Intelligence is installed).

For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

To configure a new authenticator in Oracle WebLogic Server:

1. Log in to Oracle WebLogic Server Administration Console and click **Lock & Edit** in the Change Center.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

3. Display the **Providers** tab, then display the **Authentication** sub-tab.

4. Click **New** to launch the **Create a New Authentication Provider** page.

   Complete the fields as follows:

   - **Name**: *OID Provider*, or a name of your choosing.
   - **Type**: OracleInternetDirectoryAuthenticator
   - Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.

5. Click the newly added authenticator in the **authentication providers** table.

6. Navigate to **Settings**, then select the **Configuration****Common** tab:

   - Select **SUFFICIENT** from the **Control Flag** list.
   - Click **Save**.

7. Display the **Provider Specific** tab and specify the following settings using appropriate values for your environment:

Section Name	Field Name	Description
Connection	Host	The LDAP host name. For example, <*localhost*>.
Connection	Port	The LDAP host listening port number. For example, 6050.
Connection	Principal	The distinguished name (DN) of the user that connects to the LDAP server. For example, cn=orcladmin.
Connection	Credential	The password for the LDAP administrative user entered as the Principal.
Users	User Base DN	The base distinguished name (DN) of the LDAP server tree that contains users. For example, use the same value as in Oracle Access Manager.
Users	All Users Filter	The LDAP search filter. For example, (&(uid=*) (objectclass=person)). The asterix (*) filters for all users. Click More Info... for details.
Users	User From Name Filter	The LDAP search filter. Click More Info... for details.

Section Name	Field Name	Description
Users	User Name Attribute	The attribute that you want to use to authenticate (for example, cn, uid, or mail). Set as the default attribute for user name in the directory server. For example, *uid* . **Note**: The value that you specify here must match the User Name Attribute that you are using in the authentication provider, as described in the next task Section 3.4.3.1, "Configuring User Name Attributes".
Groups	Group Base DN	The base distinguished name (DN) of the LDAP server tree that contains groups (same as User Base DN).
General	GUID attribute	The attribute used to define object GUIDs in LDAP. orclguid **Note**: You should not change this default value, in most cases the default value here is sufficient.

For more information about configuring authentication providers in Oracle WebLogic Server, see *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

8. Click **Save**.
9. Perform the following steps to set up the default authenticator for use with the Identity Asserter:
   a. At the main **Settings for myrealm** page, display the **Providers** tab, then display the **Authentication** sub-tab, then select **DefaultAuthenticator** to display its configuration page.
   b. Display the **Configuration\Common** tab and select 'SUFFICIENT' from the **Control Flag** list.

      For more information, see Section 3.4.8, "Setting the JAAS Control Flag Option".
   c. Click **Save**.
10. Perform the following steps to reorder Providers:
    a. Display the **Providers** tab.
    b. Click **Reorder** to display the **Reorder Authentication Providers** page
    c. Select a provider name and use the arrow buttons to order the list of providers as follows:
       - OID Authenticator (SUFFICIENT)
       - OAM Identity Asserter (REQUIRED)
       - Default Authenticator (SUFFICIENT)
    d. Click **OK** to save your changes.
11. In the Change Center, click **Activate Changes**.
12. Restart Oracle WebLogic Server.

4.4.2 Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server

The Oracle WebLogic Server domain in which Oracle Business Intelligence is installed must be configured to use an Oracle Access Manager asserter.

For more information about creating a new asserter in Oracle WebLogic Server, see *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

To configure Oracle Access Manager as the new asserter for Oracle WebLogic Server:

1. Log in to Oracle WebLogic Server Administration Console.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm you are configuring. For example, **myrealm**. Select **Providers**.

3. Click **New**. Complete the fields as follows:

   - **Name**: *OAM Provider*, or a name of your choosing.
   - **Type**: OAMIdentityAsserter.

4. Click **OK**.

5. Click **Save**.

6. In the **Providers** tab, perform the following steps to reorder **Providers**:

   a. Click **Reorder**

   b. In the **Reorder Authentication Providers** page, select a provider name, and use the arrows beside the list to order the providers as follows:

      – OID Authenticator (SUFFICIENT)

      – OAM Identity Asserter (REQUIRED)

      – Default Authenticator (SUFFICIENT)

   c. Click **OK** to save your changes.

7. In the Change Center, click **Activate Changes**.

8. Restart Oracle WebLogic Server.

   You can verify that Oracle Internet Directory is the new identity store (default authenticator) by logging back into Oracle WebLogic Server and verifying the users and groups stored in the LDAP server appear in the console.

9. Enable SSO authentication.

   For more information, see Section 4.7, "Enabling Oracle Business Intelligence to Use SSO Authentication".

4.5 Configuring Custom SSO Environments

For information about configuring Oracle Business Intelligence to participate in custom SSO environments (for example, setting up SSO using Active Directory or SiteMinder), see articles 1274953.1, 1287479.1 on My Oracle Support at:

`https://support.oracle.com`

4.6 Configuring SSO With SmartView

For information about configuring SSO with SmartView when Oracle Business Intelligence is SSO enabled with Active Directory and Native Authentication, see article 1900485.1 on My Oracle Support at:

https://support.oracle.com

4.7 Enabling Oracle Business Intelligence to Use SSO Authentication

After you configure Oracle Business Intelligence to use the SSO solution, you must enable SSO authentication for Oracle Business Intelligence.

After you enable SSO, the default Oracle Business Intelligence login page is not available.

- Section 4.7.1, "Enabling and Disabling SSO Authentication Using WLST Commands"
- Section 4.7.2, "Enabling SSO Authentication Using Fusion Middleware Control"

4.7.1 Enabling and Disabling SSO Authentication Using WLST Commands

This section describes how to enable or disable SSO authentication for Oracle Business Intelligence using WLST commands.

Assumptions:

- You must have file system and WebLogic Administrator permissions.
- This is an offline activity.
- Validation is limited to URL format, no connectivity or WebLogic configuration is validated.
- Changing the logoff-URL requires re-enablement (disable, then enable with new URL).
- Logon URL is not required.

Pre-requisites:

- Configure WebLogic security providers (see "Configuring WebLogic Security Providers" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*).

To enable or disable SSO authentication using WLST commands:

1. Stop the BI system.

   For example on UNIX use:

   ./stop.sh

2. Enter a SSO management command from Table 4–2 using the WLST command line.

   For more information, see "Using the WebLogic Scripting Tool (WLST)" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Table 4–2 SSO Management Commands

Command	Arguments	Return	Description
enableBISingleSignOn	DOMAIN_HOME <logoff-url>	None	Enable SSO and configure logoff URL.
disableBISingleSignOn	DOMAIN_HOME	None	Disable SSO.

3. The SSO configuration for Oracle Business Intelligence is updated.
4. Restart the Oracle Business Intelligence component processes to consume the changes.

   For example on UNIX use:

   ./start.sh

   For more information, see "Starting Oracle Business Intelligence Component Processes" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

4.7.2 Enabling SSO Authentication Using Fusion Middleware Control

This section describes how to enable SSO authentication for Oracle Business Intelligence using the **Security** tab in Fusion Middleware Control.

To enable SSO authentication in Fusion Middleware Control:

1. Log in to Fusion Middleware Control.

   For information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".
2. Go to the **Security** page and display the **Single Sign On** tab.

   Click the **Help for this page** Help menu option to access the page-level help for its elements.
3. Click **Lock and Edit**.
4. Select **Enable SSO**.

   When selected, this checkbox enables SSO to be the method of authentication into Oracle Business Intelligence. The appropriate form of SSO is determined by the configuration settings made for the chosen SSO provider.
5. Select the configured SSO provider from the list.

   The **SSO Provider** list becomes active when you select the **Enable SSO** checkbox.

   If you select 'Custom' from the **SSO Provider** list, then the system will not overwrite the changes you make to the <Authentication> section of the instanceconfig.xml file. Instead, you can manually edit this section of the instanceconfig.xml file.
6. If required, enter logon and logoff URLs for the configured SSO provider.

   The logoff URL (specified by the SSO provider) must be outside the domain and port that the SSO provider protects, because the system does not log users out.
7. Click **Apply**, then **Activate Changes**.
8. Restart the Oracle Business Intelligence components using Fusion Middleware Control.

For more information, see "Starting and Stopping the Oracle Business Intelligence Components" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

4.8 Enabling the Online Catalog Manager to Connect

The online Catalog Manager might fail to connect to Oracle BI Presentation Services when the HTTP web server for Oracle Business Intelligence is enabled for SSO. When you enable SSO in Section 4.7.2, "Enabling SSO Authentication Using Fusion Middleware Control", the Oracle Business Intelligence URL http://*hostname:port_number*/analytics becomes protected, and you must point the online Catalog Manager to the URL http://*hostname:port_number*/analytics-ws instead. The URL should remain unprotected. It is configured only to accept SOAP access as used by Oracle BI Publisher, Oracle BI Add-in for Microsoft Office, and the online Catalog Manager.

To log in to the online Catalog Manager when SSO is enabled you must change the URL suffix to point to analytics-ws/saw.dll.

5

Configuring SSL in Oracle Business Intelligence

This chapter describes how to configure Oracle Business Intelligence components to communicate over the Secure Socket Layer (SSL).

> **Note:** For a detailed list of security setup steps, see Section 1.7, "Detailed List of Steps for Setting Up Security in Oracle Business Intelligence".

The SSL Everywhere feature of Oracle Business Intelligence enables secure communications between the components. You can configure SSL communication between the Oracle Business Intelligence components and between Oracle WebLogic Server for secure HTTP communication across your deployment. This section does not cover configuring secure communications to external services, such as databases and web servers. For information about how to configure SSL for Oracle WebLogic Server, see "SSL Configuration in Oracle Fusion Middleware" in *Oracle Fusion Middleware Administrator's Guide*.

This chapter contains the following sections:

- Enabling BI Composer to Launch in an SSL Environment

5.1 What is SSL?

SSL is a cryptographic protocol that enables secure communication between applications across a network. Enabling SSL communication provides several benefits, including message encryption, data integrity, and authentication. An encrypted message ensures confidentiality in that only authorized users have access to it. Data integrity ensures that a message is received intact without any tampering. Authentication guarantees that the person sending the message is who he or she claims to be.

SSL requires that the server possess a public key and a private key for session negotiation. The public key is made available through a server certificate signed by a certificate authority. The certificate also contains information that identifies the server. The private key is protected by the server.

This section contains the following topics:

- Section 5.1.1, "Using SSL in Oracle Business Intelligence"
- Section 5.1.2, "Creating Certificates and Keys in Oracle Business Intelligence"

For more information about SSL concepts and public key cryptography, see "How SSL Works" in *Oracle Fusion Middleware Administrator's Guide*.

5.1.1 Using SSL in Oracle Business Intelligence

Oracle Business Intelligence components communicate with each other using TCP/IP by default. Configuring SSL between the Oracle Business Intelligence components enables secured network communication.

Oracle Business Intelligence components can communicate only through one protocol at a time. It is not possible to use SSL between some components, while using simple TCP/IP communications between others. To enable secure communication, all instances of the following Oracle Business Intelligence components must be configured to communicate over SSL:

- Oracle BI Server
- Oracle BI Presentation Services
- Oracle BI JavaHost
- Oracle BI Scheduler
- Oracle BI Job Manager
- Oracle BI Cluster Controller
- Oracle BI Server Clients, such as Oracle BI ODBC Client

SSL is configured throughout the Oracle Business Intelligence installation from a single centralized point. Certificates are created for you and every Oracle Business Intelligence component (except Essbase) is configured to use SSL. The following default security level is configured by SSL:

- SSL encryption is enabled.
- Mutual SSL authentication is not enabled. Since mutual SSL authentication is not enabled, clients do not need their own private SSL keys.

- The default cipher suites are used. For information about how to use a non-default cipher suite, see Section 5.13, "Manually Configuring SSL Cipher Suite".
- When scaling out, the centrally managed SSL configuration is automatically propagated to any new components that are added.

If a higher level of security is required, manual configuration might be used to augment or replace the SSL central configuration. This is considerably more complex. For more information about how to configure SSL manually, contact Oracle Support. For more information, see Documentation Accessibility.

5.1.2 Creating Certificates and Keys in Oracle Business Intelligence

Secure communication over SSL requires certificates signed by a certificate authority (CA). For internal communication, the SSL Everywhere feature creates both a private certificate authority and the certificates for you. The internal certificates cannot be used for the outward facing web server because user web browsers are not aware of the private certificate authority. The web server must therefore be provided with a web server certificate signed by an externally recognized certificate authority.

5.2 Enabling End-to-End SSL

To achieve end to end SSL you need to configure both internal BIEE SSL and WebLogic SSL. The internal SSL configuration is highly automated whereas the WebLogic SSL configuration requires multiple manual steps. The two are entirely independent, so can be performed in either order. Since the WebLogic configuration requires manual steps Oracle advises doing that first.

Note: This section does not include configuring SSL for Essbase.

Perform the following steps. Confirmation steps are highlighted:

- Section 5.2.1, "Configuring a Standard Non-SSL BIEE System"
- Section 5.2.2, "Configuring WebLogic SSL"

5.2.1 Configuring a Standard Non-SSL BIEE System

To configure a standard non-SSL Oracle Business Intelligence system:

- Install BIEE.
- Confirm the system is operational.

  Check you can login over http to use:

  – Analytics

    - http://<Host>:< ManagedServerPort >/analytics

  – Fusion Middleware Control

    - http://<Host>:< AdminPort>/em

  – WebLogic Admin Console

    - http://<Host>:<AdminPort>/console

5.2.2 Configuring WebLogic SSL

These steps configure WebLogic using the provided demo certificates. These are not secure. They must not be used in a production environment. Nevertheless configuring with demo certificates first is a useful familiarization exercise prior to configuring with real certificates.

To configure with a secure certificate signed by a real Certificate Authority see WebLogic documentation. The certificate authority should return the signed server certificate, and provide a corresponding root CA certificate. Where ever democa is mentioned in these steps replace with your real CA certificate.

This section contains the following topics:

5.2.2.1 Starting Only the Administration Server

To start only the admin server:

Starting up just the Administration Server rather than starting everything avoids the need to stop everything while the admin connection properties are in a state of flux, which confuses the stop everything script.

1. Stop everything with:

   <DomainHome>/bitools/bin/stop.sh

2. Start up just the admin server with:

   <DomainHome>/bitools/bin/start.sh -i Adminserver

5.2.2.2 Configuring HTTPS Ports

To configure HTTPs Ports:

1. Login to WebLogic Admin console.
2. Click **Lock and Edit**.
3. Select environment, servers.

   For each server:

   a. On the main Configuration tab, select **SSL Listen Port Enabled**.

   b. Click **Save**.

   c. Click **Activate Changes**.

4. Enable trust of demo certificates in your browser:

   If you are using WebLogic demo certificates your browser will not trust the WebLogic server. You will need to enable trust in your browser. If using a standard

Certificate Authority whose certificates are trusted by default by your browser then you can omit this step.

a. Go to URL https://<host>:<AdminServerSSLPort>

   Note that this is the base URL, with no em or console on the path. By first accessing the base URL you can set up a single browser certificate exception. If you go directly to the em and console paths you will have to setup multiple certificate exceptions.

   Your browser will warn you about the demo certificate.

b. Enable the certificate exception by going to the base URL.

   You only have to do this once, rather than separately for WebLogic console and Fusion Middleware Control.

   The base URL should give a 404 error once the ssl connection is made. This is fine.

5. Check the secure WebLogic console URL:

   https://<Host>:<AdminServerSSLPort>/console

6. Check the secure Fusion Middleware Control URL:

   https://<Host>:<AdminServerSSLPort>/em

   Do not disable HTTPs yet. You will run a script later that needs to access the Admin Server using the non-SSL port.

   Note: HTTPs check should be in existing browser already logged into Fusion Middleware Control using HTTP.

7. Enabling secure replication:

   a. In WebLogic Admin Console:

      Click **Lock and Edit**.

   b. Select Environment, Clusters, and bi_cluster.

   c. Select Configuration, and the Replication tab. '

   d. Select **secure replication enabled**.

      If you do not do this, the managed servers will fail to startup, remaining in admin mode. This prevents the start scripts from running.

   e. Click **Save**.

   f. Click **Activate Changes**.

5.2.2.3 Configuring Internal WebLogic Server LDAP to Use LDAPs

If an external Identity Store has already been configured omit this step. You may later wish to configure the external identity store to use a secure connection. The steps to do that depend on the type of external identity store.

The internal LDAP ID Store must have its URL amended.

> **Note:** This section only applies when using WebLogic Server LDAP and when virtualize=true is not set, as you are explicitly pointing the Adminserver.

To configure internal LDAPs to use HTTPs:

1. Login to Fusion Middleware Control 12c:

   https://<Host>/<SecureAdminPort>/em
2. Select WebLogic Domain, Security, Security Provider Configuration.
3. Expand the **Identity Store Provider** segment.
4. Click **Configure**.
   a. Click the plus symbol (+) to add a new property.
   b. Add a property ldap.url, with the value:

      ldaps://<host>:<adminServer HTTPS port>.

      For example:

      ldaps://example_machine.com:9501

      Note: This is the admin server address, not the bi_server1 address.
   c. Click **OK** in the property editor.
5. Click **OK** in the Identity Store Provider page.
6. Confirm that the change has been made.
   a. Open the jps-config.xml file located in:

      <DomainHome>/config/fmwconfig/jps-config.xml.
   b. Check the file contains the line:

      <property name="ldap.url"
      value="ldaps://<Host>:<AdminServerSecurePort>"/>

5.2.2.4 Configuring Internal WebLogic Server LDAP Trust Store

You must now provide a trust keystore.

For a full description see: "One-way SSL in a Multi-LDAP Scenario" in *Oracle Fusion Middleware Application Security Guide.*

Note: This section only applies when using WebLogic Server LDAP and when virtualize=true is set, as you are explicitly pointing the Adminserver.

To configure the internal LDAP trust store:

1. In a terminal window set the environment variables ORACLE_HOME and WL_HOME.

   For example, on Linux:

   setenv ORACLE_HOME <OracleHome>

   setenv WL_HOME <OracleHome>/wlserver/
2. Ensure that both your path and JAVA_HOME point to the JDK 8 installation.

   setenv JAVA_HOME <path_to_your_jdk8>

   setenv PATH $JAVA_HOME/bin
3. Check the java version by running:

java -version

4. Run (without the line breaks):

   <OracleHome>/oracle_common/bin/libovdconfig.sh

   -host <Host>

   -port <AdminServerNonSSLPort>

   -userName <AdminUserName>

   -domainPath <DomainHome>

   -createKeystore

   When prompted enter the existing password for <AdminUserName>.

   When prompted for the OVD Keystore password, choose a new password. You will need this later.

   For example:

```
oracle_common/bin/libovdconfig.sh -host myhost -port 7001 -userName weblogic
-domainPath /OracleHome/user_projects/domains/bi -createKeystore

Enter AdminServer password:
Enter OVD Keystore password:
OVD config files already exist for context: default
CSF credential creation successful
Permission grant already available for context: default
OVD MBeans already configured for context: default
Successfully created OVD keystore.
```

   Note: The -port <AdminServerNonSSL> command does not work against the Admin server non-SSL port when it has been disabled. If you enable SSL and then configure LDAPs you would need to temporarily re-enable the non-SSL port on the Adminserver.

5. Check the resultant keystore exists, and see its initial contents, by running:

   keytool -list -keystore
   <DomainHome>/config/fmwconfig/ovd/default/keystores/adapters.jks

6. We now need to export the demo certificate in a suitable format to import into the above keystore.

   In Fusion Middleware Control:

   If using the demo WebLogic certificate you can get the required root CA from the system keystore using Fusion Middleware Control.

   a. Select WebLogicDomain, Security, Keystore.

   b. Expand System.

   c. Select Trust.

   d. Click Manage.

   e. Select democa (NOT olddemoca).

   f. Click Export.

   g. Select export certificate.

   h. Choose a file name.

For example, demotrust.pem

If not using the demo WebLogic certificate then you will need to obtain the root CA of the CA which singed your secure server certificate.

7. Now import into the just created keystore:

```
keytool -importcert -keystore
<DomainHome>/config/fmwconfig/ovd/default/keystores/adapters.jks -alias
localldap -file <DemoTrustFile>
```

8. When prompted enter the keystore password you chose earlier, and confirm that the certificate is to be trusted.
9. If you repeat the keystore -list command you should see a new entry under localldap, for example:

```
localldap, Jul 8, 2015, trustedCertEntry,
```

Certificate fingerprint (SHA1):

```
CA:61:71:5B:64:6B:02:63:C6:FB:83:B1:71:F0:99:D3:54:6A:F7:C8
```

5.2.2.5 Disable HTTP

The system is only fully secure if in addition to HTTPS being enabled we also disable HTTP.

To disable HTTP:

1. Login to WebLogic Admin console.
2. Click **Lock & Edit**.
3. Select environment, servers.

   For each server:

   a. Display the Configuration tab

   b. Clear **Listen Port Enabled**.

   c. Click **Save**.
4. Click **Activate Changes**.

5.2.2.6 Restart

To restart Oracle Business Intelligence:

1. Stop the Administration Server from within WebLogic Admin console.

   Everything should now be stopped.
2. Use the <DomainHome>/bitools/bin/start.sh script to start everything.

   You won't yet be able to login through Analytics since Oracle Web Service Manager (OWSM) is still using the disabled HTTP port.
3. Confirm that HTTP is disabled by logging into both the HTTP and HTTPs WebLogic console URLs. Only the HTTPs one should work.

   HTTP should quickly display an 'Unable to connect error' (the wording varies with the browser). Be careful not to mix the protocols and ports. The browser may hang when attempting to connect to a running port with the wrong protocol.

5.2.2.7 Configure OWSM to Use t3s

You must now change the Oracle Web Services Manager (OWSM) configuration to use the HTTPs port.

To configure OWSM to use t3s:

1. Login to Fusion Middleware Control 12*c*.

   https://<Host>/<SecureAdminPort>/em).

2. Select WebLogic domain, and cross component wiring, components.
3. Select component type, OWSM agent.
4. Select the row owsm-pm-connection-t3 status 'Out of Sync', and click 'Bind'.

   The HTTP(s) OWSM link is not used when using a local OWSM.

5. Select **Yes** in the pop-up box.
6. Confirm by accessing the policy via the validator:

   https://<host>:<ManagedServerSSLPort>/wsm-pm/validator

5.2.2.8 Restart System

To restart Oracle Business Intelligence:

1. Stop all servers using the <DomainHome>/bitools/bin/stop.sh script.

   Everything should now be stopped.

2. Use the <DomainHome>/bitools/bin/start.sh script to start everything.
3. Confirm that you can login to Analytics at:

   https://<Host>:<SecureManagedServerPort>/analytics

   The WebLogic tier is now using HTTPs only for its outward facing ports and therefore for all WebLogic infrastructure. The internal BI channel and BI system components are still using HTTP.

5.3 Enabling BIEE Internal SSL

This section describes how to enable SSL on internal communication links.

To enable BIEE internal SSL:

You must run commands from the master host. Oracle Business Intelligence must have been configured by the BI configuration assistant, WebLogic managed servers must have been created, and any scaling out must be complete.

1. Stop the system using:

   ORACLE_HOME/user_projects/domains/bi/bitools/bin/stop.sh

2. Run the following command to enable SSL on WebLogic internal channels and internal components:

   ORACLE_HOME/user_projects/domains/bi/bitools/bin/ssl.sh internalssl true

3. (Optional) Configure advanced options by editing the file:

   ORACLE_HOME/user_
   projects/domains/bi/config/fmwconfig/biconfig/core/ssl/bi-ssl.xml

   Options supported are:

- Enable server checking of client certificates.
- Specify cipher suite to use.

  For more information, see "Manually Configuring SSL Cipher Suite".

4. Restart the domain and BI component processes using:

   ORACLE_HOME/user_projects/domains/bi/bitools/bin/start.sh

5. Confirm setup as follows:

   a. Check WebLogic certificates and corresponding trust have been correctly configured using:

      ORACLE_HOME/user_projects/domains/bi/bitools/bin/ssl.sh report

      This command checks that WebLogic certificates and corresponding trust are correctly configured.

   b. Confirm you can login to Analytics at:

      https://<host>:<SecureManagedServerPort>/analytics

      This confirms the HTTPs listener is enabled on each server, before you enable end-to-end SSL. Note that any communication between internal components is encrypted, but is only verifiable using 'ssl.sh report' command, or by checking server traffic.

Post conditions:

- WebLogic servers:
  - Have https listener enabled on internal channels.
  - The external port configuration is unaltered. See "Enabling End-to-End SSL" for how to enable SSL on the external ports as well.

    There is a separate internal identity (key/certificate pair) for each listener address. The certificate has a common name matching the listening address, which is compatible with standard https practice. The certificates are signed by the internal certificate authority.
- System components (other than Essbase Studio):
  - Have https listener enabled on internal channels.
  - The external port configuration is unaltered. See "Enabling End-to-End SSL" for how to enable SSL on the external ports as well.
  - There is a separate internal identity (key or certificate pair) for each listener address. The certificate has a common name matching the listening address, which is compatible with standard https practice. The certificates are signed by the internal certificate authority.
- Essbase Studio:
  - No change. Continues with existing connectivity.

5.4 Disabling Internal SSL

This section describes how to disable SSL on internal communication links.

To disable BIEE internal SSL:

You must run commands from the master host. Oracle Business Intelligence must have been configured by the BI configuration assistant, WebLogic managed servers must have been created, and any scaling out must be complete.

1. Stop the system using:

   <*DomainHome*>/bitools/bin/stop.sh

2. Run the following command to enable SSL on WebLogic internal channels and internal components:

   <*DomainHome*>/ bitools/bin/ssl.sh internalssl false

3. Restart the domain using:

   <*OracleHome*>/bi/bin/start.sh

Post conditions:

- WebLogic servers:
  - Have https listener disabled on internal channels.
  - The external port configuration is unaltered.
- System components (other than Essbase Studio):
  - Only listens on non SSL. SSL connections are not accepted.
- Essbase Studio:
  - No change. Continues with existing connectivity.

5.5 Exporting Trust and Identity for Clients

You can provide the keys and certificates required to allow Oracle BI EE clients (for example the Administration Tool, and Job Manager) to connect to SSL-enabled servers.

Assumptions:

- You run commands from master host.
- You can complete this operation online and offline.

Prerequisites

- Certificates are created using either the configuration assistant or by running ./ssl.sh regenerate command.
- SSL on WebLogic is enabled (Section 5.2.2, "Configuring WebLogic SSL").
- The system can be stopped or running.

To export trust and identity for clients:

Use the following command to export client identity and trust to 'mydir':

```
./ssl.sh exportclientcerts mydir
```

Note certificates and zip file are generated.

Post Conditions

- Mydir contains zip file clientcerts.zip
- Mydir also contains expanded content of the zip file for immediate use:
  - clientcert.pem

  - clientkey.pem
  - identity.jks
  - internaltrust.jks
  - internaltrust/internalca.pem
  - internaltrust/<hashed form of above>
- java clients such as Job Manager can successfully connect with secure option 'verify server certificate' set using identity.jks to define identity, and internaltrust.jks for their trust.
- openssl clients such as the Administration Tool can successfully connect with secure option 'verify peer' set using clientcert.pem and clientkey.pem to define their identity, and internalca.pem as the trust file.

5.6 Configuring SSL for Clients

Clients accessing the BIEE components must be configured to use BIEE certificates.

Note: First you must export the certificates by running the following command:

```
<DomainHome>/bitools/bin/ssl.sh exportclientcerts <exportDir>
```

This section explains how to configure SSL for clients, and contains the following topics:

5.6.1 Exporting Client Certificates

First you must export the client certificates.

To export the client certificates:

1. Run the following command:

   ```
   <DomainHome>/bitools/bin/ssl.sh exportclientcerts <exportDir>
   ```

2. When prompted enter a new passphrase.

   The passphrase is used to protect the export certificates. You must remember this passphrase for use when configuring each client.

The command exports Java keystores for use by Java clients, and individual certificate files for use non Java clients. To make moving the certificates to a remote machine more convenient, the export also packages all the files into a single zip file.

5.6.2 Using SASchInvoke when BI Scheduler is SSL-Enabled

When the BI Scheduler is enabled for communication over SSL, you can invoke the BI Scheduler using the SASchInvoke command line utility.

To invoke the BI Scheduler when SSL-enabled using the SASchInvoke utility:

1. Create a new text file containing on a single line the passphrase you used when running the ./ssl.sh exportclientcerts command (see Section 5.6.1, "Exporting Client Certificates").

   Ensure this file has appropriately restrictive file permissions to protect it. Typically it should only be readable by the owner.

2. Use the following syntax to run the SASchInvoke command:

   ```
   SASchInvoke -u <Admin Name>  (-j <job id> | -i <iBot path>)  [-m <machine
   name>[:<port>]]  [(-r <replace parameter filename> | -a <append parameter
   filename>)] [-l [ -c <SSL certificate filename> -k <SSL certificate private key
   filename> [ -w <SSL passphrase>  | -q <passphrase file>  | -y ]] [-h <SSL
   cipher list>] [-v [-e <SSL verification depth>] [-d <CA certificate directory>]
   [-f <CA certificate file>] [-t <SSL trusted peer DNs>] ] ]

   where:
   SSL certificate filename = clientcert.pem
   SSL certificate private key filename = clientkey.prm
   passphrase file = location of the passphrase file created above.
   ```

   The command prompts you to enter the administrator password.

3. Enter the administrator password to start BI Scheduler.

5.6.3 Configuring Oracle BI Job Manager

To successfully connect to BI Scheduler that has been enabled for SSL, Oracle BI Job Manager must also be configured to communicate over SSL.

Oracle BI Job Manager is a Java based component and the keys and certificates that it uses must be stored in a Java keystore database.

Use this procedure to configure Oracle BI Job Manager to communicate with the BI Scheduler server over SSL.

To configure Oracle BI Job Manager:

1. From the **File** menu, select **Oracle BI Job Manager**, then select **Open Scheduler Connection**.
2. In the Secure Socket Layer section of the dialog box, select the **SSL** check box.
3. If the server setting 'verify client certificates' is false (one way SSL) then you can leave Key Store and Key Store Password blank. This is the default setting.
4. If the server setting 'verify client certificates' is true (two way SSL) then you must set Key Store and Key Store Password as follows:
   - Key Store=<*exportclientcerts_directory*>\identity.jks

- Key Store Password = passphrase entered in Section 5.6.1, "Exporting Client Certificates".

5. To provide a secure link you should tick the verify server certificate. Without verification the connection will still work, but a person in the middle attack which impersonates the server will not be detected.

   a. Select the **Verify Server Certificat**e check box. When this is checked, the trust store file must be specified. This trust store contains the CA that verifies the Scheduler server certificate.

   b. In the **Trust Store** text box, set the trust store to:

   <*exportclientcerts_directory*>\internaltrust.jks

   c. Set the **Trust Store Password** to the passphrase entered in Section 5.6.1, "Exporting Client Certificates".

5.6.4 Enabling the Online Catalog Manager to Connect

The online Catalog Manager might fail to connect to Oracle BI Presentation Services when the HTTP web server for Oracle Business Intelligence is enabled for SSL. You must import the SSL server certificate or CA certificate from the web server into the Java Keystore of the JVM that is specified by the system JAVA_HOME variable.

To enable the online Catalog Manager to connect:

1. Navigate to Java's default trust store located at *ORACLE_HOME/JAVA_HOME*/jre/lib/security.

   The default trust store is named cacerts.

2. Copy the certificate exported from the web server to the same location as Java's default truststore.

3. Execute the command to import the certificate to the default truststore:

   ```
   keytool -importcert -trustcacerts -alias bicert -file $WebServerCertFilename
   -keystore cacerts -storetype JKS
   ```

   where the web server certificate file $WebserverCertFilename is imported into Java's default trust store named cacerts under an alias of bicert.

   For example if using the Oracle WebLogic Server default demonstration certificate, then use the full path to the certificate located in *ORACLE_HOME*/wlserver/server/lib/CertGenCA.der.

   Note: The default password for the Java trust store is "changeit".

4. Restart Catalog Manager.

   Note: You must start Catalog Manager using the secure HTTPS URL.

5.6.5 Configuring the Oracle BI Administration Tool to Communicate Over SSL

To successfully connect to a BI Server that has been enabled for SSL, the Administration Tool must also be configured to communicate over SSL. The DSN for the Oracle BI Server data source is required.

To configure the Administration Tool to communicate over SSL:

1. Determine the Oracle BI Server data source DSN being used by logging into the Presentation Services Administration page as an administrative user.

   For more information, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

2. Locate the **Oracle BI Server Data Source** field in the upper left corner. The DSN is listed in the following format: coreapplication_OH<*DSNnumber*>.

3. In the Administration Tool, enter the DSN name by selecting **File**, then **Open**, then **Online**. Select the DSN from the list.

4. Enter the repository user name and password.

   The Administration Tool is now connected to the BI Server using SSL.

5.6.6 Configuring an ODBC DSN for Remote Client Access

You can create an ODBC DSN for the Oracle BI Server to enable remote client access. For more information about how to enable SSL communication for an ODBC DSN, see "Integrating Other Clients with Oracle Business Intelligence" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*.

5.6.7 Configuring Oracle BI Publisher to Communicate Over SSL

You can configure BI Publisher to communicate securely over the internet using SSL. For more information, see "Configuring BI Publisher for Secure Socket Layer (SSL) Communication" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*.

If BI Publisher does not work after configuring SSL, you might need to reconfigure the HTTPs protocol, and SSL Port. For more information, see "Configuring Integration with Oracle BI Presentation Services" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher*.

5.7 Checking Certificate Expiry

This task provides a warning if certificates are expired or about to expire.

You must run commands from the master host. The system can be running or stopped.

To check certificate expiry:

1. Run the following command to check certificate expiry:

   <*DomainHome*>/ bitools/bin/ssl.sh expiry

Post conditions:

- Detailed expiry information on certificate authority and server certificates is listed.
- The ssl.sh command returns the following status:
  - 13 – if certificates expired.
  - 14 – if certificates are due to expire in less than 30 days.
  - 0 – if certificates have more than 30 days life remaining.

5.8 Replacing the Certificates

Certificate replacement allows replacement of all certificates by new ones. You may want to do this because:

- The existing certificates have expired, or are about to expire.

  Both server certificates and CA (trust) certificates have defined lifespans. Once they expire connections using those certificates will no longer work.
- Your organization has a policy requiring a different certificate expiry from the default provided by the BI configuration assistant.
- The security of the existing certificates and keys has been compromised.

Assumptions:

- You run commands from the master host.
- This is an offline operation.

To replace the certificates:

1. Replace internal BIEE or client certificates.

   When you use the regenerate command, it invalidates existing client certificates so you must re-export them.

   ```
   ./ssl.sh regenerate
   ./ssl.sh exportclientcerts mydir
   ```

2. Restart the domain using:

   ```
   ./start.sh
   ```

3. Check WebLogic certificates and corresponding trust are correctly configured using:

   ```
   ./ssl.sh report
   ```

Post conditions

The domain now runs with SSL, and uses the new certificates. Servers will not connect to a WebLogic instance using the old trust.

You can run the `ssl.sh expiry` command to list the new certificates with the new expiry date.

5.9 Update Certificates After Changing Listener Addresses

You can update certificates following a change of listener address, for example by setting an explicit listener address in WebLogic console to replace the default (blank). The ssl.sh scan command shows errors due to incorrect certificate common names. Connections to servers whose certificates do not match their listening addresses will be rejected.

Assumptions:

- You run commands from the master host.
- This is an offline operation.

To update the certificates after changing listening addresses:

1. Update certificates by running:

   ```
   ./ssl.sh rebindchannelcerts
   ```

2. Restart the domain using:

```
./start.sh
```

3. Check WebLogic certificates and corresponding trust are correctly configured using:

```
./ssl.sh report
```

Post conditions

The domain now runs with SSL, and uses the new certificates. The new certificates have the same expiry as existing certificates. The certificates are signed by the existing internal certificate authority so previously exported client trust remains valid.

You can run the `ssl.sh expiry` command to list the new certificates with the new expiry date.

5.10 Adding New Servers

This task provides the same internal SSL configuration for a new server.

Assumptions:

- You run commands from the master host.
- This is an offline operation.
- One or more new servers have been created, either by cloning an existing server or creating from scratch.

To add a new server:

1. For each new server run:

```
./ssl.sh channel <new_bi_server> <port>
```

2. Alternatively you can repeatedly run:

```
./ssl.sh internalssl true
```

   Then run the channel command as indicated in the `internalssl` command's error message.

3. Restart the domain using:

```
./start.sh
```

4. Check WebLogic certificates and corresponding trust are correctly configured using:

```
./ssl.sh report
```

Post conditions

The domain now runs with SSL, with all WebLogic managed servers using the internal SSL. If the servers were cloned, the cloned internal channel port has been replaced by the port given by the channel command. If the servers were created from scratch the internal channel has been created and configured to use SSL.

5.11 Scaling Out an SSL-Enabled System

This task enables you to scale out a system which already has internal SSL enabled.

For information, see in "Adding New Computers" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*, where the necessary ssl.sh bindchannelcerts call is made.

5.12 Enabling SSL in a Configuration Template Configured System

This task provides the same SSL internal channel configuration as provided by the BI configuration assistant for systems configured using WLST or by direct application of configuration templates in the WebLogic configuration assistant.

Assumptions:

- You run commands from the master host.
- This is an offline operation.

To enable SSL in a configuration template configured system:

1. Run the following commands:

   ```
   <domain_home>/bitools/bin/ssl.sh regenerate <days>
   <domain_home>/bitools/bin/ssl.sh targetapps bi_cluster
   ```

2. For each new server run:

   ```
   ./ssl.sh channel <new_bi_server> <port>
   ```

3. Alternatively you can repeatedly run:

   ```
   ./ssl.sh internalssl true
   ```

   Then run the channel command as indicated in the `internalssl` command's error message.

4. Restart the domain using:

   ```
   ./start.sh
   ```

5. Check WebLogic certificates and corresponding trust are correctly configured using:

   ```
   ./ssl.sh report
   ```

Post conditions

The domain now runs with SSL, with all WebLogic managed servers using the internal SSL.

5.13 Manually Configuring SSL Cipher Suite

The default SSL configuration uses default cipher suite negotiation. You can configure the system to use a different cipher suite if your organization's security standards do not allow for the default choice. You can view the default choice in the output from the SSL status report.

This advanced option involves editing a configuration file. Be careful to observe the syntactic conventions of this file type.

A manually configured SSL environment can co-exist with a default SSL configuration.

To manually configure SSL cipher suite:

1. Configure SSL.
2. Select the desired Java Cipher Suite name from the options located at http://download.oracle.com/javase/1.5.0/docs/guide/security/jsse/JSSERefGuide.html#AppA.
3. Create an Open SSL Cipher Suite Name that matches the cipher suite chosen, using the list at http://www.openssl.org/docs/apps/ciphers.html#CIPHER_LIST_FORMAT.

   For example, Java Cipher Suite name SSL_RSA_WITH_RC4_128_SHA maps to Open SSL: RSA+RC4+SHA.
4. Edit the bi-ssl.xml file located at:

   <DOMAIN_HOME>/config/fmwconfig/core/ssl/bi-ssl.xml

   and add following sub-element to the JavaHost/Listener/SSL element. For example:

   ```
   <EnabledCipherSuites>SSL_RSA_WITH_RC4_128_SHA</EnabledCipherSuites>
   ```
5. Restart the Oracle Business Intelligence components using:

   ```
   ./start.sh
   ```

   For more information, see "Starting and Stopping Oracle Business Intelligence System Components" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

5.14 Configuring SSL Connections to External Systems

This section contains the following topics:

- Section 5.14.1, "Configuring SSL for the SMTP Server Using Fusion Middleware Control"
- Section 5.14.2, "Configuring SSL when Using Multiple Authenticators"

5.14.1 Configuring SSL for the SMTP Server Using Fusion Middleware Control

You must obtain the SMTP server certificate to complete this task.

To configure SSL for the SMTP server using Fusion Middleware Control:

1. Login to Fusion Middleware Control.

   For more information, see Section 1.6.2, "Using Oracle Fusion Middleware Control".
2. Go to the **Business Intelligence Overview** page.
3. Display the **Mail** tab of the **Deployment** page.

   Click the **Help** button on the page to access the page-level help for its elements.
4. Lock the configuring by clicking **Lock and Edit Configuration**.
5. Complete the fields under **Secure Socket Layer (SSL)** as follows:
   - **Connection Security**: Select an option, other fields may become active afterward.
   - **Specify CA certificate source**: Select **Directory** or **File**.
   - **CA certificate directory**: Specify the directory containing CA certificates.

- **CA certificate file**: Specify the file name for the CA certificate.
- **SSL certificate verification depth**: Specify the verification level applied to the certificate.
- **SSL cipher list**: Specify the list of ciphers matching the cipher suite name that the SMTP server supports. For example, RSA+RC4+SHA.

6. Click **Apply**, then **Activate Changes**.

5.14.2 Configuring SSL when Using Multiple Authenticators

If you are configuring multiple authenticators, and have configured an additional LDAP Authenticator to communicate over SSL (one-way SSL only), you need to put the corresponding LDAP server's root certificate in an additional keystore used by the virtualization (libOVD) functionality.

To configure SSL when using multiple authenticators:

Note: Before completing this task, you must configure the custom property called `virtualize` (lower case), and set its value to `true` (for more information, see Section 3.4.6, "Configuring Identity Store Virtualization Using Fusion Middleware Control").

---

1. Create the keystore:
   a. Set environment variables ORACLE_HOME, WL_HOME and JAVA_HOME.

      For example (on UNIX):

      ```
      set ORACLE_HOME=orahome

      set WL_HOME=orahome/wlserver

      set JAVA_HOME=orahome/oracle_common/jdk
      ```

   b. Set up the keystore by running libovdconfig.sh (on UNIX), or libovdconfig.bat (on Windows), using -createKeystore option.

      For example, on UNIX, open a shell prompt and change the directory to <*OracleHome*>/oracle_common/bin. Then, run the following command (which prompts for the Oracle Business Intelligence administrator user name and password), for example:

      ```
      ./libovdconfig.sh -host <hostname> -port <Admin_Server_Port>
      -username <BI Admin User> -domainPath <OracleHome>/user_
      projects/domains/bi/config/fmwconfig/ovd/default/keystores
      -createKeystore
      ```

   c. When prompted, enter the Oracle Business Intelligence administrator password, and the OVD Keystore password (a new password that will be used to secure a Keystore file), created by the libovdconfig.sh -createKeystore command.

      Once this command runs, you should see two new credentials in the Credential Store and a new Keystore file called adapters.jks under <*OracleHome*>/user_projects/domains/bi/config/fmwconfig/ovd/default/keystores.

2. Export the root certificate from the LDAP directory (refer to your LDAP documentation on how to do this).

3. Import the root certificate to the libOVD keystore using the keytool command:

   <OracleHome>*/jdk/jre/bin/keytool -import -keystore* <*OracleHome*>`\user_projects/domains/bi/config/fmwconfig/ovd/default/keystores/adapters.jks -storepass` <*KeyStore password*> `-alias` <*alias of your choice*> `-file` <*Certificate filename*>

4. Restart WebLogic Server and Oracle Business Intelligence processes.

   For more information, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

5.15 WebLogic Artifacts Reserved for BIEE Internal SSL Use

The following WebLogic artifacts are reserved for BIEE internal use:

- Virtual hosts:

  bi_internal_virtualhost1

- Channels (on each managed server):

  bi_internal_channel1

5.16 Enabling BI Composer to Launch in an SSL Environment

This section explains how to enable BI Composer to launch from BI Answers when in an SSL environment, by manually updating a JMX MBean value using Fusion Middleware Control.

In a non SSL environment, integration between BI Answers and BI Composer works without additional configuration. However, in an SSL environment, you must manually change the protocol value from http to https for integration to work properly.

To enable BI Composer to launch in an SSL environment:

1. Log in to Fusion Middleware Control in an SSL-enabled environment.
2. Display the WebLogic Server menu, and choose the **System MBean Browser** option.
3. Open Application Defined MBeans, and expand the following items:

   oracle.adf.share.connections > Server: bi_server1 > Application: bicomposer > ADFConnections > ADFConnections > BISoapConnection > bi-default

4. Select bi-default and change the value of attribute 13, **Protocol** as follows:

   Replace the value `http` with the value `https`

5. Click **Apply**.

A

Legacy Security Administration Options

This appendix describes legacy security administration options included for backward compatibility with upgraded systems and are not considered a best practice. This appendix contains the following sections:

- Legacy Authentication Options
- Alternative Authorization Options

> **Note:** For any particular user, both authentication and authorization must be performed either by the Oracle Fusion Middleware security model or using the legacy mechanisms. You cannot mix the two. So a user cannot perform authentication using Oracle Fusion Middleware security and then authorization using initialization blocks.

A.1 Legacy Authentication Options

Several Oracle Business Intelligence legacy authentication options are still supported for backward compatibility. The best practice for upgrading systems is to begin implementing authentication using an identity store and authentication provider as provided by the default security model. An embedded directory server is configured as the default identity store and authentication provider during installation or upgrade and is available for immediate use. For more information about the default security model, see Chapter 1, "Introduction to Security in Oracle Business Intelligence" and Appendix B, "Understanding the Default Security Configuration".

Authentication is the process by which the user name and password presented during login is verified to ensure the user has the necessary credentials to log in to the system. The BI Server authenticates each connection request it receives. The following legacy authentication methods are supported by the BI Server for backward compatibility in this release:

- External LDAP-based directory server.
- External initialization block authentication.
- Table-based.

This section contains the following topics:

- Section A.1.1, "Setting Up LDAP Authentication Using Initialization Blocks"
- Section A.1.2, "Setting Up External Table Authentication"
- Section A.1.3, "About Oracle BI Delivers and External Initialization Block Authentication"

A.1.1 Setting Up LDAP Authentication Using Initialization Blocks

You can set up the BI Server to pass user credentials to an external LDAP server for authentication.

The legacy LDAP authentication method uses Oracle Business Intelligence session variables that you define using the Variable Manager in the Oracle BI Administration Tool. For more information about the session variables, see "Using Variables in the Oracle BI Repository" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

To set up LDAP authentication using initialization blocks:

1. Create an LDAP Server as follows:
   a. Select **Manage** then **Identity** in the Administration Tool to launch the Identity Manager.
   b. Select **Directory Servers** from the left pane in Identity Manager.
   c. Right-click in the right pane in Identity Manager and select **New LDAP Server**. The LDAP Server dialog is displayed.
   d. Create the LDAP server by completing the fields.
2. Create an LDAP initialization block and associate it with an LDAP server. For more information, see "Creating Initialization Blocks" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
3. Define a system variable named USER and assign the USER variable to an LDAP attribute (for example, uid, sAMAccountName, cn).

   Session variables get their values when a user begins a session by logging on. Certain session variables, called system session variables, have special uses. The system session variable USER is used with authentication. For more information about the USER system session variable, see "Defining a USER Session Variable for LDAP Authentication". For more information about system session variables, see "About System Session Variables" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
4. If applicable, delete users from the repository file.
5. Associate the USER system variable with the LDAP initialization block. For more information, see "Defining a USER Session Variable for LDAP Authentication" and "Associating Variables with Initialization Blocks" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

> **Note:** When using secure LDAP you must restart the Administration Tool before testing if you have done the following: set the key file name and password, tested the LDAP parameter setting successfully in the Administration Tool, and then changed the key file name and password again.

A.1.1.1 Setting Up an LDAP Server

For instances of Oracle Business Intelligence that use ADSI as the authentication method, the following options should be used when setting up the Active Directory instance:

- In **Log On To**, select **All Computers**, or if you list some computers, include the Active Directory server as a Logon workstation.
- Ensure that **User must change password at next logon** is not selected.

In the Administration Tool, the CN user used for the BIND DN in the LDAP Server section must have both ldap_bind and ldap_search authority.

> **Note:** The BI Server uses cleartext passwords in LDAP authentication. Make sure your LDAP Servers are set up to allow this.

To set up LDAP authentication for the repository:

1. Open a repository in the Administration Tool in either offline or online mode.
2. From **Identity Manager**, select **Action**, then **New**, then **LDAP Server**.
3. In the LDAP Server dialog, in the General tab, complete the necessary fields. The following list of options and descriptions contain additional information to help you set up the LDAP server:
   - **Name**. The name to identify this connection (for example, My LDAP).
   - **Host name**. The name of your LDAP server.
   - **Port number**. The default LDAP port is 3060.
   - **LDAP version**. LDAP 2 or LDAP 3 (versions). The default is LDAP 3.
   - **Base DN**. The base distinguished name (DN) identifies the starting point of the authentication search. For example, if you want to search all of the entries under the o=Oracle.com subtree of the directory, o=Oracle.com is the base DN.
   - **Bind DN and Bind Password**. The optional DN and its associated user password that are required to bind to the LDAP server.

     If these two entries are blank, anonymous binding is assumed. For security reasons, not all LDAP servers allow anonymous binding.

     These fields are optional for LDAP V3, but required for LDAP V2, because LDAP V2 does not support anonymous binding.

     These fields are required if you select the **ADSI** option. If you leave these fields blank, a warning message appears asking if you want to leave the password empty anyway. If you click **Yes**, anonymous binding is assumed.
   - **Test Connection**. Use this button to verify your parameters by testing the connection to the LDAP server.
4. Click the **Advanced** tab, and enter the required information. The BI Server maintains an authentication cache in memory that improves performance when using LDAP to authenticate large numbers of users. Disabling the authentication cache can slow performance when hundreds of sessions are being authenticated.

   The following list of fields and descriptions contain additional information to help you set up the LDAP server:

- **Connection timeout**. When the BI Server attempts to connect to an LDAP server for user authentication, the connection times out after the specified interval.
- **Domain identifier** (Optional). Typically, the identifier is a single word that uniquely identifies the domain for which the LDAP object is responsible. This is especially useful when you use multiple LDAP objects. If two different users have the same user ID and each is on a different LDAP server, you can designate domain identifiers to differentiate between them. The users log in to the BI Server using the following format:

  domain_id/user_name

  If a user enters a user name without the domain identifier, then it is authenticated against all available LDAP servers in turn. If there are multiple users with the same name, then only one user can be authenticated.
- **ADSI**. (Active Directory Service Interfaces) A type of directory server. If you select the **ADSI** option, **Bind DN** and **Bind password** are required.
- **SSL**. (Secure Sockets Layer) Select this option to enable SSL.
- **User Name Attribute Type**. This parameter uniquely identifies a user. In many cases, this is the attribute used in the RDN (relative distinguished name). Typically, you accept the default value. For most LDAP servers, you would use the user ID. For ADSI, use sAMAccountName.

A.1.1.2 Defining a USER Session Variable for LDAP Authentication

To set up LDAP authentication using initialization blocks, you define a system session variable called USER and associate it with an LDAP initialization block that is associated with an LDAP server. When a user logs in to the BI Server, the user name and password is passed to the LDAP server for authentication. After the user is authenticated successfully, other session variables for the user could also be populated from information returned by the LDAP server.

Note: If the user exists in both an external LDAP server using the legacy method and in an LDAP-based identity store based on Oracle Platform Security Services, the user definition in the identity store takes precedence. The legacy LDAP mechanism is only attempted if authentication fails against Oracle Platform Security Services.

The information in this section assumes that an LDAP initialization block has been defined.

For users not defined in an LDAP-based identity store, the presence of the defined system variable USER determines that external authentication is performed. Associating USER with an LDAP initialization block determines that the user is authenticated by LDAP. To provide other forms of authentication, associate the USER variable with an initialization block associated with an external database.

To define the USER session variable for LDAP authentication:

1. Open a repository in the Administration Tool in either offline or online mode.
2. Select **Manage**, then **Variables** from the Administration Tool menu.
3. Select the **Session -> Initialization Blocks** leaf of the tree in the left pane.
4. Right-click in the right pane and select **New Initialization Block**.

5. In the Session Variable - Initialization dialog box, enter `Authentication` in the **Name** field.
6. Click **Edit Data Source**.
7. Select LDAP Server from the **Data Source Type** drop down list.
8. Browse to select the appropriate LDAP server from the list.
9. Click **OK**.
10. Click **Edit Data Target**.
11. Click **New**.
12. Enter `USER` in the **Name** field.
13. Click **OK**.
14. Click **Yes** to the warning message about the USER session variable having a special purpose.
15. Enter in the **Mapped Variable** field, the LDAP attribute that holds the user ID.
16. Click **OK**.
17. Select the **Required for Authentication** checkbox.
18. Click **OK**.

A.1.1.3 Setting the Logging Level

Use the system variable LOGLEVEL to set the logging level for users who are authenticated by an LDAP server.

A.1.2 Setting Up External Table Authentication

You can maintain lists of users and their passwords in an external database table and use this table for authentication purposes. The external database table contains user names and passwords, and could contain other information, including group membership and display names used for Oracle BI Presentation Services users. The table could also contain the names of specific database catalogs or schemas to use for each user when querying data.

> **Note:** If a user belongs to multiple groups, the group names should be included in the same column, separated by semicolons. This only applies if you are not using row wise variable for groups or roles.

External table authentication uses session variables that you define using the Variable Manager in the Administration Tool. For more information about the Variable Manager, see "Using Variables in the Oracle BI Repository" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

Session variables get their values when a user begins a session by logging on. Certain session variables, called system variables, have special uses. The variable USER is a system variable that is used with external table authentication.

To set up external table authentication, you define a system variable called USER and associate it with an initialization block that is associated with an external database table. Whenever a user logs in, the user ID and password are authenticated using SQL that queries this database table for authentication. The initialization block uses the database connection in the physical layer to connect to the database. The connection in

the physical layer contains the log in information. After the user is authenticated successfully, other session variables for the user could also be populated from the results of this SQL query.

The presence of the defined system variable USER determines that external authentication is performed. Associating USER with an external database table initialization block determines that the user is authenticated using the information in this table. To provide other forms of authentication, associate the USER system variable with an initialization block associated with a LDAP server or XML source. For more information, see "Setting Up LDAP Authentication Using Initialization Blocks".

To set up external table authentication:

1. Import information about the external table into the Physical layer.
2. Select **Manage**, then **Variables** in the Administration Tool to open the Variable Manager.
3. Select **Initialization Blocks** in the left pane.
4. Right-click in the right pane and select **New Initialization Block**.
5. In the Initialization Block dialog box, enter a name for the initialization block.
6. Select **Database** from the **Data Source Connection** list.
7. Click **Browse** to search for the name of the connection pool this block uses.
8. In the **Initialization String** area, enter the SQL statement that is issued at authentication time.

   The values returned by the database in the columns in the SQL statement is assigned to variables. The order of the variables and the order of the columns determines which columns are assigned to which variables. Consider the SQL in the following example:

   ```
   SELECT username, grp_name, SalesRep, 2 FROM securitylogons WHERE username =
   ':USER' and pwd = ':PASSWORD'
   ```

   This SQL contains two constraints in the `WHERE` clause:

   – :USER (note the colon) equals the name the user entered when logging on.

   – :PASSWORD (note the colon) equals the password the user entered.

   The query returns data only if the user name and password match values found in the specified table.

   You should test the SQL statement outside of the BI Server, substituting valid values for :USER and :PASSWORD to verify that a row of data returns.
9. If this query returns data, then the user is authenticated and session variables are populated. Because this query returns four columns, four session variables are populated. Create these variables (USER, GROUP, DISPLAYNAME, and LOGLEVEL) by clicking **New** in the Variables tab.

   If a variable is not in the desired order, click the variable you want to reorder and use the **Up** and **Down** buttons to move it.
10. Click **OK** to save the initialization block.

A.1.3 About Oracle BI Delivers and External Initialization Block Authentication

Oracle BI Scheduler Server runs Delivers jobs for users without accessing or storing their passwords. Using a process called impersonation, Oracle BI Scheduler uses one

user name and password with Oracle Business Intelligence administrative privileges that can act on behalf of other users. Oracle BI Scheduler initiates an Agent by logging on to Oracle BI Presentation Services with the Oracle Business Intelligence administrative name and password.

For Delivers to work, all database authentication must be performed in only one connection pool, and that connection pool can only be selected in an initialization block for the USER system session variable. This is typically called the Authentication Initialization Block. When impersonation is used, this initialization block is skipped. All other initialization blocks must use connection pools that do not use database authentication.

Caution: An authentication initialization block is the only initialization block in which it is acceptable to use a connection pool where :USER and :PASSWORD are passed to a physical database.

For other initialization blocks, SQL statements can use :USER and :PASSWORD. However, because Oracle BI Scheduler Server does not store user passwords, the WHERE clause must be constructed as shown in the following example:

```
SELECT username, groupname, dbname, schemaname FROM users
WHERE username=':USER'
NQS_PASSWORD_CLAUSE(and pwd=':PASSWORD')NQS_PASSWORD_CLAUSE
```

When impersonation is used, everything in the parentheses is extracted from the SQL statement at runtime.

For more information, see the Oracle BI Delivers examples in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

A.1.4 Order of Authentication

The BI Server populates session variables using the initialization blocks in the desired order that are specified by the dependency rules defined in the initialization blocks. If the server finds the session variable USER, it performs authentication against an LDAP server or an external database table, depending on the configuration of the initialization block with which the USER variable is associated.

Authentication against the identity store configured in Oracle WebLogic Server Administration Console occurs first, and if that fails, then initialization block authentication occurs.

A.1.5 Authenticating by Using a Custom Authenticator Plug-In

You can create a customized authentication module using initialization blocks. An **authenticator** is a dynamic link library (DLL), or shared object on UNIX, written by a customer or developer that conforms to the Oracle BI Authenticator API Specification and can be used by the BI Server to perform authentication and other tasks at run time. The dynamically loadable authentication module is a BI Server module with a cache layer that uses the authenticator to perform authentication and related tasks at run time.

Sample custom authenticator code can be found in the BI EE Sample Application downloadable from Oracle Technology Network (OTN).

After you create an authentication object (authenticator plug-in) and specify a set of parameters for the authentication module (such as configuration file path, number of

cache entries, and cache expiration time), you must associate the authentication object with an initialization block. You can associate the USER variable (required) and other variables with the initialization blocks.

When a user logs in, if the authentication is successful, this populates a list of variables, as specified in the initialization block.

A custom authenticator is an object in the repository that represents a custom C authenticator plug-in. This object is used with an authentication init block to enable the BI Server component to authenticate users against the custom authenticator. The recommended method for authentication is to use Oracle WebLogic Server's embedded LDAP server. However, the practice of using custom authenticators can continue to be used.

To add a custom authenticator:

1. In the Administration Tool, select **Manage**, then **Identity**. Select **Custom Authenticators** from the navigation tree. Select from the following options:
   - To create a new custom authenticator: Right-click in the right pane and select **New Custom Authenticator**.
   - To edit a custom authenticator: Double-click the name.
2. In the **Custom Authenticator** dialog, complete the necessary fields.
   - **Authenticator plug-in**: The path and name of the plug-in DLL for this custom authenticator.
   - **Configuration parameters**: The parameters that have been explicitly exposed for configuration for this custom authenticator.
   - **Encrypted parameter**: The parameters that have been encrypted, such as passwords for this custom authenticator.
   - **Cache persistence time**: The interval at which the authentication cache entry for a logged on user is refreshed, for this custom authenticator.
   - **Number of cache entries**: The maximum number of entries in the authentication cache for this custom authenticator (preallocated when the Oracle BI Server starts). If the number of users exceeds this limit, cache entries are replaced using the LRU algorithm. If this value is 0, then the authentication cache is disabled.
3. Click **OK**.

A.1.6 Managing Session Variables

System session variables obtain their values from initialization blocks and are used to authenticate Oracle Business Intelligence users against external sources such as LDAP servers or database tables. Every active BI Server session generates session variables and initializes them. Each session variable instance can be initialized to a different value. For more information about how session variable and initialization blocks are used by Oracle Business Intelligence, see "Using Variables in the Oracle BI Repository" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

A.1.7 Managing Server Sessions

The Administration Tool Session Manager is used in online mode to monitor activity. The Session Manager shows all users logged in to the session, all current query requests for each user, and variables and their values for a selected session.

Additionally, an administrative user can disconnect any users and terminate any query requests with the Session Manager.

How often the Session Manager data is refreshed depends on the amount of activity on the system. To refresh the display at any time, click **Refresh**.

A.1.7.1 Using the Session Manager

The Session Manager contains an upper pane and a lower pane:

- The top pane, the Session pane, shows users currently logged in to the BI Server. To control the update speed, from the **Update Speed** list, select **Normal**, **High**, or **Low**. Select **Pause** to keep the display from being refreshed.
- The bottom pane contains two tabs:
  - The Request tab shows active query requests for the user selected in the Session pane.
  - The Variables tab shows variables and their values for a selected session. You can click the column headers to sort the data.

Table A–1 and Table A–2 describe the columns in the Session Manager dialog.

Table A–1 Fields in the Session Manager Dialog

Column Name	Description
Client Type	The type of client connected to the server.
Last Active Time	The time stamp of the last activity on the session.
Logon Time	The time stamp that shows when the session initially connected to the BI Server.
Repository	The logical name of the repository to which the session is connected.
Session ID	The unique internal identifier that the BI Server assigns each session when the session is initiated.
User	The name of the user connected.

Table A–2 Some Fields in the Request Tab of the Session Manager Dialog

Column Name	Description
Last Active Time	The time stamp of the last activity on the query.
Request ID	The unique internal identifier that the BI Server assigns each query when the query is initiated.
Session ID	The unique internal identifier that the BI Server assigns each session when the session is initiated.
Start Time	The time of the individual query request.

To view the variables for a session:

1. In the Administration Tool, open a repository in online mode and select **Manage** then **Sessions**.
2. Select a session and click the **Variables** tab.

   For more information about variables, see "Using Variables in the Oracle BI Repository" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

3. To refresh the view, click **Refresh**.
4. To close Session Manager, click **Close**.

To disconnect a user from a session:

1. In the Administration Tool, open a repository in online mode and select **Manage** then **Sessions**.
2. Select the user in the Session Manager top pane.
3. Click **Disconnect**.

   The user session receives a message that indicates that the session was terminated by an administrative user. Any currently running queries are immediately terminated, and any outstanding queries to underlying databases are canceled.
4. To close the Session Manager, click **Close**.

To terminate an active query:

1. In the Administration Tool, open a repository in online mode and select **Manage** then **Sessions**.
2. Select the user session that initiated the query in the top pane of the Session Manager.

   After the user is highlighted, any active query requests from that user are displayed in the bottom pane.
3. Select the request that you want to terminate.
4. Click **Kill Request** to terminate the selected request.

   The user receives a message indicating that the query was terminated by an administrative user. The query is immediately terminated, and any outstanding queries to underlying databases are canceled.

   Repeat this process to terminate any other requests.
5. To close the Session Manager, click **Close**.

A.2 Alternative Authorization Options

For backward capability, this release supports the ability to manage catalog object privileges using Catalog groups, and the ability to set application role membership for users using initialization blocks, when authentication is also being performed by initialization blocks.

> **Note:** It is not possible to set application role membership using initialization blocks, when authentication is performed by Oracle Platform Security Services.

This section contains the following topics:

- Section A.2.1, "Changes Affecting Security in Presentation Services"
- Section A.2.2, "Managing Catalog Privileges Using Catalog Groups"
- Section A.2.3, "Setting Up Authorization Using Initialization Blocks"

A.2.1 Changes Affecting Security in Presentation Services

If you have upgraded from a previous release, the best practice is to begin managing catalog privileges and catalog objects using application roles maintained in the policy store.

Oracle Business Intelligence uses the Oracle Fusion Middleware security model and its resources are protected by a role-based system. This has significance for upgrading users as the following security model changes affect privileges in the Oracle BI Presentation Catalog:

- Authorization is now based on fine-grained JAAS permissions. Users are granted permissions by membership in corresponding application roles.
- Users and groups are maintained in the identity store and are no longer maintained in the BI Server. Members of BI Server groups are no longer automatically made members of Catalog groups having the same name, as was the practice in earlier releases.
- Privileges continue to be stored in the Oracle BI Presentation Catalog and cannot be accessed from the administrative interfaces used to manage the policy store.
- The Everyone Catalog group is no longer available and has been replaced by the AuthenticatedUser application role. Members of the Everyone Catalog group automatically become members of AuthenticatedUser role after upgrade.
- Catalog groups can no longer be password protected. All Catalog groups migrated during upgrade no longer have a password.

A.2.2 Managing Catalog Privileges Using Catalog Groups

Existing Catalog groups are migrated during upgrade and available for your use. You can continue to create new Catalog groups. For information about how to create, edit, or delete Catalog groups, see Section D.2.2, "Working with Catalog Groups".

You can grant these privileges by assigning other Catalog groups, users, or application roles to a Catalog group.

> **Note:** Assigning Catalog groups to become members of an application role creates complex group inheritance and maintenance situations, and is not considered a best practice.

To grant privileges using a Catalog group:

1. From the Home page in Presentation Services, select **Administration**.
2. Click the **Manage Privileges** link to display the Manage Privileges page.
3. Click the link for the privilege from the Manage Privileges page.
4. To assign the privilege to the Catalog group:
   - Click **Add Users/Roles**.
   - Select **Catalog Groups** from the list and click **Search**.
   - Select the Catalog group from the results list.
   - Use the shuttle controls to move the Catalog group to **Selected Members**.
5. Click **OK**.

6. Set the permission for the Catalog group by selecting **Granted** or **Denied** in the Privileges dialog.

   Explicitly *denying* a Presentation Services privilege takes precedence over user access rights either granted or inherited as a result of group or application role hierarchy.

7. Click **OK**.

8. Repeat Steps 3 through 7 until the privileges have been granted or denied as needed.

A.2.3 Setting Up Authorization Using Initialization Blocks

To set application role membership for users using initialization blocks, the following conditions apply:

- Initialization blocks to set ROLES or GROUP session variables will only function when the user fails to authenticate through an authenticator configured in the WebLogic security realm, and the user instead authenticates through an initialization block.
- You must set up an initialization block to set the values of either ROLES or GROUP, and the BI Server will make the values of both variables the same.
- When using an initialization block to set ROLES or GROUP session variables, the values of the variables should be set to match by name against one or more application roles configured using Fusion Middleware Control, for example, BIConsumer. A user will be assigned these application roles and associated permissions during authentication.
- For information about application roles, and how to add a new application role, see Section 2.4, "Managing Application Roles and Application Policies Using Fusion Middleware Control".
- When using initialization blocks to set ROLES or GROUP session variables, the association of groups to application roles is performed using the logic previously described. Assignment of groups to application roles in the policy store is not used in this case.
- Any value of the ROLES or GROUP variable that does not match an application role will be matched by name against the available Catalog groups in the Oracle BI Presentation Catalog. The user will be assigned these Catalog groups and associated privileges.
- Any value of ROLES or GROUP that does not match an application role or a Catalog group will be ignored.

To define the ROLES session variable for database authorization:

1. Open a repository in the Administration Tool in either offline or online mode.
2. Select **Manage**, then **Variables** from the Administration Tool menu.
3. Select the **Session -> Initialization Blocks** leaf of the tree in the left pane.
4. Right-click in the right pane and select **New Initialization Block**.
5. In the Session Variable - Initialization dialog box, enter `Authorization` in the **Name** field.
6. Click **Edit Data Source**.
7. Select Database from the **Data Source Type** drop down list.

8. Enter the SQL.

   The SQL can be anything that returns either a list of groups, or a single group if row-wise initialization is not used.

   For more information, see "Using Variables in the Oracle BI Repository" in the *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

9. Click **Browse** to select a connection pool.
10. Click **Select**.
11. Click **OK**.
12. Click **OK**.
13. Click **Edit Data Target**.
14. Click **New**.
15. Enter `ROLES` in the **Name** field.
16. Click **OK**.
17. Click **Yes** to the warning message about the ROLES session variable having a special purpose.
18. Click **OK**.
19. Clear the **Required for Authentication** checkbox.
20. Click **OK**.

B

Understanding the Default Security Configuration

Controlling access to system resources is achieved by requiring users to authenticate at log in (**authentication**) and by restricting users to only the resources for which they are authorized (**authorization**). Security providers are configured to manage user identities, credentials, and permission grants.

This chapter contains the following sections:

> **Note:** Unless otherwise stated, the privileges discussed in this chapter are those maintained in the policy store provider, such as the Oracle Business Intelligence Presentation Services privileges. Catalog permissions are distinct because they are maintained in the Oracle BI Presentation Catalog. For more information about Presentation Services privileges, see Section D.2.3, "Managing Presentation Services Privileges".

B.1 About Securing Oracle Business Intelligence

Securing Oracle Business Intelligence can be broken down into two broad areas:

- System access security: Controlling access to the components and features that make up Oracle Business Intelligence.
- Data access security: Controlling access to business source data and metadata used by Oracle Business Intelligence.

System access security is discussed in this guide and topics include how to limit system access to authorized users, control software resources based on permission grants, and enable secure communication among components.

Data access security is discussed in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

B.2 About the Security Framework

The Oracle Fusion Middleware security model is built upon the Oracle Fusion Middleware platform, which incorporates the Java security model. The Java model is a role-based, declarative model that employs container-managed security where resources are protected by roles that are assigned to users. However, extensive knowledge of the Java-based architecture is unnecessary when using the Oracle Fusion Middleware Security model. By being based upon this security model, Oracle Business Intelligence can furnish uniform security and identity management across the enterprise.

Oracle Business Intelligence is installed into an Oracle WebLogic Server domain during installation, which is a logically related group of resources that are managed as a unit. During installation, an Oracle WebLogic Server domain named bi is created and Oracle Business Intelligence is installed into this domain. This name might vary depending upon the installation type performed. One instance of Oracle WebLogic Server in each domain is configured as an Administration Server. The Administration Server provides a central point for managing an Oracle WebLogic Server domain. The Administration Server hosts the Administration Console, which is a web application accessible from any supported web browser with network access to the Administration Server. Oracle Business Intelligence uses the active security realm configured for the Oracle WebLogic Server domain into which it is installed. For more information, see Section B.2.2, "Oracle WebLogic Server Domain".

For more information about the Oracle Fusion Middleware platform and the common security framework, see *Oracle Fusion Middleware Application Security Guide*. For more information about managing the Oracle WebLogic Server domain and security realm, see *Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server* and *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

B.2.1 Oracle Platform Security Services

Oracle Platform Security Services (OPSS) is the underlying platform on which the Oracle Fusion Middleware security framework is built. Oracle Platform Security Services is standards-based and complies with role-based-access-control (RBAC), Java Enterprise Edition (Java EE), and Java Authorization and Authentication Service (JAAS). Oracle Platform Security Services enables the shared security framework to furnish uniform security and identity management across the enterprise.

For more information about Oracle Platform Security Services, see *Oracle Fusion Middleware Application Security Guide*.

Note: In future versions of the documentation, references to Oracle Platform Security Services (OPSS) will be replaced by references to Oracle Entitlements Server Basic (OES Basic), with no change to customer-visible behavior.

B.2.2 Oracle WebLogic Server Domain

An Oracle WebLogic Server administration domain is a logically related group of Java components. A domain includes a special WebLogic Server instance called the Administration Server, which is the central point from which you configure and manage all resources in the domain. You typically configure a domain to include additional WebLogic Server instances called Managed Servers. You deploy Java components, such as web applications, EJBs, and web services, and other resources to

the Managed Servers and use the Administration Server for configuration and management purposes only.

Oracle WebLogic Server Administration Console and Fusion Middleware Control run in the Administration Server. Oracle WebLogic Server Administration Console is the Web-based administration console used to manage the resources in an Oracle WebLogic Server domain, including the Administration Server and Managed Servers. Fusion Middleware Control is a Web-based administration console used to manage Oracle Fusion Middleware, including the components that comprise Oracle Business Intelligence. For more information about the Oracle Business Intelligence individual components, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Oracle Business Intelligence authentication is handled by the Oracle WebLogic Server authentication providers. An authentication provider performs the following functions:

- Establishes the identity of users and system processes
- Transmits identity information

Upon installation Oracle Business Intelligence is configured to use the directory server embedded in Oracle WebLogic Server as both the default authentication provider and the repository for users and groups. Alternative authentication providers can be used if desired, and managed in the Oracle WebLogic Server Administration Console. For more information, see System Requirements and Certification.

B.3 Key Security Elements

The Oracle Fusion Middleware security platform depends upon the following key elements to provide uniform security and identity management across the enterprise. For more information about the Oracle Fusion Middleware security platform, see *Oracle Fusion Middleware Application Security Guide*.

Oracle Business Intelligence uses these security platform elements as follows:

Application Policy

For more information about application policies, see Section 1.9, "Terminology".

An **application stripe** defines a subset of policies in the policy store. The Oracle Business Intelligence application stripe is named **obi**.

Application Role

For more information about application roles, see Section 1.4.1, "About Application Roles". For example, having the Sales Analyst application role can grant a user access to view, edit and create reports relating to a company's sales pipeline. The application role is also the *container* used to grant permissions and access to its members. When members are assigned to an application role, that application role becomes the container used to convey access rights to its members. For example:

- Oracle Business Intelligence Permissions

  These permission grants are defined in an application policy. After an application role is assigned to a policy, the permissions become associated with the application role through the relationship between policy and role. If groups of users have been assigned to that application role, the corresponding permissions are in turn granted to all members equally. More than one user or group can be members of the same application role.

- Data Access Rights

Application roles can be used to control access rights to view and modify data in the repository file. Data filters can be applied to application roles to control object level permissions in the Business Model and Mapping layer and the Presentation layer. For more information about using application roles to apply data access security and control repository objects, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

- Presentation Services Object-Level Access

  Application roles can be used to grant access rights to reports and other objects in Oracle BI Presentation Services. For more information about using application roles to control access in Presentation Services, see *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Authentication Provider

For more information about authentication providers, see Section 1.3, "About Authentication".

B.4 Security Configuration Using the Sample Application

When operating in a development or test environment you might find it convenient to use the security configuration provided when you use the default directory server and the sample application. You then add user definitions and credentials specific to your business, and customize the existing application roles and permission grants to meet your requirements. After the authentication, policy, and credential providers are fully configured and populated with data specific to your business, they provide all user, policy, and credential information needed by the Oracle Business Intelligence components during authentication and authorization.

BI security with the embedded directory server and sample application has three security providers that are integrated to ensure safe, controlled access to system and data resources. These security providers are configured during installation as follows:

- Section B.4.1, "Default Authentication Provider"

  The authentication provider is DefaultAuthenticator, which authenticates against Oracle WebLogic Server embedded directory server (identity store). The default identity store is managed using Oracle WebLogic Server Administration Console.

- Section B.4.2, "Policy Store Provider"

  The policy store provider is the database specified during the initial BI configuration. It contains the application role definitions with their corresponding Oracle Business Intelligence permission grants, and the mapping definitions between groups and application roles. The assigning of a group to an application role serves to convey the corresponding permissions to members of the group. The default policy store provider is managed using Oracle Enterprise Manager Fusion Middleware Control.

- Credential Store Provider

  The credential store provider is the database specified during the initial BI configuration. It contains the passwords and other security-related credentials either supplied or system-generated. The default credential store is managed using Fusion Middleware Control.

Table B–1 summarizes the security providers and their initial state after installation.

Table B–1 Default Security Providers

Security Provider Type	Purpose	Default Provider	Options
Authentication provider	Used to control authentication.	▪ DefaultAuthenticator. Authenticates against the users and groups stored in Oracle WebLogic Server embedded directory server (identity store). ▪ Oracle WebLogic Server embedded directory server is managed with Oracle WebLogic Server Administration Console.	Oracle Business Intelligence can be reconfigured to use different authentication providers and directory servers. For more information, see System Requirements and Certification.
Policy store provider	▪ Used to control authorization. ▪ Contains the definition of application roles, application policies, and the members assigned to application roles.	▪ Stored in a database schema. ▪ Managed with Fusion Middleware Control.	Oracle Business Intelligence can be configured to use Oracle Internet Directory.
Credential store provider	Trusted store for holding system passwords and other security-related credentials. The data stored here is used for connecting to external systems, opening repositories, or for SSL.	▪ Stored in a database. ▪ Managed with Fusion Middleware Control.	Oracle Business Intelligence can be configured to use Oracle Internet Directory.

Figure B–1 shows the relationship between Oracle Business Intelligence and the authentication and policy store providers.

Figure B–1 Relationship with the Default Security Providers

B.4.1 Default Authentication Provider

An **authentication provider** accesses user and group information and is responsible for authenticating users. An **identity store** contains user name, password, and group membership information and in Oracle Business Intelligence. The default security configuration authenticates against the Oracle WebLogic Server embedded directory server using an authentication provider named DefaultAuthenticator.

When a user logs in to a system with a user name and password combination, Oracle WebLogic Server validates identity based on the combination provided. During this process, a Java principal is assigned to the user or group that is undergoing authentication. The principal can consist of one or more users or groups and is stored within subjects. A **subject** is a JAAS element used to group and hold identity information.

Upon successful authentication, each principal is signed and stored in a subject. When a program call accesses a principal stored in a subject, the default authenticator provider verifies the principal has not been altered since signing, and the principal is returned to the program making the call. For example, in the Oracle WebLogic Server default authenticator, the subject contains a principal for the user (WLSUserPrincipal) and a principal for the group (WLSGroupsPrincipals) of which the user is a member. If an authentication provider other than the installation default is configured, consult that provider's documentation because how identity information is stored might differ.

B.4.1.1 Groups and Members

Groups are logically ordered sets of users. Creating groups of users who have similar system resource access needs enables easier security management. Managing a group is more efficient than managing a large number of users individually. Groups are then assigned to application roles to grant rights. Oracle recommends that you organize your users into groups for easier maintenance.

No default groups are created during the installation of BI.

B.4.1.2 Default Users and Passwords

When you configure your BI deployment a Weblogic domain is created and populated with a single user that is specified as part of the configuration steps.

- This user name is entered by the person performing the configuration and can be any desired name.
- The password entered during installation can be changed later using the administration interface for the identity store provider.
- During the configuration of the BI service instance, the Weblogic domain administrator is automatically made the owner of the service instance and made a member of the application role that confers administrative privileges (e.g. BIServiceAdministrator or BIAdministrator)

B.4.2 Policy Store Provider

The policy store provider contains the Oracle Business Intelligence application-specific policies, application roles, permission grants, and membership mappings. A policy store can be database-based or LDAP-based, but the installation default provides a policy store that is database-based.

Catalog privileges and permissions are not maintained in the policy store provider.

B.4.2.1 Oracle Business Intelligence Permissions

All Oracle Business Intelligence permissions and permission sets are provided; you cannot create additional permissions or permission sets. If you chose to configure your service instance based on the Sample Application, sample application policies and application roles are pre-configured to assign these permission sets according to the access requirements of the Oracle Business Intelligence common user types: administrator, author, and consumer. If you chose to import an 11*g* upgrade bundle into your service instance, the 11*g* permission grants will be used along with any new permission sets that were not available in 11*g*. Permission grants can be changed as needed using Fusion Middleware Control.

Note: Permission set grants can be viewed in Enterprise Manager Fusion Middleware Control but can only be changed using WLST.

B.5 Granting Permissions To Users Using Groups and Application Roles

The default Oracle Business Intelligence security configuration provides preconfigured permission sets that group together related permissions.s If you choose to import the Sample or Starter Application into your service instance these permission sets have been granted to the sample or starter set of application roles. If you start with an clean slate by importing the empty BAR file into your service instance, you will need to use WLST to assign permission sets to the application roles that you create. Application roles typically have groups as members, and permissions are inherited by users through their membership of groups. A group assigned to an application role conveys the role's permissions to all members of the group.

You grant permissions through Oracle Business Intelligence application roles by establishing the following relationships:

- A group defines a set of users having similar system access requirements. Users are added as members of one or more groups according to the level of access required.
- An application role defines the role a user typically performs when using Oracle Business Intelligence. The security policy in the Sample Application provides the following roles: administrator (BIServiceAdministrator), author (BIContentAuthor), and consumer (BIConsumer).
- A group is assigned to one or more application roles that match the type of access required by each group.
- An application policy defines Oracle Business Intelligence permissions that grant a set of access rights corresponding to each role type.
- An application role is assigned to an application policy that grants the set of permissions required by the role type (for example administrator, author, consumer). Once configured, the application role is the grantee of the application policy.
- Group membership can be inherited by nature of the group hierarchy. Application roles assigned to inherited groups are also inherited, and their permissions are likewise conveyed.

How the system determines a user's permissions:

1. A user enters credentials into a web browser at login. The user credentials are authenticated by the authentication provider against data contained the identity store.

2. After successful authentication, a Java subject and principal combination is issued, which is populated with the user name and the user's groups.
3. A list of the user's groups is checked against the application roles. A list is created of the application roles that are assigned to each of the user's groups.
4. A user's permission grants are determined from knowing which application roles the user is a member of. The list of groups is generated only to determine what roles a user has, and is not used for any other purpose.

For example, the ability to open a repository file in online mode from the Oracle BI Administration Tool requires the relevant permission (the oracle.bi.repository resource type with a resource scope of * and an action of manage). In the Sample and Starter Application security policies, this permission is granted by membership in the BIServiceAdministrator application role. The BIServiceAdministrator application policy contains the actual permission grant definitions, and in this example, the BIServiceAdministrator application policy contains the permission set grant that includes the relevant permission. The BI installation does not automatically create any (LDAP) groups. Therefore to convey this permission set to a user in your environment, create a suitable group (e.g. create a BIAdministrators group in the Weblogic LDAP or the Idenetiy Store you have configured BI against if any), add that user to the BIServiceAdministrators group, then use EM FMW control or WLST to map the BIServiceAdministrators group to the BIServiceAdministrator application role. Every user who needs to manage a repository in online mode should be added to this group (for example, BIServiceAdministrators) instead of granting the required permission to each user individually. If a user no longer requires the manage repository permission, you then remove the user from the BIServiceAdministrators group. After removal from the BIServiceAdministrators group, the user no longer has the BIServiceAdministrator application role or the manage repository permission granted by role membership.

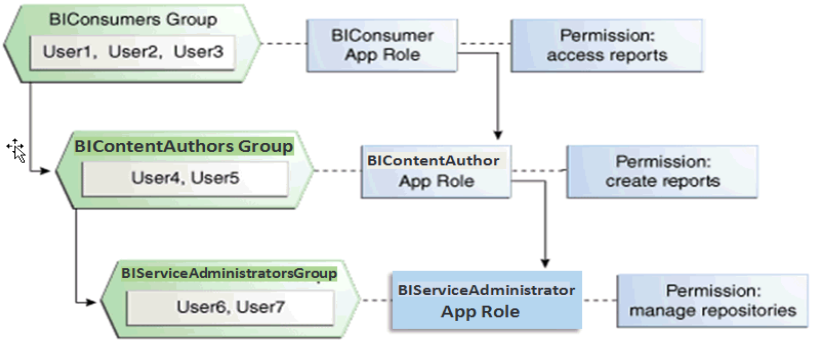
Users can also obtain permissions by inheriting group membership and application roles. For more information and an example of how this is accomplished, see Section B.5.1, "Permission Inheritance and Role Hierarchy".

B.5.1 Permission Inheritance and Role Hierarchy

In Oracle Business Intelligence, the members of an application role can include groups and other application roles. The result is a hierarchical application role structure where permissions can be inherited in addition to being explicitly granted. A group that is a member of an application role is granted both the permissions of the application role and the permissions for all application roles descended from that application role. It is important when constructing an application role hierarchy that circular dependencies are not introduced.

Figure B–2 shows the relationship between application roles and how permissions are granted to members.

Figure B–2 Application Role Hierarchy Example



In Figure B–2 the role hierarchy grants permissions using several of the Oracle Business Intelligence default groups and application roles. In the Sample and Starter applications, the default BIServiceAdministrator role is a member the BIContentAuthor role, and BIContentAuthor role is a member of BIConsumer role. The result is that members of the BIServiceAdministrator application role are granted *all* the permissions of the BIServiceAdministrator role, the BIContentAuthor role, and the BIConsumer role. So a user who is a member of a particular group mapped to an application role is granted both *explicit* permissions and any additional *inherited* permissions.

> **Note:** By themselves, groups and group hierarchies do not provide access rights to application resources. Privileges are conveyed by the permission grants defined in an application policy. A user, group, or application role becomes a grantee of the application policy. The application policy grantee conveys the permissions and this is done by direct association (such as a user) or by becoming a member of the grantee (such as a group or application role).

B.6 Common Security Tasks After Installation

The common security tasks performed after a successful Oracle Business Intelligence software installation are different according to purpose. Common reasons to install Oracle Business Intelligence are:

- Evaluate the product
- Implement the product

Implementation typically involves moving through the product lifecyle of using the product in one or more of the following environments:

- Development
- Test
- Production

This section contains the following topics:

- Section B.6.1, "Common Security Tasks to Evaluate Oracle Business Intelligence"
- Section B.6.2, "Common Security Tasks to Implement Oracle Business Intelligence"

B.6.1 Common Security Tasks to Evaluate Oracle Business Intelligence

Table B–2 contains common security tasks performed to evaluate Oracle Business Intelligence and provides links for more information.

Table B–2 Task Map: Common Security Tasks to Evaluate Oracle Business Intelligence

Task	Description	For Information
Understand the Oracle Fusion Middleware security model and the Oracle Business Intelligence default security configuration.	Familiarize yourself with the key elements of the Oracle Fusion Middleware security model and the Oracle Business Intelligence default security configuration after a successful installation.	Chapter 1, "Introduction to Security in Oracle Business Intelligence" Section B.4, "Security Configuration Using the Sample Application" *Oracle Fusion Middleware Application Security Guide*
Add users and groups to the default identity store.	Create new User and group definitions for the embedded directory server using Oracle WebLogic Server Administration Console.	Section 2.3.2, "Creating a New User in the Embedded WebLogic LDAP Server" *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*
Add a new member to an application role.	Add a new user or group as a member to an application role, such as BIConsumer.	Section 2.4.4, "Modifying Application Roles Using Fusion Middleware Control" *Oracle Fusion Middleware Application Security Guide*
Create a new application role based on an existing application role.	Create a new application role based on an existing application role by copying it and naming the copy.	Section 2.4.2, "Creating and Deleting Application Roles Using Fusion Middleware Control" *Oracle Fusion Middleware Application Security Guide*

B.6.2 Common Security Tasks to Implement Oracle Business Intelligence

Table B–3 contains common security tasks performed when you implement Oracle Business Intelligence and provides links for more information. The following tasks are performed in addition to the tasks listed in Section B.6.1, "Common Security Tasks to Evaluate Oracle Business Intelligence".

Table B–3 Task Map: Common Security Tasks to Implement Oracle Business Intelligence

Task	Description	For Information
Transition to using your enterprise directory server as the authentication provider and identity store.	Configure your enterprise directory server to become the authentication provider and identity store.	Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers" Appendix A, "Legacy Security Administration Options"
Create a new application role.	Create a new application role and make the role a grantee of an application policy.	Section 2.4.2, "Creating and Deleting Application Roles Using Fusion Middleware Control"

Table B–3 (Cont.) Task Map: Common Security Tasks to Implement Oracle Business Intelligence

Task	Description	For Information
Assign a group to a newly created application role.	Assign a group to a newly created application role to convey the permission grants to group members.	Section 2.4.4, "Modifying Application Roles Using Fusion Middleware Control"
Decide whether to use SSL.	Decide whether to use SSL communication and devise a plan to implement.	Chapter 5, "Configuring SSL in Oracle Business Intelligence"
Decide whether to use an SSO provider in your deployment.	Decide whether to use SSO authentication and devise a plan to implement.	Chapter 4, "Enabling SSO Authentication"

C

Troubleshooting Security in Oracle Business Intelligence

This appendix describes common problems that you might encounter when using and configuring Oracle Business Intelligence security, and explains how to solve them. It contains the following sections

- Resolving User Login Authentication Failure Issues
- Resolving Inconsistencies with the Identity Store
- Resolving Inconsistencies with the Policy Store
- Resolving SSL Communication Problems
- Resolving Custom SSO Environment Issues
- Resolving RSS Feed Authentication When Using SSO

C.1 Resolving User Login Authentication Failure Issues

This section helps you resolve some of the most common user login authentication failure issues encountered while using Oracle Business Intelligence Enterprise Edition 11*g*. It is not intended to be a comprehensive list of every possible scenario, and contains the following topics:

- Section C.1.1, "Authentication Concepts"

  This section describes the basic concepts of authentication in Oracle Business Intelligence Enterprise Edition. You must understand the concepts used throughout this guide as a prerequisite for using this section.

- Section C.1.2, "Identifying Causes of User Login Authentication Failure"

  This section provides a cause-and-effect diagram to use as a checklist for identifying authentication failure causes.

- Section C.1.3, "Resolving User Login Authentication Failures"

  This section provides reasons and solutions for login authentication failure.

C.1.1 Authentication Concepts

This section describes authentication concepts, helps you to resolve login issues, and contains the following topics:

- Section C.1.1.1, "Authentication Defaults on Install"
- Section C.1.1.2, "Using Oracle WebLogic Server Administration Console and Fusion Middleware Control to Configure Oracle Business Intelligence"

- Section C.1.1.3, "WebLogic Domain and Log Locations"
- Section C.1.1.4, "Oracle Business Intelligence Key Login User Accounts"
- Section C.1.1.5, "Oracle Business Intelligence Login Overview"

C.1.1.1 Authentication Defaults on Install

Immediately after install, Oracle Business Intelligence is configured to authenticate users against the WebLogic embedded LDAP server through the DefaultAuthenticator. Default user accounts will have been set up, including a WebLogic Server administrator that uses the credentials entered during installation.

C.1.1.2 Using Oracle WebLogic Server Administration Console and Fusion Middleware Control to Configure Oracle Business Intelligence

You configure Oracle Business Intelligence using Oracle WebLogic Server Administration Console and Fusion Middleware Control. For more information about using these applications, see Section 1.6, "Using Tools to Configure Security in Oracle Business Intelligence".

You must log in to Oracle WebLogic Server Administration Console and Fusion Middleware Control with the username and password that you specified for the administrator user during the install process, unless you have altered or removed that account or configured another account with the appropriate access (see Section C.1.1.4, "Oracle Business Intelligence Key Login User Accounts").

C.1.1.3 WebLogic Domain and Log Locations

To diagnose and resolve user login authentication issues, you must know the locations of the WebLogic domain, and log files, as follows:

> **Note:** This section assumes that the install used the default locations. If you specified different install locations, you must modify the paths accordingly.

- WebLogic domain where Oracle Business Intelligence is installed

  ORACLE_HOME/user_projects/domains/bi/
- WebLogic Administration Server logs

  ORACLE_HOME/user_projects/domains/bi/servers/AdminServer/logs/
- WebLogic Managed Server logs:

  ORACLE_HOME/user_projects/domains/bi/servers/bi_server1/logs/
- BI Server logs:

  ORACLE_HOME/user_projects/domains/bi/servers/obis1/logs/

C.1.1.4 Oracle Business Intelligence Key Login User Accounts

This section describes the key login user accounts, and contains the following sections:

- Section C.1.1.4.1, "WebLogic Server Administrator User Account"

C.1.1.4.1 WebLogic Server Administrator User Account The WebLogic Server administrator user account enables you to start the WebLogic Server, and to administer WebLogic Server using the Oracle WebLogic Server Administration Console and Fusion

Middleware Control. The WebLogic Server administrator account must have the WebLogic Server global role called Admin (this is not an Oracle Business Intelligence application role), which also enables them to add new WebLogic Server administrator accounts.

To add or remove users to or from the global admin role using the Oracle WebLogic Server Administration Console:

1. Log in to Oracle WebLogic Server Administration Console as a WebLogic Server administrator, and click **Lock & Edit** in the Change Center.

   For more information, see Section 1.6.1, "Using Oracle WebLogic Server Administration Console".

2. Select **Security Realms** from the left pane and click **myrealm**.

   The default Security Realm is named **myrealm**.

3. Select **Roles and Policies** from the tabs along the top.

4. In the list of roles, click on the plus sign to expand Global Roles, then Roles, then click the **View Role Conditions** link for the Admin global role.

5. Check to ensure that the specified conditions match your user, either directly, or through a group they belong to.

   For example, condition may be User=myadminaccount or Group=Administrators.

6. If you have made any changes, click **Save**.

7. In the Change Center, click **Activate Changes**.

C.1.1.5 Oracle Business Intelligence Login Overview

When a user logs in to Oracle Business Intelligence without Single Sign-On, authentication and user profile lookup occurs. In a Single Sign-On (SSO) environment, authentication is performed outside the Oracle Business Intelligence system, and identity is asserted instead, but user profile lookup still occurs.

Authentication and identity assertion is performed by authentication providers and asserters respectively, and is configured using Oracle WebLogic Server Administration Console. The user profile is looked up within the Identity Store to retrieve various attributes, such as email, display name, description, language etc. Successful login to Oracle Business Intelligence requires that the first configured authentication provider contains your user population. For more information, see Section 3.4, "Configuring Oracle Business Intelligence to Use Alternative Authentication Providers".

The login process flow begins with the user credentials entered in the login screen, being sent to Presentation Services, and then to the BI Server. The BI Server attempts to authenticate the user credentials by calling the BI Security web service (deployed in the WebLogic Managed Server, and protected by a web service security policy). The call requires the BI Server to authenticate itself to Oracle Web Services Manager, before it can be received by the BI Security Service.

C.1.2 Identifying Causes of User Login Authentication Failure

This section helps you to identify causes of authentication failure when logging in to Oracle Business Intelligence.

Figure C–1 and Figure C–2 are cause and effect diagrams that you can use to identify possible causes of user login authentication failure. Once you have identified the likely cause of user login identification failure, refer to Section C.1.3, "Resolving User Login Authentication Failures" for information about how to resolve the issues.

Figure C–1 Causes of User Login Failure - Part 1

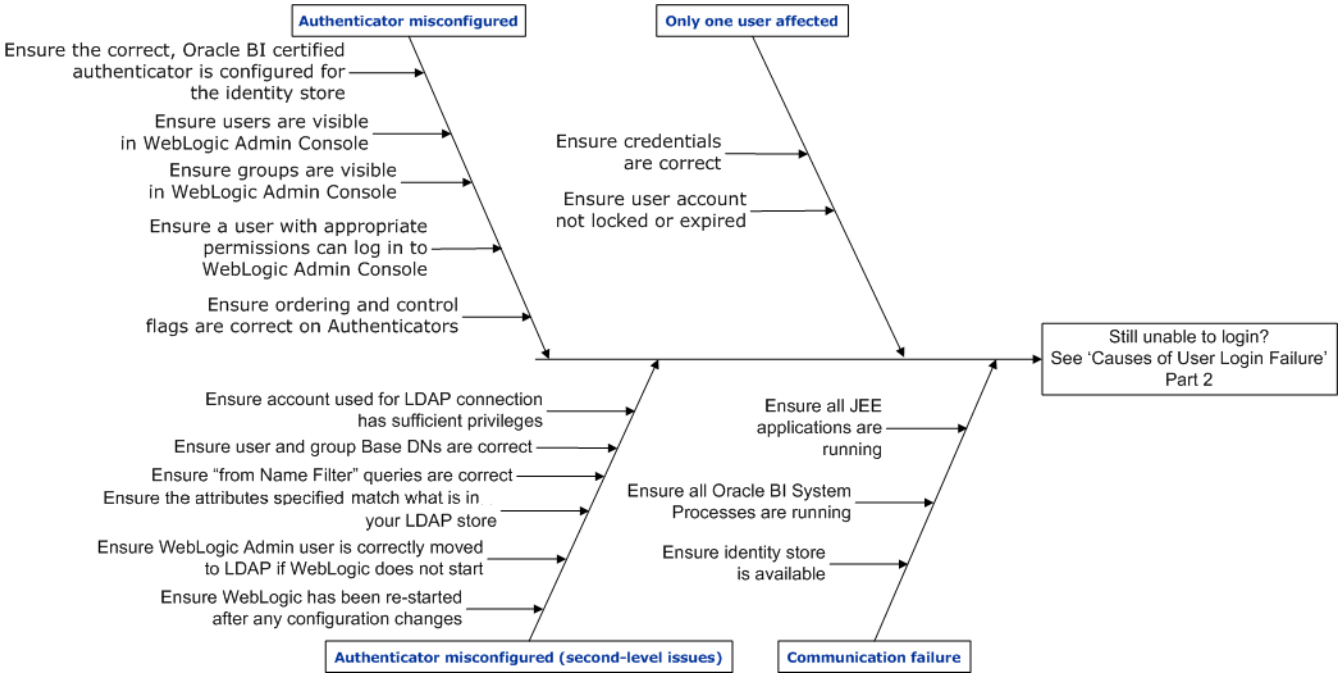


Figure C–1 helps you identify causes of login failure. If you cannot identify the cause of login failure using Figure C–1, then use Figure C–2 instead.

The description for Figure C–1 is as follows:

- **Authenticator misconfigured**.
  - Ensure that the correct Oracle Business Intelligence certified authenticator is configured for the identity store.
  - Ensure that users are visible in the Oracle WebLogic Server Administration Console.
  - Ensure that groups are visible in the Oracle WebLogic Server Administration Console.
  - Ensure that a user with appropriate permissions can log in to Oracle WebLogic Server Administration Console.
  - Ensure that the ordering and control flags on authenticators are correct.
- **Authenticator misconfigured (second-level issues)**.
  - Ensure that WebLogic Server has been re-started after any configuration changes.
  - Ensure that the WebLogic Server administrator user is correctly moved to LDAP, if WebLogic Server does not start.
  - Ensure that the attributes specified match what is in your LDAP store.
  - Ensure that 'from Name Filter' queries are correct.
  - Ensure that user and group Base DN settings are correct.
  - Ensure that the account used for LDAP connection has sufficient privileges.
- **Only one user affected**.
  - Ensure that correct credentials are used.

- Ensure that the user account is not locked or expired.

- **Communication failure**.
  - Ensure that the identity store is available.
  - Ensure that all BI System processes are running.
  - Ensure that all JEE applications are running.

Figure C–2 Causes of User Login Failure - Part 2

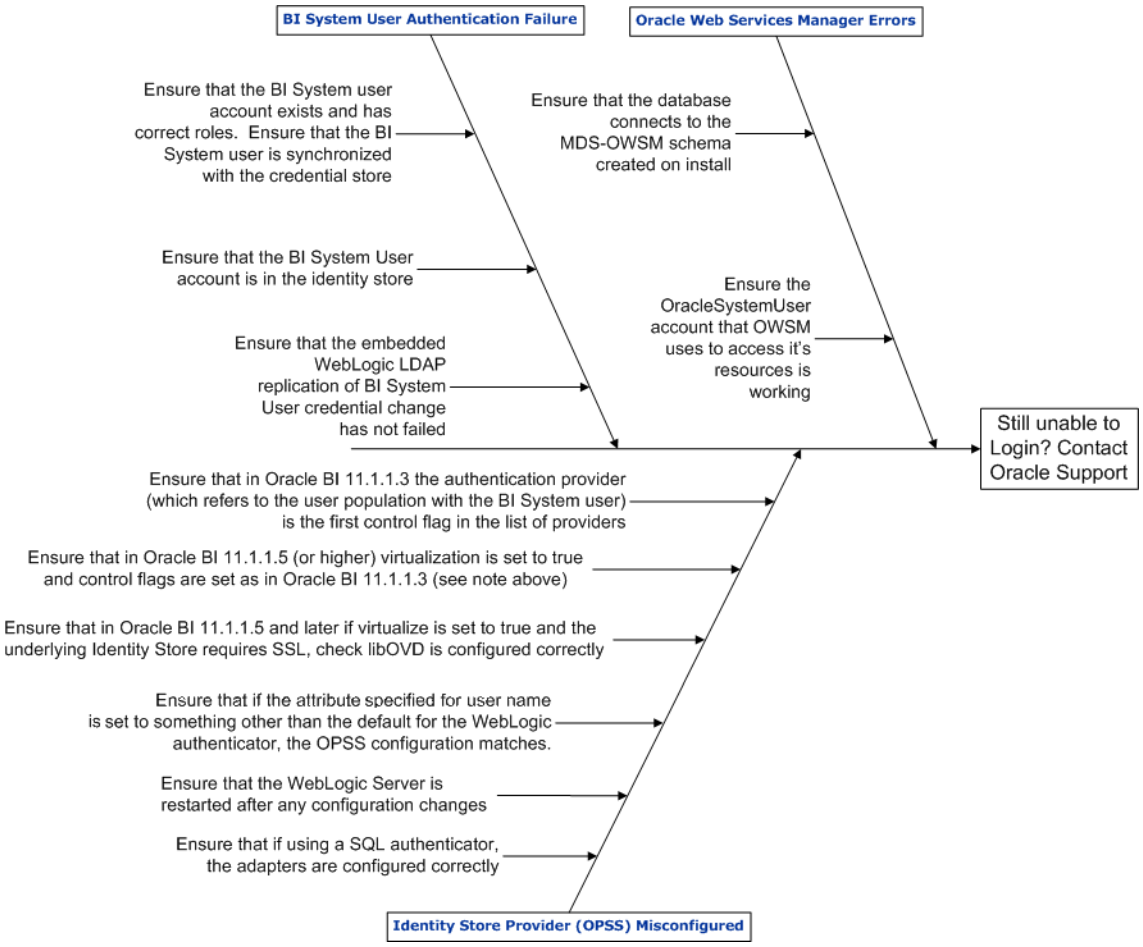


Figure C–2 helps you identify alternative causes of login failure if you cannot identify them using Figure C–1. However, if you still cannot identify the causes of login failure after using Figure C–2, contact Oracle Support at:

`https://support.oracle.com`

The description for Figure C–2 is as follows:

- **BI System User authentication failure**.
  - Ensure that the BISystem user account exists and has correct roles.
  - Ensure that the BISystem user is synchronized with credential store.
  - Ensure that the BISystem user account is in the identity store.
  - Ensure that WebLogic embeddedLDAP replication of BI System User credential change has not failed.

- **Identity store provider (OPSS) misconfigured**.
  - Ensure that if using a SQL authenticator, the adapters are configured correctly.
  - Ensure that if the attribute specified for username is set to something other than the default value for the WebLogic authenticator, the OPSS configuration matches.
  - Ensure that in Oracle Business Intelligence Release 11.1.1.5 (or higher):
    * Virtualization is set to true.
    * Control flags are set as in Oracle Business Intelligence Release 11.1.1.3 (see following bullet).
  - Ensure that in Oracle Business Intelligence Release 11.1.1.3 the authentication provider (which refers to the user population with the BI System User), is the first control flag in the list of providers.
  - Ensure that the WebLogic Server is re-started after any configuration changes.
  - Ensure that in Oracle Business Intelligence Release 11.1.1.5 (or higher), if virtualization is set to true and the identity store requires SSL, virtualization must be configured correctly. For more information, see Section 5.14.2, "Configuring SSL when Using Multiple Authenticators".
- **Oracle Web Services Manager errors**.
  - Ensure the database connects to the MDS-OWSM schema created on install.
  - Ensure the OracleSystemUser account that OWSM uses to access its resources is working.

C.1.3 Resolving User Login Authentication Failures

This section explains user login authentication failures, describes how to resolve them, and contains the following topics:

C.1.3.1 Single User Cannot Log in to Oracle Business Intelligence

This section contains the following topics:

C.1.3.1.1 Is Login Failure the Result of User Error? The first check is whether the user cannot log in to Oracle Business Intelligence due to a simple error for example, did the user enter the wrong password? If other users can log in to Oracle Business Intelligence, but one user cannot, check that user's credentials. Alternatively, see Section C.1.3.1.2.

C.1.3.1.2 Is User Account Locked? Many LDAP authenticators lock a user account when attempts to log in exceed a specified threshold. For example, an account may be locked after more than three failed login attempts to defeat a potential automated attack.

Refer to the documentation for your chosen identity store to discover how to unlock user accounts. For example, to unlock a locked user account when using WebLogic Server embedded LDAP, see "Unlock user accounts" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*.

C.1.3.2 Users Cannot Log in to Oracle Business Intelligence Due to Misconfigured Authenticators

The most common cause of authentication failure is misconfiguration of authenticators in WebLogic Server as follows:

> **Note:** Make sure you have read, and are familiar with the steps and concepts identified in Chapter 3, "Using Alternative Authentication Providers".

- Section C.1.3.2.1, "Have You Specified the Correct Authenticator for the Identity Store or LDAP Server?"
- Section C.1.3.2.2, "Is the Authenticator for the LDAP Server Configured Correctly?"
- Section C.1.3.2.3, "Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?"

C.1.3.2.1 Have You Specified the Correct Authenticator for the Identity Store or LDAP Server? WebLogic Server uses a variety of server-specific authenticators in addition to the embedded LDAP authenticator. However, the embedded LDAP authenticator might not be able to query against some LDAP server products because they do not appear to be generic LDAP servers. For example, the generic LDAP server does not work with Active Directory (AD), even though AD does apparently fully implement LDAP and successfully presents itself as an LDAP server to many LDAP query tools. Configure the appropriate authenticator based on the LDAP server that the system uses.

C.1.3.2.2 Is the Authenticator for the LDAP Server Configured Correctly? If the configuration settings for the LDAP server used as the primary identity store are incorrectly configured, then users cannot be correctly authenticated. Some common things to check include:

- Account used for LDAP connection.

  In the LDAP Authenticator provider-specific configuration, you must specify the DN of a principal that is used to connect to the LDAP server. This account must exist and have sufficient privileges to be able to run queries to retrieve the user or group population from the trees specified in the User or Group Base DNs. In a restricted LDAP environment, this may require elevated privileges beyond those granted to ordinary user accounts.

- Ensure user and group Base DNs are correct.

  Search for groups and users in the tree specified by the user or group Base DN, and ensure that the tree specified actually contains your user or group population.

- Ensure 'from Name Filter' queries are correct.

  Search for groups and users in the trees specified in the base DN by using the query specified in 'User from name filter' and 'Group from Name filter'. %u is a placeholder for the user id used for querying a specific user (including during authentication), and %g is a placeholder for the group name used for querying a specific group. Check that queries are syntactically and logically correct for your directory, and that you can run them (and return expected results) from an LDAP browser, using the credentials specified in the authenticator configuration.

- Ensure the attributes specified match what is in your LDAP store.

  The attributes and object classes for users and groups, are specified in the Authenticator configuration. You should not necessarily use an authenticator's pre-configured default values. For example, you should ensure that the value specified in User Name Attribute exists, and is being used for the users' names in the LDAP server on your site.

- WebLogic Server administrator user moved to LDAP and cannot boot WebLogic Server.

  If you move the WebLogic Server administrator user from the embedded LDAP server to another LDAP server, and also remove the DefaultAuthenticator from the embedded LDAP Server, you are relying only on LDAP to authenticate the administrator user. If you have misconfigured the LDAP authenticator, WebLogic Server does not start.

- Ensure users can log in to Oracle WebLogic Server Administration Console.

  If you can log in to Oracle WebLogic Server Administration Console using the credentials you used to start WebLogic Server, you can check whether other LDAP users can log in to Oracle WebLogic Server Administration Console as follows:

  Grant the WebLogic Server global Admin role to an LDAP user, and if they can log in to the Oracle WebLogic Server Administration Console (using the URL http://<*biserver*>:9501/console), the LDAP authenticator configuration is correct.

  > **Note:** If you temporarily grant the WebLogic Server global Admin role to a user to test this scenario, you must remove the grant when testing is complete to ensure the user does not have privileges to which they are not entitled.

  If the LDAP user cannot log in to Oracle Business Intelligence:

  - Check that the identity store containing your users is exposed as an identity store to OPSS - check the authenticator ordering and control flags section (see Section C.1.3.2.3, "Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?").
  - Check whether the BI System user is preventing the BI Security Service from authenticating users, if users are authenticating correctly to LDAP (see Section C.1.3.4, "Users Cannot Log in to Oracle Business Intelligence - Is BI System User Authentication Working?").

C.1.3.2.3 Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?

The primary identity store must be set as the first one in the list of authenticators (note that this restriction is lifted from Oracle Business Intelligence Release 11.1.1.5 (or higher) when virtualization is set to true). Oracle Business Intelligence uses the user role Application Programming Interface (API) from OPSS which only picks up the first identity store from the list of authenticators for example, when looking up users, profile information, roles. This situation enables a user to log in to Oracle WebLogic Server Administration Console (showing that authentication has succeeded), but prevents the user logging in to Oracle Business Intelligence (because the identity store containing the user is not first in the list).

Where more than one authenticator is configured, in the general case the control flags should all be set to SUFFICIENT. This enables each one to be tried in turn until authentication succeeds. If authentication is successful, no further authenticators are tried. If none of the authenticators can authenticate the supplied credentials, the overall authentication process fails.

> **Note:** During install, the DefaultAuthenticator is set to REQUIRED; if you configure another authenticator, the DefaultAuthenticator must be set to SUFFICIENT or OPTIONAL, if it is being retained. SUFFICIENT is the recommended setting.

C.1.3.3 Users Cannot Log in to Oracle Business Intelligence When Oracle Web Services Manager is not Working

Oracle Web Services Manager (OWSM) secures the BI Security Service, so if OWSM is not working, then nothing can call the BI Security Service, and authentication cannot succeed until this issue is resolved.

Common causes of OWSM failure are:

- Section C.1.3.3.1, "Database Issues - OWSM Cannot Retrieve Policies"

  Issues connecting to the MDS-OWSM schema created on install.

- Section C.1.3.3.2, "OracleSystemUser Issues - OWSM Cannot Retrieve Policies"

  Issues with the OracleSystemUser account that OWSM uses to access it's resources.

For information about BI System User authentication failure, see Section C.1.3.4, "Users Cannot Log in to Oracle Business Intelligence - Is BI System User Authentication Working?".

C.1.3.3.1 Database Issues - OWSM Cannot Retrieve Policies

OWSM stores its metadata, including its policy definitions, in an OWSM subsection of the MDS schema. It accesses this metadata using a connection pool created on install, named mds-owsm. If there is a problem accessing the schema (for example, if the database is not available, there are incorrect credentials, or the database account is locked), then Oracle Business Intelligence authentication fails.

You see an error message like the following one in the Managed Server diagnostic log:

```
[2011-06-28T14:59:27.903+01:00] [bi_server1] [ERROR] []
[oracle.wsm.policymanager.bean.util.PolicySetBuilder] [tid: RTD_Worker_2]
[userId: <anonymous>] [ecid:
de7dd0dc53f3d0ed:11d7f503:130d6771345:-8000-0000000000000003,0] [APP:
OracleRTD#11.1.1] The policy referenced by URI "oracle/wss_username_token_
client_policy" could not be retrieved as connection to Policy Manager
```

```
cannot be established at "t3://biserver:7001,biserver:9704" due to invalid
configuration or inactive state.
```

In addition, you see multiple errors related to a failure to establish or create the connection pool for the data source in the Administration Server logs.

To correct this issue, you must check the following:

- Is the database schema you specified for the MDS-OWSM data source available?
- Did you specify the correct credentials?
- Can you access the schema using standard database tools (for example, SQL Plus, Jdeveloper DB tools) using those credentials?
- Is the mds-owsm data source configured correctly?

To test the MDS-OWSM data source:

1. Log in to Oracle WebLogic Server Administration Console.
2. Click **Services** in the left hand pane and click **Data Sources**.
3. Display the Configuration page and click **mds-owsm**.
4. Select the Monitoring tab and display the Testing page.
5. Select a server and click **Test Data Source**.

To configure the MDS-OWSM data source:

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.
2. Click **Services** in the left hand pane and click **Data Sources**.
3. Display the Configuration page and click **mds-owsm**.
4. Select the Configuration tab and display the Connection Pool page.
5. Configure appropriate changes.
6. Click **Save** to save your changes.
7. In the Change Center, click **Activate Changes**.
8. Restart WebLogic Server and Oracle Business Intelligence components.

C.1.3.3.2 OracleSystemUser Issues - OWSM Cannot Retrieve Policies

By default, OWSM uses the OracleSystemUser account to retrieve policies. If the account is missing, and cannot be authenticated or does not have the correct WebLogic Server global role assignments, this causes failures.

You see a log message like the following one in the Managed server diagnostic logs:

```
 [2011-06-28T14:59:27.903+01:00] [bi_server1] [ERROR] []
[oracle.wsm.policymanager.bean.util.PolicySetBuilder] [tid: RTD_Worker_2]
[userId: <anonymous>] [ecid:
de7dd0dc53f3d0ed:11d7f503:130d6771345:-8000-0000000000000003,0] [APP:
OracleRTD#11.1.1] The policy referenced by URI "oracle/wss_username_token_
client_policy" could not be retrieved as connection to Policy Manager
cannot be established at "t3://biserver:7001,biserver:9704" due to invalid
configuration or inactive state.[[
```

After this entry, if the problem is that OWSM is not in the OracleSystemRole WebLogic Server global role, you see the following log entry:

```
java.rmi.AccessException: [EJB:010160]Security Violation: User:
'OracleSystemUser' has insufficient permission to access EJB: type=<ejb>,
application=wsm-pm, module=wsm-pmserver-wls.jar, ejb=DocumentManager,
method=retrieveDocuments, methodInterface=Remote,
signature={java.lang.String,java.util.Map}.
```

You must ensure that the OracleSystemUser is a member of the OracleSystemGroup group in your identity store and that the group has the WebLogic Server global role OracleSystemRole assigned to it. For more information, see Steps 3-6 in Section 3.4.9.1, "Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator" (these steps still apply for other LDAP servers):

Alternately, if the problem is that the OracleSystemUser account cannot be authenticated or does not exist (for example, because you migrated to an LDAP identity store and removed DefaultAuthenticator without creating a new OracleSystemUser account in your new identity store), you see a log entry like this:

```
Caused by: javax.security.auth.login.FailedLoginException:
[Security:090304]Authentication Failed: User OracleSystemUser
javax.security.auth.login.FailedLoginException:
[Security:090302]Authentication Failed: User OracleSystemUser denied

at
weblogic.security.providers.authentication.LDAPAtnLoginModuleImpl.login(LD
APAtnLoginModuleImpl.java:261)
```

This error message can be caused by several different issues:

- You have removed the DefaultAuthenticator and not created an account named OracleSystemUser in the new identity store you are using instead.
- You have misconfigured the authenticator for your new identity store such that the OracleSystemUser account cannot be found.
- The OracleSystemUser account has been locked or disabled in some way on your LDAP server.

Check the system for each of the possible causes, reconfigure and restart the system if needed, before retrying.

C.1.3.4 Users Cannot Log in to Oracle Business Intelligence - Is BI System User Authentication Working?

The BI System User account (named BISystemUser by default) is critical to the functioning of the BI Security Service and Oracle Business Intelligence authentication as a whole. The BI System User account authenticates the calls that the BI Server makes to the BI Security Service when it is trying to check the credentials the user has supplied when logging in. If this call fails, then Oracle Business Intelligence cannot authenticate user logins against Fusion Middleware security (that is, users in an identity store configured through WebLogic), the preferred mechanism. BI System User authentication can fail with the following error message in the BI Server nqserver.log:

```
[2011-06-28T11:30:36.000+00:00] [OracleBIServerComponent] [ERROR:1] [] []
[ecid: c594c519d241c3b9:-2173cea0:130d2098159:-8000-00000000000019ba]
[tid: 4734ba0] Error Message From BI Security Service:
FailedAuthentication : The security token cannot be authenticated.

[2011-06-28T11:30:36.000+00:00] [OracleBIServerComponent] [ERROR:1] [] []
[ecid: c594c519d241c3b9:-2173cea0:130d2098159:-8000-00000000000019ba]
```

```
[tid: 4734ba0] [nQSError: 43126] Authentication failed: invalid
user/password.
```

You also see a corresponding entry in the Managed Server diagnostic log like this:

```
[2011-06-27T11:06:46.698-07:00] [bi_server1] [NOTIFICATION] []
[oracle.bi.security] [tid: [ACTIVE].ExecuteThread: '0' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: BISystemUser] [ecid:
004dfIJ^08LATOB[2011-06-28T04:27:48.011-07:00] [bi_server1] [ERROR]
[WSM-00008] [oracle.wsm.resources.security] [tid: [ACTIVE].ExecuteThread:
'2' for queue: 'weblogic.kernel.Default (self-tuning)'] [userId:
<anonymous>] [ecid:
c594c519d241c3b9:-2173cea0:130d2098159:-8000-00000000000019a1,0:1:1:8:1]
[WSM_POLICY_NAME: oracle/wss_username_token_service_policy] [APP:
bimiddleware#11.1.1] Web service authentication failed.[[

javax.security.auth.login.LoginException: [Security:090303]Authentication
Failed: User BISystemUser
weblogic.security.providers.authentication.LDAPAtnDelegateException:
[Security:090295]caught unexpected exception

at
oracle.security.jps.internal.jaas.module.authentication.JpsUserAuthenticat
ionLoginModule.login(JpsUserAuthenticationLoginModule.java:71)
```

This message indicates that OWSM does not allow the call from the BI Server to the BI Security Service to succeed because it cannot authenticate the credentials supplied by the BI Server (not the end user on login) as being valid. The BI Server retrieves the credentials it uses for this call from the credential store by looking in the oracle.bi.system map for the system.user key. These are the credentials that are being authenticated by OWSM.

The following list shows the possible reasons behind failures with the BISystemUser account:

- Section C.1.3.4.1, "The BI System User Account Does Not Exist, Does Not Have Correct Roles, or Is Not Synchronized with the Credential Store"
  - You removed the DefaultAuthenticator because you are using an external LDAP store and did not create the BI System User account in the new identity store.
  - You changed the account specified in the system.user key in the credential store but the new account does not have the correct roles.
  - You changed the password of the account specified but have not updated the credential store with the new credentials (or not restarted the system afterwards).
- Section C.1.3.4.2, "Problem With BI System User Account in Underlying Identity Store"

  The account specified as the BI System User account has been locked or the password expired (there is a problem with the account in the underlying identity store).
- Section C.1.3.4.3, "Embedded WebLogic Server LDAP Replication of BI System User Credential Change Failed"

  You have changed the password of the account specified and replication to the Managed Server has failed (this only applies when you use the DefaultAuthenticator with WebLogic Server embedded LDAP).

C.1.3.4.1 The BI System User Account Does Not Exist, Does Not Have Correct Roles, or Is Not Synchronized with the Credential Store You can resolve these BISystemUser account issues by following the instructions in Section 3.5, "Resetting the BI System User Credential".

The account specified must have the BISystem application role and the WebLogic Server global Admin role, and the system.user key in the credential store must be updated with the new account name and password.

Once you complete these steps restart all Oracle Business Intelligence components and the WebLogic Managed Servers and Administration Server to synchronize the Oracle Business Intelligence components with the BI Security Service otherwise the problems may persist.

C.1.3.4.2 Problem With BI System User Account in Underlying Identity Store It is not uncommon for some LDAP servers to be configured to lock a user account after multiple failed authentication attempts. The BI Server automatically presents the BI System User credentials when attempting to communicate with the BI Security Service. If you change your password without re-synchronizing the credential store or restarting the services, the BI Server may make multiple failed authentication attempts, and lock the account by accident.

Equally, some servers are configured to require that credentials expire and be reset after a given period of time, which again lead to the BI System User failing authentication.

Check the policies on your LDAP server and make sure that the account has not become locked by mistake or expired.

C.1.3.4.3 Embedded WebLogic Server LDAP Replication of BI System User Credential Change Failed This scenario occurs rarely and only when the system uses the WebLogic Server embedded LDAP through the DefaultAuthenticator. To understand this scenario you need to understand a BI System User password change (using Oracle WebLogic Server Administration Console) is made initially in the Administration Server and then replicated in the Managed Servers. The BI Security Service authenticates against the replicated copy in the Managed Servers. However, if replication in the Managed Servers failure goes unnoticed, and you change the credentials in the credential store to synchronize with the new password, the two will not match. When this situation occurs, a log entry similar to the following is created in the Administration Server log:

```
####<2011/06/09 17:18:17 GMT> <Error> <EmbeddedLDAP> <bisrv01>
<AdminServer> <VDE Replication Thread> <<anonymous>> <>
<3425d20f6361741a:-2e8537d2:130736e27a9:-8000-000000000000000f>
<1307607517792> <BEA-000000> <Agreement 'bi_server1': Error Transmitting
Change#1698- Invalid name: cn=",ou=groups,ou=myrealm,dc=bifoundation_
domain>
```

If you appear to have this problem but you do not see such an entry, the most likely explanation is that there is a genuine mismatch between the credentials stored in the credential store and those in the identity store. Double check that the change was applied correctly in both places and that all services were restarted after the change was made.

C.1.3.5 Users Cannot Log in to Oracle Business Intelligence - Is the External Identity Store Configured Correctly?

If you have configured an external identity store as your primary user population, check the following aspects of the provider configuration:

- The authentication provider which refers to the primary user population must be set first in the order of providers (unless you are using Release 11.1.1.5 or higher, and virtualization is set to true).
- If the DefaultAuthenticator is still enabled, ensure that both it and the authentication provider referring to the primary user population are set to 'SUFFICIENT'.
- If you set the username attribute to something other than the default, you need to follow the instructions in Section 3.4.3, "Configuring User and Group Name Attributes in the Identity Store". For example, the OID authentication provider defaults to expecting the UserName attribute to be "cn", but many organizations actually use the attribute "uid" instead. In this instance, follow the instructions to set both username.attr and user.login.attr to uid in the identity store configuration in Fusion Middleware Control.

C.1.3.6 Users Can Log in With Any or No Password

In Oracle Business Intelligence Release 10*g*, authentication is managed through the Metadata Repository, and users wanting to authenticate against external database tables can do so using initialization block settings. The facility still exists in Oracle Business Intelligence 11*g*, and 12*c* and unfortunately it is possible to configure these blocks such that the query issued does not check the password of the user. For example, the query:

SELECT USER_ID FROM USERS WHERE USER_ID = ':USER'

only checks the user id and not whether the password is correct. In a scenario where such an initialization block is configured, it can lead to users being able to log in with any (or no) password.

This scenario also leads to some apparently inconsistent behavior. For example, if user A and B exist in the primary identity store (Oracle Internet Directory), but user B also exists in a database which is referenced by the initialization block described in this section. When user A and user B try to log in using the wrong password they both fail authentication against OID. However, the BI Server will also attempt to run the initialization block for each user. User A fails, but user B logs in successfully because its user name is in the USER_ID column of the USERS table, and the initialization block query succeeds, despite not checking the user's password. This kind of scenario must be avoided, so if you find an authentication initialization block that behaves in this way you must remove, or alter it.

C.1.3.7 Have Removed Default Authenticator and Cannot Start WebLogic Server

WebLogic Server must be started using administrator user credentials which are associated with the WebLogic Server (not Oracle Business Intelligence) global Admin role. When you install Oracle Business Intelligence the installer prompts for administrator user name and password, which are created in the embedded LDAP, and accessed through the DefaultAuthenticator. When you want to move from using the embedded LDAP to using an external LDAP identity store, you create a new WebLogic Server administrator user in the external store, ensure it has the WebLogic Server global Admin role, and remove the DefaultAuthenticator.

However, if you have performed these steps and have not correctly configured the authenticator configuration for the identity store that now contains the user that you want to use to start the WebLogic Server with, then you cannot start the server. The work around is to revert to the configuration settings that existed before you removed the DefaultAuthenticator.

The domain home for your WebLogic BI Domain (unless you specifically requested otherwise on install), is located in:

ORACLE_HOME/user_projects/domains/bi/

This directory contains a configuration directory with the configuration file for the overall domain, including any authenticators. When you update the configuration settings, a backup of the main configuration file, config.xml, is created, starting with backup_config.xml and then numbered versions (for example, backup_config7.xml) for each subsequent revision.

Make sure you copy the current config.xml and the most recent backup_config xml file in case you run into problems. To restore your configuration, replace the current config.xml file with the most recent backup_config xml file, and restart WebLogic Server and all Oracle Business Intelligence components. When WebLogic Server restarts, the DefaultAuthenticator will be restored.

C.2 Resolving Inconsistencies with the Identity Store

A number of inconsistencies can develop between a repository, the Oracle BI Presentation Catalog, and an identity store. The following sections describe the usual ways this can occur and how to resolve the inconsistencies.

C.2.1 User Is Deleted from the Identity Store

Behavior

If a user is deleted from the identity store then that user can no longer log in to Oracle Business Intelligence. However, references to the deleted user remain in the repository until an administrator removes them.

Cause

References to the deleted user still remain in the repository but that user cannot log in to Oracle Business Intelligence. This behavior ensures that if a user was deleted by accident and re-created in the identity store, then the user's access control rules do not need to be entered again.

Action

An administrator can run the Consistency Checker in the Oracle BI Administration Tool in online mode to identify inconsistencies.

C.2.2 User Is Renamed in the Identity Store

Behavior

A user is renamed in the identity store and then cannot log in to the repository with the new name.

Cause

This can occur if a reference to the user under the original name still exists in the repository.

Action

An administrator must either restart the BI Server or run the Consistency Checker in the Oracle BI Administration Tool to update the repository with a reference to the user

under the new name. Once this has been resolved Oracle BI Presentation Services updates the Oracle BI Presentation Catalog to refer to the new user name the next time this user logs in.

C.2.3 Group Associated with User Name Does Not Exist in the Identity Store

Behavior

If a group that is associated with a user name does not exist in the identity store, you might see the following error in the nqserver.log:

```
[2012-10-04T12:00:00.000+00:00] [OracleBIServerComponent] [ERROR:1] [] []
[ecid: <ecidID>] [tid: d10] SecurityService::assertUserWithLanguage
[OBI-SEC-00018] Identity found <GUID> but could not be asserted
```

Look for the ECID in the bi_server1-diagnostic.log (or adminserver-diagnostic.log if using a simple install), you might see a warning something like the following:

```
[2012-10-04T12:00:00.314+02:00] [bi_server1] [WARNING] []
[oracle.jps.authentication] [tid: [ACTIVE].ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: OBISystemUser] [ecid:
<ecidID>] [WEBSERVICE_PORT.name: SecurityServicePort] [APP:
bimiddleware#11.1.1] [J2EE_MODULE.name: bimiddleware/security]
[WEBSERVICE.name: SecurityService] [J2EE_APP.name: bimiddleware_11.1.1]
javax.security.auth.login.FailedLoginException:
[Security:090305]Authentication Failed Getting Groups for User <UserID>
weblogic.management.utils.NotFoundException: [Security:090255]User or
Group
<Groupname>[[
oracle.security.jps.internal.api.jaas.AssertionException:
javax.security.auth.login.FailedLoginException:
[Security:090305]Authentication Failed Getting Groups for User <UserID>
weblogic.management.utils.NotFoundException: [Security:090255]User or
Group
<Groupname>
...
   at
oracle.bi.security.subject.SubjectAsserter.assertUser(SubjectAsserter.java
:85)
   at
oracle.bi.security.service.URServiceBean.assertUserWithLanguage(URServiceB
ean.
java:97)
   at
```

```
oracle.bi.security.service.SecurityServiceBean.getGrantedRolesForUser(Secu
rityServiceBean.java:270)

  at

oracle.bi.security.service.SecurityWebService$1GetGrantedRolesForUserActio
n.run(SecurityWebService.java:391)

  at

oracle.bi.security.service.SecurityWebService$1GetGrantedRolesForUserActio
n.run(SecurityWebService.java:381)

  at java.security.AccessController.doPrivileged(Native Method)

  at

oracle.bi.security.service.SecurityWebService.getGrantedRolesForUser(Secur
ityWebService.java:397)

...

Caused by: javax.security.auth.login.FailedLoginException:

[Security:090305]Authentication Failed Getting Groups for User <UserID>

weblogic.management.utils.NotFoundException: [Security:090255]User or
Group

<Groupname>
```

Cause

This can occur if a group associated with a user name does not exist in the identity store.

Action

Check the LDAP groups assigned to this user do actually exist and are readable by the principal used by WebLogic to access the LDAP.

C.3 Resolving Inconsistencies with the Policy Store

A number of inconsistencies can develop between the Oracle BI Presentation Catalog and the policy store. The following sections describe the usual ways this can occur and how to resolve the inconsistencies.

C.3.1 Application Role Was Deleted from the Policy Store

Behavior

After an application role is deleted from the policy store the role name continues to appear in the Oracle BI Administration Tool when working in offline mode. But the role name no longer appears in Presentation Services and users are no longer granted the permissions associated with the deleted role.

Cause

References to the deleted role name persist in the repository enabling the role name to appear in the Administration Tool when working in offline mode.

Action

An administrator runs the Consistency Checker in the Oracle BI Administration Tool in online mode to remove references in the repository to the deleted application role name.

C.3.2 Application Role Is Renamed in the Policy Store

Behavior

After an application role is renamed in the policy store the new name does not appear in the Administration Tool in offline mode. But the new name immediately appears in lists in Presentation Services and the Administration Tool. Users continue to see the permissions the role grants them.

Cause

References to the original role name persist in the repository enabling the role name to appear in the Administration Tool when working in offline mode.

Action

An administrator either restarts the BI Server or runs the Consistency Checker in the Administration Tool to update the repository with the new role name.

C.4 Resolving SSL Communication Problems

Behavior

Communication error. A process (the client) cannot communicate with another process (the server).

Action

When there is an SSL communication problem the client typically displays a communication error. The error can state only "client refused" with no further information. Check the server log file for the corresponding failure error message which typically provides more information about the issue.

Behavior

The following error message is displayed after the commit operation is performed using the BIDomain MBean (oracle.biee.admin:type=BIDomain, group=Service).

```
SEVERE: Element Type: DOMAIN, Element Id: null, Operation Result:
VALIDATION_FAILED, Detail Message: SSL must be enabled on AdminServer
before enabling on BI system; not set on server: AdminServer
```

Action

This message indicates that SSL has not been enabled on the Oracle WebLogic Server Managed Servers, which is a prerequisite step. For more information, see Section 5.2.2.5, "Disable HTTP".

C.5 Resolving Custom SSO Environment Issues

You might encounter issues when setting up custom SSO environments. For example, when setting up SSO with Windows Native Authentication and Active Directory, or with SiteMinder.

For more information, see article IDs 1287479.1 and 1274953.1 on My Oracle Support at:

https://support.oracle.com

C.6 Resolving RSS Feed Authentication When Using SSO

When attempting to read an Oracle BI RSS feed, trouble authenticating an RSS reader using SSO may stem from the way Oracle SSO is intercepting requests from that particular RSS reader. In this case Oracle cannot control the feed reader application. There are two scenarios, however, where SSO may be supportable:

- Using a browser-based RSS reader like Wizz RSS for Firefox, and using Firefox to log in to SSO before accessing the feed.
- Using Windows integrated authentication with an RSS reader that uses Internet Explorer.

  Firefox can support Windows authentication so you can use it in this case.

You must validate deployment strategies for your environment.

D

Managing Security for Dashboards and Analyses

This appendix explains how to manage security for dashboards and analyses such that users have only:

- Access to objects in the Oracle BI Presentation Catalog that are appropriate to them.
- Access to features and tasks that are appropriate to them.
- Access to saved customizations that are appropriate to them.

This appendix contains the following sections:

D.1 Managing Security for Users of Oracle BI Presentation Services

System administrators must configure a business intelligence system to ensure that all functionality (including administrative functionality) is secured so that only authorized users can access the system to perform appropriate operations. Administrators also must be able to configure the system to secure all middle-tier communications.

This overview section contains the following topics:

D.1.1 Where Are Oracle BI Presentation Services Security Settings Made?

Security settings that affect users of Presentation Services are made in the following Oracle Business Intelligence components:

- **Oracle BI Administration Tool** — Enables you to perform the following tasks:
  - Set permissions for business models, tables, columns, and subject areas.

  - Specify database access for each user.
  - Specify filters to limit the data accessible by users.
  - Set authentication options.

  For information, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

- **Oracle BI Presentation Services Administration** — Enables you to set privileges for users to access features and functions such as editing views and creating agents and prompts.
- **Oracle BI Presentation Services** — Enables you to assign permissions for objects in the Oracle BI Presentation Catalog.

  In previous releases, you could assign permissions to objects from the Presentation Services Administration pages. In this release, you set permissions either in the Catalog Manager or the Catalog page of Presentation Services. See *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* for information on assigning permissions in Presentation Services.
- **Catalog Manager** — Enables you to set permissions for Oracle BI Presentation Catalog objects. For information on the Catalog Manager, see "Configuring and Managing the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Note: Security Administrators should advise report users to not edit Subject Area security privileges within BI EE Answers. Data security should be enforced by the Security Administrator.

D.1.2 What Are the Security Goals in Oracle BI Presentation Services?

When maintaining security in Presentation Services, you must ensure the following:

- Only the appropriate users can sign in and access Presentation Services. You must assign sign-in rights and authenticate users through the BI Server.

  Authentication is the process of using a user name and password to identify someone who is logging on. Authenticated users are then given appropriate authorization to access a system, in this case Presentation Services. Presentation Services does not have its own authentication system; it relies on the authentication system that it inherits from the BI Server.

  All users who sign in to Presentation Services are granted the AuthenticatedUser Role and any other roles that they were assigned in Fusion Middleware Control.

  For information about authentication, see Section 1.3, "About Authentication".
- Users can access only the objects that are appropriate to them. You apply access control in the form of permissions, as described in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*.
- Users have the ability to access features and functions that are appropriate to them. You apply user rights in the form of privileges. Example privileges are "Edit systemwide column formats" and "Create agents."

  Users are either granted or denied a specific privilege. These associations are created in a privilege assignment table, as described in Section D.2.3, "Managing Presentation Services Privileges."

You can configure Oracle Business Intelligence to use the single sign-on feature from the web server. Presentation Services can use this feature when obtaining information for end users. For complete information on single sign-on, see Chapter 4, "Enabling SSO Authentication".

D.1.3 How Are Permissions and Privileges Assigned to Users?

When you assign permissions and privileges in Presentation Services, you can assign them in one of the following ways:

- To application roles — This is the recommended way of assigning permissions and privileges. Application roles provide much easier maintenance of users and their assignments. An application role defines a set of permissions granted to a user or group that has that role in the system's identity store. An application role is assigned in accordance with specific conditions. As such, application roles are granted dynamically based on the conditions present at the time authentication occurs.

  See Section 1.4.1, "About Application Roles" for information on application roles.

- To individual users — You can assign permissions and privileges to specific users, but such assignments can be more difficult to maintain and so this approach is not recommended.

- To Catalog groups — This approach is not recommended, but is maintained for backward compatibility with previous releases only.

  See Section D.2.2, "Working with Catalog Groups" for information on Catalog groups.

D.2 Using Oracle BI Presentation Services Administration Pages

You can use the Administration pages in Oracle BI Presentation Services to perform the tasks that are described in the following sections:

- Section D.2.1, "Understanding the Administration Pages"
- Section D.2.2, "Working with Catalog Groups"
- Section D.2.3, "Managing Presentation Services Privileges"
- Section D.2.4, "Managing Sessions in Presentation Services"

D.2.1 Understanding the Administration Pages

The main Administration page contains links that allow you to display other administration pages for performing various functions, including those related to users in Presentation Services. You can obtain information about all these pages by clicking the Help button in the upper-right corner.

Note: Use care if multiple users have access to the Administration pages, because they can overwrite each other's changes. Suppose UserA and UserB are both accessing and modifying the Manage Privileges page in Presentation Services Administration. If UserA saves updates to privileges while UserB is also editing them, then UserB's changes are overwritten by those that UserA saved.

D.2.2 Working with Catalog Groups

While you can continue to use Catalog groups, it is recommended that you move to the use of application roles rather than Catalog groups for organizing users. For more information, see "Migrating Catalog Groups to Application Roles".

In previous releases, Catalog groups were used for organizing users. Catalog group membership was used to determine the permissions and privileges that are associated with a user, either by explicit assignment or inheritance. In this release, Catalog groups have the following characteristics:

- Are referred to as Catalog groups.
- Can contain users, application roles, or other Catalog groups.
- Exist only for the purposes of compatibility with previous releases and only with Presentation Services.
- No longer have their own passwords.

Presentation Services administrators must ensure that the names of Catalog groups are different from any user IDs that are used to log in to Oracle BI Presentation Services. If a user and a Catalog group share the same name, then the user receives an Invalid Account message when attempting to log in to Oracle BI Presentation Services.

This section contains the following topics:

D.2.2.1 Migrating Catalog Groups to Application Roles

Although Catalog groups continue to function as in previous releases, they are not being supported in future releases. Oracle recommends that you start to migrate your Catalog groups to application roles now. Once you have migrated your Catalog groups to application roles, you must manually remove them from the Catalog.

This section explains how to migrate your Catalog groups from the Catalog to application roles, and remove them from the Catalog:

D.2.2.1.1 Generating Catalog Groups reports Before migrating Catalog groups, run reports that identify:

- Current Catalog groups and their members.
- Privileges that reference Catalog groups.
- Catalog paths that use or reference the Catalog groups.

To generate Catalog group reports:

1. Determine Catalog groups and membership Information.

Enter the following command:

```
runcat.cmd | runcat.sh -cmd report -offline <catalog path> -outputFile <output
file> -type "Accounts" -accounts "group;;*" -fields "Account Name:Group
Members" [-jaznFormat] [-excludeJaznHeader] [-expandGroups]
```

Generates a list of Catalog groups and their associated members within each group either in plain text or Jazn format.

Where:

- jaznFormat

  Generates a Jazn-formatted output file (used for importing new roles that are converted from existing groups).

- excludeJaznHeader

  Generates Jazn file without the header, so that you can insert the contents into an existing Jazn file.

- expandGroups

  Expands and lists the members of child Catalog groups or just lists the application role name.

2. Determine Catalog groups used in privileges that you maintain in the Presentation Services Manage Privileges page (see Section 2.6.3, "Setting Presentation Services Privileges for Application Roles").

   Enter the following command:

   ```
   runcat.cmd | runcat.sh -cmd report -offline <catalog path> -outputFile <output
   file> -folder /system/privs -type "Security ACL" -accountsInPrivilege
   "group;;*" -fields "Path:Privilege"
   ```

   Generates a list of privileges that reference Catalog groups.

3. Determine paths of Catalog objects that contain references to Catalog groups.

   Enter the following command:

   ```
   runcat.cmd | runcat.sh -cmd report -offline <catalog path> -outputFile <output
   file> -type "All" -accountsInACL "group;;*" -fields "Path:ACL"
   ```

   Generates a list of catalog paths that use or reference the Catalog groups.

D.2.2.1.2 Migrating Catalog Groups to Application Roles This section describes how to migrate Catalog groups to Application roles.

> **Note:** Because Catalog groups can inherit permissions from the parent, and application roles cannot, there is no direct mapping between Catalog groups and application roles.

Identifying Security Gaps

Please review the following sections for additional information on the behavioral differences that can occur when groups are replaced with application roles:

- Section D.3.1, "Rules for Determining a User's Privileges or Permissions"
- Section D.3.2, "Example of Determining a User's Privileges with Application Roles"

- Section D.3.3, "Example of Determining a User's Permissions with Application Roles"
- Section D.3.4, "Example of Determining a User's Privileges with Deprecated Catalog Groups"
- Section D.3.5, "Example of Determining a User's Permissions with Deprecated Catalog Groups"

When a Catalog object contains one or more Catalog groups, an automatic conversion from a group to role is error prone and may need manual intervention. During the migration we attempt to identify and log all potential security gaps, and recommend which Catalog objects would need to be examined further for potential security issues.

To migrate Catalog groups to application roles:

1. Identify the top level catalog folder from the following page.

   For example:

   http://example.com:9402/analytics/saw.dll?Admin

2. Stop Presentation Services, navigate to:

   DOMAIN_HOME/bitools/bin/

   For example, on UNIX, run the following command:

   ./stop.sh

3. Backup the catalog, because migration changes cannot be reversed.

   Use a tool such as tar or zip.

4. Migrate Catalog groups to application roles and export groups to a Jazn file format.

   Optionally control whether the new application roles are prefixed with '_ GRP2ROLE_'.

   Enter the following command:

   ```
   runcat.cmd/runcat.sh -cmd migrateWebcatGroupsToApproles -offline<catalog path>
   -outputFile <output JAZN File> [-noGroupPrefix]
   ```

   - Generates a Jazn file that you use to import the new roles.
   - Removes the catalog groups and replaces them with application roles during the upgrade.
   - Prefixes the new application roles unless you specify the -noGroupPrefix.

   Note: The migration log file can highlight the security gap during the migration as follows:

   When multiple catalog groups have a parent/child relationship, it is flagged as a potential object that needs closer scrutiny and perhaps manual intervention. See *ORACLE_HOME*/user_ projects/domains/bi/servers/obips1/logs/ migratewebcatgroups_ <timestamp>.log file for objects that may have security gaps.

   The file format is <Object path> for the group names that have a parent/child relationship.

D.2.2.1.3 Migrating Catalog Groups to Application Roles During Migration From 11*g* to 12*c*

Use this task when you move from 11*g* to 12*c*.

To migrate Catalog groups to application roles during migration from 11g to 12c:

1. Stop Presentation Services.
2. Backup the catalog prior to executing this command because migration changes cannot be reversed.

   Use a tool such as tar or zip.
3. Determine Catalog groups and membership Information.

   Enter the following command:

   ```
   runcat.cmd | runcat.sh -cmd report -offline <catalog path> -outputFile <output
   file> -type "Accounts" -accounts "group;;*" -fields "Account Name:Group
   Members" [-jaznFormat] [-excludeJaznHeader] [-expandGroups] [-noGroupPrefix]
   ```

   Generates a list of Catalog groups and their associated members within each group either in plain text or Jazn format.

   Where:

   - jaznFormat

     Generates a Jazn-formatted output file (used for importing new roles that are converted from existing groups).
   - excludeJaznHeader

     Generates Jazn file without the header, so that you can insert the contents into an existing Jazn file.
   - expandGroups

     Expands and lists the members of child Catalog groups or just lists the application role name.
   - noGroupPrefix

     Prefixes the new application roles unless you specify the -noGroupPrefix.
4. Migrate Catalog groups to application roles (during upgrade from 11*g* to 12*c*).

   Enter the following command:

   ```
   runcat.cmd/runcat.sh -cmd upgradeCatalog -offline<catalog path> [-migrateGroups
   <withPrefix | noPrefix>]
   ```

   - Optionally removes the catalog groups and replaces them with application roles during the upgrade.
   - Optionally determines if the newly replaced application roles will use a prefix or not.
5. Import the Jazn file created in step3 "Determine Catalog groups and membership Information." back into your security system.

D.2.2.1.4 Removing Migrated Application Roles

To remove migrated application roles:

For information, see "Deleting an Application Role".

D.2.2.2 Creating Catalog Groups

Oracle **strongly** recommends that you do not create any new Catalog groups in Release 12.2.1 and later.

Although Catalog groups continue to function as in previous releases, they are not being supported in future releases. Oracle recommends that you start to migrate your Catalog groups to application roles now. Once you have migrated your Catalog groups to application roles, you must go to each and every object and then right click to remove the Catalog groups manually.

To create Catalog groups:

1. From the Home page in Presentation Services, select **Administration**.
2. Click the **Manage Catalog Groups** link.
3. Click **Create a New Catalog Group**.
4. In the Add Group dialog, enter a name for the group.
5. Use the shuttle control to select the Catalog groups, users, and application roles to include in this group.

   Tip: It is best practice to not include application roles in Catalog groups, to avoid complex group inheritance and maintenance situations. In particular do not add the AuthenticatedUser Role to any other Catalog groups that you create. This ensures that only the desired Catalog groups (and users) have the specified permissions and privileges, by preventing users or authenticated users from unintentionally inheriting permissions and privileges from another Catalog group.

6. Click **OK**.

D.2.2.3 Deleting Catalog Groups

To delete Catalog groups:

This only removes the groups, but not the internal references from privileges and other catalog objects.

1. From the Home page in Presentation Services, select **Administration**.
2. Click the **Manage Catalog Groups** link.
3. On the Manage Catalog Groups page, select the one or more groups to delete.

   To help you locate the group that you want, enter text in the **Name** field and click **Search**.

4. Click **Delete Selected Groups**.
5. Click **OK** to confirm the deletion.

D.2.2.4 Editing Catalog Groups

To edit Catalog groups:

1. From the Home page in Presentation Services, select **Administration**.
2. Click the **Manage Catalog Groups** link.
3. On the Manage Catalog Groups page, select the group to edit.

To help you locate the group that you want, enter text in the **Name** field and click **Search**.

You can click the **More Groups** button to display the next 25 groups in the list.

4. In the Edit Group dialog, change the name or add or remove application roles, Catalog groups, and users.
5. Click **OK**.

D.2.3 Managing Presentation Services Privileges

This section contains the following topics about Presentation Services privileges:

- Section D.2.3.1, "What Are Presentation Services Privileges?"
- Section D.2.3.2, "Setting Presentation Services Privileges for Application Roles"
- Section D.2.3.3, "Default Presentation Services Privilege Assignments"

D.2.3.1 What Are Presentation Services Privileges?

Presentation Services privileges control the rights that users have to access the features and functionality of Presentation Services. Privileges are granted or denied to specific application roles, individual users, and Catalog groups using a privilege assignment table.

Like permissions, privileges are either explicitly set or are inherited through role or group membership. Explicitly denying a privilege takes precedence over any granted, inherited privilege. For example, if a user is explicitly denied access to the privilege to edit column formulas, but is a member of an application role that has inherited the privilege, then the user cannot edit column formulas.

Privileges are most commonly granted to the BIContentAuthor or BIConsumer roles. This allows users access to common features and functions of Presentation Services. While you can continue to grant privileges to Catalog groups, it is recommended that you switch the grants to application roles.

D.2.3.2 Setting Presentation Services Privileges for Application Roles

You can set Presentation Services privileges for application roles, individual users, and Catalog groups from the Presentation Services Administration Manage Privileges page.

For more information, see Section 2.6.3, "Setting Presentation Services Privileges for Application Roles".

D.2.3.3 Default Presentation Services Privilege Assignments

Table D–1 lists the privileges that you can manage, along with the application role that is granted access to that privilege by default. For additional information, reference links are also provided in the table.

These privileges apply to the Oracle Business Intelligence infrastructure. If your organization uses prebuilt applications, then some privileges might be preconfigured. For more information, see the documentation for the application.

Note: When building KPIs, KPI watchlists, or within Oracle Scorecard and Strategy Management, a combination of privileges might be required to perform specific tasks. See Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding."

Note: To login to an Oracle BI EE connection from SmartView you must have at least the following BI Presentation Service privileges (for more information, see Table D–1):

- Access SOAP
- Access CatalogService Service
- Access SecurityService Service
- Access Oracle BI for MS Office

You must also have access to open the **Shared** Catalog folder.

Table D–1 Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to Dashboards	Allows users to view dashboards.	BI Consumer	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "What Are Dashboards?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Answers	Allows users to access the analysis editor.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "What Are Analyses?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and for Displaying and Processing Data in Views" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to BI Composer	Allows users to access the BI Composer wizard.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "What Is BI Composer?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Manually Changing Presentation Settings" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to Delivers	Allows users to create and edit agents.	BI Content Author	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "About Controlling Access to Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Briefing Books	Allows users to view and download briefing books.	BI Consumer	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Adding Content to New or Existing Briefing Books" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Modifying the Table of Contents for PDF Versions of Briefing Books" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Mobile	Allows users to access Presentation Services from the Oracle Business Intelligence Mobile application.	BI Consumer	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Getting Started with Oracle BI Mobile" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Mobile*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to Administration	Allows users to access the administration pages in Presentation Services.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring Application Roles and Users" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Segments	Allows users to access segments in Oracle's Siebel Marketing.	BI Consumer	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ *Oracle Marketing Segmentation Guide* ▪ "Configuring for Connections to the Marketing Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Segment Trees	Allows users to access segment trees in Oracle's Siebel Marketing.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ *Oracle Marketing Segmentation Guide* ▪ "Configuring for Connections to the Marketing Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to List Formats	Allows users to access list formats in Oracle's Siebel Marketing.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ *Oracle Marketing Segmentation Guide* ▪ "Configuring for Connections to the Marketing Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Metadata Dictionary	Allows users to access the metadata dictionary information for subject areas, folders, columns, and levels.	BI Service Administrator	"Providing Access to Metadata Dictionary Information" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Oracle BI for Microsoft Office	Shows the Download BI Desktop Tools link with the **Oracle BI for MS Office** option.	BI Consumer	▪ "Integrating with Microsoft Office" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.2, "Access to Oracle BI for Microsoft Office Privilege"
Access	Access to Oracle BI Client Installer	Allows users to download the Oracle BI Client Tools installer, which installs the Business Intelligence Administration Tool and the Oracle Business Intelligence Job Manager.	BI Consumer	▪ "Downloading BI Desktop Tools" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Installing and Deinstalling Oracle Business Client Tools" in *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence* ▪ "What System Administration Tools Manage Oracle Business Intelligence?" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Catalog Preview Pane UI	Allows users access to the catalog preview pane, which shows a preview of each catalog object's appearance.	BI Consumer	▪ "Previewing How Views Are Displayed on a Dashboard" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Preview Pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Export	Allows users access to all export functionality, such as the **Export** link. In addition, to allow users access to the dashboard export to Excel functionality, that is, the **Export entire dashboard** and **Export current page** options, you also must set the **Export Entire Dashboard To Excel** and **Export Single Dashboard Page To Excel** privileges, respectively.	BI Consumer	▪ "Exporting and Copying Results" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Integrating with Microsoft Office" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Manually Configuring for Export" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to KPI Builder	Allows users to create KPIs.	BI Content Author	▪ "How Do I Create a KPI?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Table D–2, " Privileges Required for KPI Tasks"
Access	Access to Scorecard	Allows users access to Oracle BI Scorecard, and this also allows users access to KPI watchlists.	BI Consumer	▪ "How Do I Create a Scorecard?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Table D–4, " Privileges Required for Scorecard and Scorecard Object Tasks"
Actions	Create Navigate Actions	Set the privileges that determine whether Actions functionality is available to users and specify which user types can create Actions.	BI Content Author	▪ "Actions that Navigate to Related Content" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Actions	Create Invoke Actions	Set the privileges that determine whether Actions functionality is available to users and specify which user types can create Actions.	BI Content Author	▪ "Actions that Invoke Operations, Functions or Precesses in External Systems" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions"
Actions	Save Actions Containing Embedded HTML	Allows users to embed HTML code in the customization of web service action results.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Who Can Create Actions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions" ▪ "Action Options dialog: Action Results tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Catalog	Change Permissions	Allows users to modify permissions for catalog objects.	BI Content Author	▪ "Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Catalog	Toggle Maintenance Mode	Shows the Toggle Maintenance Mode link on the Presentation Services Administration page, which allows users to turn maintenance mode on and off. In maintenance mode, the catalog is read-only; no one can write to it.	BI Service Administrator	"Administration page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Manage Sessions	Shows the Manage Sessions link on the Presentation Services Administration page, which displays the Manage Sessions page in which users manage sessions.	BI Service Administrator	"Administration: Manage Sessions page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Admin: General	Manage Dashboards	Allows users to create and edit dashboards, including editing their properties.	BI Service Administrator	▪ "Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Building and Using Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	See Session IDs	Allows users to see session IDs on the Manage Sessions page.	BI Service Administrator	"Administration: Manage Sessions page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Issue SQL Directly	Shows the Issue SQL link on the Presentation Services Administration page, which displays the Issue SQL page in which users enter SQL statements.	BI Service Administrator	"Administration: Issue SQL page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	View System Information	Allows users to view information about the system at the top of the Administration page in Presentation Services.	BI Service Administrator	"Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Performance Monitor	Allows users to monitor performance.	BI Service Administrator	"Diagnostics and Performance Monitoring" in *Oracle Fusion Middleware Administrator's and Developer's Guide for Oracle Business Intelligence Publisher*
Admin: General	Manage Agent Sessions	Shows the Manage Agent Sessions link on the Presentation Services Administration page, which displays the Manage Agent Sessions page in which users manage agent sessions.	BI Service Administrator	▪ "Administration: Manage Agent Sessions page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Manage Device Types	Shows the Manage Device Types link on the Presentation Services Administration page, which displays the Manage Device Types page in which users manage device types for agents.	BI Service Administrator	▪ "Administration: Manage Device Types page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Managing Device Types for Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Admin: General	Manage Map Data	Shows the Manage Map Data link on the Presentation Services Administration page, which displays the Manage Map Data page in which users edit layers, background maps, and images for map views.	BI Service Administrator	■ "Administration: Manage Map Data page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Administering Maps" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	See Privileged Errors	Allows users to see privileged error messages. Users can see detailed error messages about database connections or other details when lower level components fail.	BI Service Administrator	■ "Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Diagnosing and Resolving Issues in Oracle BI" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	See SQL Issued in Errors	Allows users to see SQL statements that are returned by the BI Server in error messages.	BI Consumer	■ "Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Diagnosing and Resolving Issues in Orals BI" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Manage Global Variables	Allows users to manage (add, update, and delete) global variables. Global variables are created during the process of creating analyses.	BI Service Administrator	"What Are Global Variables?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Manage Marketing Jobs	Shows the Manage Marketing Jobs link on the Presentation Services Administration page, which displays the Marketing Job Management page in which users manage marketing jobs.	BI Content Author	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ *Oracle Marketing Segmentation Guide* ■ "Configuring for Connections to the Marketing Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Admin: General	Manage Marketing Defaults	Shows the Manage Marketing Defaults link on the Presentation Services Administration page, which displays the Manage Marketing Defaults page in which users manage defaults for Oracle's Siebel Marketing application.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ *Oracle Marketing Segmentation Guide* ▪ "Configuring for Connections to the Marketing Content Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	Manage Catalog Groups	Shows the Manage Catalog Groups link on the Presentation Services Administration page, which displays the Manage Catalog Groups page in which users edit Catalog groups.	BI Service Administrator	▪ "Administration: Manage Catalog Groups page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	Manage Privileges	Shows the Manage Privileges link on the Presentation Services Administration page, which displays the Manage Privileges page in which users manage the privileges that are described in this table.	BI Service Administrator	▪ "Assigning Ownership of Objects" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	Set Ownership of Catalog Objects	Allows users to take ownership of catalog items that they did not create and do not own. Shows the "Set ownership of this item" link for individual objects and the "Set ownership of this item and all subitems" link for folders on the Properties page.	BI Service Administrator	▪ "Administration: Manage Catalog Groups page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Admin: Security	User Population - Can List Users	Allows users to see the list of users for which they can perform tasks such as assigning privileges and permissions.	BI Consumer, BI System	▪ "What Are Permissions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Oracle WebLogic Server Administration Console" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	User Population - Can List Groups	Allows users to see the list of groups for which they can perform tasks such as assigning privileges and permissions.	BI Consumer, BI System	▪ "What Are Permissions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Oracle WebLogic Server Administration Console" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	User Population - Can List Application Roles	Allows users to see the list of application roles for which they can perform tasks such as assigning privileges and permissions.	BI Consumer, BI System	▪ "What Are Permissions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Oracle WebLogic Server Administration Console" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	Access to Permissions Dialog	Allows users to access the Permissions dialog, where they can set permissions for a catalog object.	BI Consumer	▪ "What Are Permissions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Oracle WebLogic Server Administration Console" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Briefing Book	Add To or Edit a Briefing Book	Allows users to see the **Add to Briefing Book** link on dashboard pages and analyses and the **Edit** link in briefing books.	BI Content Author	"Working with Briefing Books" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Briefing Book	Add to snapshot briefing book	Allows users to add content to a briefing book as a snapshot (that is, the **Snapshot** option for **Content Type** is available in the Save Briefing Book Content dialog and in the Page Properties dialog).	BI Consumer	"Adding Content to New or Existing Briefing Books" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Briefing Book	Download Briefing Book	Allows users to download briefing books.	BI Consumer	▪ "Downloading Briefing Books" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Modifying the Table of Contents for PDF Versions of Briefing Books" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	Personal Storage	Allows users to have write access to their own My Folders folders and create content there. If users do not have this privilege, then they can receive email alerts but cannot receive dashboard alerts.	BI Consumer	▪ "Where Do I Store and Manage Oracle BI EE Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Securing Catalog Objects for Tenants" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Catalog	Reload Metadata	Allows users to click the **Reload Server Metadata** link from the Refresh menu in the toolbar of the Subject Areas pane.	BI Service Administrator	▪ "Subject Areas pane (Toolbar - Refresh button)" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Using Online and Offline Repository Modes" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	See Hidden Items	Allows users to see hidden items in catalog folders. Users can also select the **Show Hidden Items** box on the Catalog page.	BI Content Author	▪ "Catalog page (Show Hidden Items)" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Controlling Presentation Object Visibility" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	Create Folders	Allows users to create folders in the catalog.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Catalog	Archive Catalog	Allows users to archive the folders and objects in the catalog.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	Unarchive Catalog	Allows users to unarchive catalog objects that have been archived previously.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	Upload Files	Allows users to upload files into an existing catalog.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Integrating with Microsoft Office Using Oracle Business Intelligence Add-in for Microsoft Office" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions of Catalog Objects" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Catalog	Perform Global Search	Allows user to search the catalog using the basic catalog search, which is included by default with the Oracle BI Enterprise Edition installation.	BI Content Author	▪ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring for Searching with Oracle Secure Enterprise Search" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Catalog	Perform Extended Search	Allows users to search the catalog using the full-text search. To provide full-text search, the administrator must have integrated Oracle BI Enterprise Edition with Oracle Secure Enterprise Search.	BI Content Author	▪ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring for Searching with Oracle Secure Enterprise Search" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring for Searching with Oracle Secure Endeca Server" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Conditions	Create Conditions	Allows users to create or edit named conditions.	BI Content Author	▪ "What Are Named Conditions?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Dashboards	Save Customizations	Allows users to save and view later dashboard pages in their current state with their most frequently used or favorite choices for items.	BI Consumer	▪ "What Are Saved Customizations for Dashboard Pages?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.5, "Controlling Access to Saved Customization Options in Dashboards"
Dashboards	Assign Default Customizations	Allows users to save and view later dashboard pages in their current state with their most frequently used or favorite choices for items.	BI Content Author	▪ "What Are Saved Customizations for Dashboard Pages?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.5, "Controlling Access to Saved Customization Options in Dashboards"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Dashboards	Create Bookmark Links	Allows users to create bookmark links by showing the **Create Bookmark Link** option on the Page Options menu on a dashboard page, but only if the ability to create bookmark links has been enabled.	BI Consumer	▪ "About Creating Links to Dashboard Pages" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Enabling the Ability to Create Links to Dashboard Pages" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Dashboards	Create Prompted Links	Allows users to create prompted links by showing the **Create Prompted Link** option on the Page Options menu on a dashboard page, but only if the ability to create prompted links has been enabled.	BI Consumer	▪ "About Creating Links to Dashboard Pages" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Enabling the Ability to Create Links to Dashboard Pages" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Dashboards	Export Entire Dashboard To Excel	Allows users to download an entire dashboard to Excel by showing the **Export entire dashboard** option on the Page Options menu on a dashboard page. Note that you also must set the **Access to Export** privilege.	BI Consumer	▪ "Exporting and Copying Results" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Enabling the Ability to Export Dashboard Pages to Oracle BI Publisher" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Dashboards	Export Single Dashboard Page To Excel	Allows users to download a single dashboard page to Excel by showing the **Export current page** option on the Page Options menu on a dashboard page. Note that you also must set the **Access to Export** privilege.	BI Consumer	▪ "Exporting and Copying Results" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Enabling the Ability to Export Dashboard Pages to Oracle BI Publisher" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Formatting	Save SystemWide Column Formats	Allows users to save systemwide defaults when specifying formats for columns.	BI Service Administrator	"Saving Formatting Defaults" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Home and Header	Access Home Page	Allows users to access the home page from the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "What Is the Oracle BI EE Home Page?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Home page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	Access Catalog UI	Allows users to access the catalog from the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Catalog page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Home and Header	Access Catalog Search UI	Allows users to access the search fields from the global header.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Search pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	Simple Search Field	Allows users to access the **Search** field in the global header.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Search pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Home and Header	Advanced Search Link	Allows users to access the Advanced link in the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Search pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Catalog page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	Open Menu	Allows users to access the **Open** menu from the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Open dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	New Menu	Allows users to access the **New** menu from the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Home and Header	Help Menu	Allows users to access the **Help** menu from the global header.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	Dashboards Menu	Allows users to access the **Dashboards** menu from the global header.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Opening and Using Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Making Advanced Configuration Changes for Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Home and Header	Favorites Menu	Allows users to access the **Favorites** menu from the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "What Are Favorites?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Making Advanced Configuration Changes for Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	My Account Link	Allows users to access the **My Account** link when they click on their **Signed In As** name in the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "My Account dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Home and Header	Custom Links	Allows users to access the custom links that the administrator added to the global header.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
My Account	Access to My Account	Allows users to access the My Account dialog.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Acting for Other Users" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "My Account dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
My Account	Change Preferences	Allows users to access the Preferences tab of the My Account dialog.	BI Consumer	▪ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Preferences" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "My Account dialog: Preferences tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
My Account	Change Delivery Options	Allows users to access the Delivery Options tab of the My Account dialog.	BI Consumer	■ "What Is the Oracle BI EE Global Header?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "What Are Devices and Delivery Profiles?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Setting Preferences" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "My Account dialog: Delivery Options tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Providing Custom Links in Presentation Services" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Create Views	Allows users to create views.	BI Content Author	■ "What Are Views?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring for Displaying and Processing Data in Views" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Create Prompts	Allows users to create prompts.	BI Content Author	■ "Prompting in Dashboards and Analyses" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring for Prompts" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Answers	Access Advanced Tab	Allows users to access the Advanced tab in the Analysis editor.	BI Content Author	▪ "What Is the Analysis Editor?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Examining the Logical SQL Statements for Analyses" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Logical SQL Reference" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Analysis editor: Advanced tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Edit Column Formulas	Allows users to edit column formulas.	BI Content Author	▪ "Editing the Formula for a Column" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Edit Column Formula dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Save Content with HTML Markup	In addition to allowing HTML markup in analyses and dashboards, this also allows users to save mission and vision statements in Oracle Scorecard and Strategy Management.	BI Service Administrator	▪ "Working with HTML Markup" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.3, "Save Content with HTML Markup Privilege"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Answers	Enter XML and Logical SQL	Allows users to use the Advanced SQL tab.	BI Content Author	■ "What Is the Analysis Editor?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Examining the Logical SQL Statements for Analyses" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Logical SQL Reference" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Analysis editor: Advanced tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Edit Direct Database Analysis	Allows users to create and edit requests that are sent directly to the back-end data source.	BI Service Administrator	■ "Working with Direct Database Requests" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Setting Privileges for Direct Requests" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Create Analysis from Simple SQL	Allows users to select the **Create Analysis from Simple SQL** option in the Select Subject Area list.	BI Service Administrator	■ "Examining the Logical SQL Statements for Analyses" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Logical SQL Reference" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Analysis editor: Advanced tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Analysis Simple SQL Statement dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Answers	Create Advanced Filters and Set Operations	Allows users access to the following components: ▪ **Combine results based on union, intersection, and difference operations** button on the Criteria tab in the Analysis editor. This option allows users to combine columns from one or more subject areas using Set operations such as Union or Intersect. ▪ **is based on the results of another analysis** option in the New Filter dialog. This option allows users to use a saved analysis as a filter. ▪ **Convert this filter to SSL** option in the New Filter dialog. This option allows users to create and edit the SQL statements for a column filter in an analysis.	BI Content Author	▪ "Combining Columns Using Set Operations" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Using a Saved Analysis as a Filter" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Creating and Editing the SQL Statements for a Column Filter in an Analysis" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Save Filters	Allows users to save filters.	BI Content Author	▪ "Saving Filters as Inline or Named" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Filters pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Save Column	Allows users to save columns to the catalog for reuse in other analyses.	BI Content Author	▪ "Saving Columns to the Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Selected Columns pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Answers	Add EVALUATE_ PREDICATE Function	Allows users to add the EVALUATE_PREDICATE function to an inline filter.	BI Content Author	■ "Working with the EVALUATE_PREDICATE Function" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Filters pane (Add EVALUATE_PREDICATE Function component)" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Execute Direct Database Analysis	Allows users to issue requests directly to the back-end data source.	BI Service Administrator	■ "Working with Direct Database Requests" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Analysis editor: Criteria tab (Direct Database Request Components)" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*
Delivers	Create Agents	Allows users to create agents.	BI Content Author	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Creating Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Delivers	Publish Agents for Subscription	Allows users to publish agents for subscription.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Controlling Access to Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Delivers	Deliver Agents to Specific or Dynamically Determined Users	Allows users to deliver agents to other users.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Controlling Access to Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Delivers	Chain Agents	Allows users to chain agents.	BI Content Author	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Controlling Access to Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Delivers	Modify Current Subscriptions for Agents	Allows users to modify the current subscriptions for agents, including unsubscribing users.	BI Service Administrator	▪ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Controlling Access to Agents" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Agents" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Proxy	Act As Proxy	Allows users to act as proxy users for other users.	Denied: BI Consumer	▪ "Acting for Other Users" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Act As dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.6, "Enabling Users to Act for Others"
RSS Feeds	Access to RSS Feeds	Allows users to subscribe to and receive RSS feeds with alerts and contents of folders. If Presentation Services uses the HTTPS protocol, then the RSS Reader that you use must also support the HTTPS protocol.	BI Content Author	▪ "Subscribing to an RSS Feed for Alerts" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Alerts dialog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create/Edit Scorecards	Allows users to create and edit scorecards.	BI Content Author	▪ "How Do I Create a Scorecard?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
Scorecard	View Scorecards	Allows users to view scorecards. A user needs either this privilege or the Scorecard - Create/Edit Scorecards privilege to access the KPI watchlist editor to either view or edit KPI watchlists.	BI Consumer	▪ "How Do I Create a Scorecard?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create/Edit Objectives	Allows users to create and edit objectives.	BI Content Author	▪ "Creating Objectives" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
Scorecard	Create/Edit Initiatives	Allows users to create and edit initiatives.	BI Content Author	▪ "Creating Initiatives" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create Views	Allows users to create and edit scorecard objects that present and analyze corporate strategy, such as vision and mission statements, strategy maps, cause & effect maps, and so on.	BI Content Author	▪ "What Are Scorecard Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
Scorecard	Create/Edit Causes and Effects Linkages	Allows users to create and edit cause and effect relationships.	BI Content Author	▪ "What Are Cause and Effect Maps?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create/Edit Perspectives	Allows users to create and edit perspectives.	BI Service Administrator	▪ "Creating Custom Perspectives" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
Scorecard	Add Annotations	Allows users to add comments to KPIs and scorecard components.	BI Consumer	▪ "Configuring the Repository for Comments and Status Overrides" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
Scorecard	Override Status	Allows users to override statuses of KPIs and scorecard components.	BI Consumer	▪ "Configuring the Repository for Comments and Status Overrides" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create/Edit KPIs	Allows users to create and edit KPIs and KPI watchlists.	BI Content Author	▪ "What Are Key Performance Indicators (KPIs)?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Understanding Watchlists" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Write Back to Database for KPI	Allows users to enter and submit a KPI's actual and target settings values to the repository.	BI Consumer	■ "What Are Target Settings?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Column Properties dialog: Write Back tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ■ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding" ■ "Configuring for Write Back in Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Add Scorecard Views to Dashboards	Allows users to add scorecard views (such as strategy trees) and KPI watchlists to dashboards.	BI Consumer	▪ "Adding Scorecard Objects to Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "About Scorecard Privileges and Permissions" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring the Repository for Oracle Scorecard and Strategy Management" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D.2.3.3.4, "Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding"
List Formats	Create List Formats	Allows users to create list formats in Oracle's Siebel Marketing.	BI Content Author	*Oracle Marketing Segmentation Guide*
List Formats	Create Headers and Footers	Allows users to create headers and footers for list formats in Oracle's Siebel Marketing.	BI Content Author	▪ *Oracle Marketing Segmentation Guide* ▪ "Specifying Dashboard Page Defaults Including Headers and Footers" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
List Formats	Access Options Tab	Allows users to access the Options tab for list formats in Oracle's Siebel Marketing.	BI Content Author	*Oracle Marketing Segmentation Guide*
List Formats	Add/Remove List Format Columns	Allows users to add and remove columns for list formats in Oracle's Siebel Marketing.	BI Service Administrator	*Oracle Marketing Segmentation Guide*
Segmentation	Create Segments	Allows users to create segments in Oracle's Siebel Marketing.	BI Content Author	*Oracle Marketing Segmentation Guide*
Segmentation	Create Segment Trees	Allows users to create segment trees in Oracle's Siebel Marketing.	BI Content Author	*Oracle Marketing Segmentation Guide*
Segmentation	Create/Purge Saved Result Sets	Allows users to create and purge saved result sets in Oracle's Siebel Marketing.	BI Service Administrator	*Oracle Marketing Segmentation Guide*
Segmentation	Access Segment Advanced Options Tab	Allows users to access the Segment Advanced Options tab in Oracle's Siebel Marketing.	BI Service Administrator	*Oracle Marketing Segmentation Guide*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Segmentation	Access Segment Tree Advanced Options Tab	Allows users to access the Segment Tree Advanced Options tab in Oracle's Siebel Marketing.	BI Service Administrator	*Oracle Marketing Segmentation Guide*
Segmentation	Change Target Levels within Segment Designer	Allows users to change target levels within the Segment Designer in Oracle's Siebel Marketing.	BI Service Administrator	*Oracle Marketing Segmentation Guide*
Mobile	Enable Local Content	Allows users of Oracle Business Intelligence Mobile to save local copies of BI content to their mobile devices.	BI Consumer	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Getting Started with Oracle BI Mobile" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Mobile*
Mobile	Enable Search	Allows users of Oracle Business Intelligence Mobile to search the catalog.	BI Consumer	■ "Managing Objects in the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "How Can I Search for Objects?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Performing Searches" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Mobile* ■ "Configuring for Searching with Oracle Secure Enterprise Search" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access SOAP	Allows users to access various web services.	BI Consumer, BI System	■ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ■ "AccessControlToken Structure" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Impersonate as System User	Allows users to impersonate a system user using a web service.	BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "impersonate() Method" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access MetadataService Service	Allows users to access the MetadataService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "MetadataService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access ReportEditingService Service	Allows users to access the ReportEditingService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "ReportEditingService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access ConditionEvaluationService Service	Allows users to access the ConditionEvaluationService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "ConditionService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Access CatalogIndexingService Service	Allows users to access the CatalogIndexingService web service to index the Oracle BI Presentation Catalog for use with full-text search.	BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Common Steps for Configuring Full-Text Search" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access DashboardService Service	Allows users to access the DashboardService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ Section D, "Managing Security for Dashboards and Analyses"
SOAP	Access SecurityService Service	Allows users to access the SecurityService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "SecurityService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access SchedulerService Service	Allows users to access the SchedulerService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "SchedulerService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access Tenant Information	Internal only.	BI System	"Working with Tenants" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Access ScorecardMetadataService Service	Allows users to access the ScorecardMetadataService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "ScorecardMetadataService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "ScorecardMetadataService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access ScorecardAssessmentService Service	Allows users to access the ScorecardAssessmentService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "ScorecardAssessmentService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access HtmlViewService Service	Allows users to access the HtmlViewServiceService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "HtmlViewService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access CatalogService Service	Allows users to access the CatalogService web service.	BI Consumer, BI System	*Oracle Fusion Middleware Java API Reference for Oracle Identity Manager*
SOAP	Access iBotService Service	Allows users to access the iBotService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "iBotService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Access XmlGenerationService Service	Allows users to access the XmlGenerationService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "XMLQueryExecutionOptions Structure" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access JobManagementService Service	Allows users to access the JobManagementService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "JobManagementService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access KPIAssessmentService Service	Allows users to access the KPIAssessmentService web service.	BI Consumer, BI System	▪ "Introduction to Oracle Business Intelligence Web Services" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "KPIAssessmentService Service" in *Oracle Fusion Middleware Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
Subject Area (*by its name*)	Access within Oracle Business Intelligence	Allows users to access the specified subject area within the Oracle Business Intelligence editor.	BI Content Author	▪ "Viewing Metadata Information from the Subject Areas Pane" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Setting Permissions for Presentation Layer Objects" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Providing Access to Metadata Dictionary Information" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit AnalyzerView	Allows users to access the Analyzer view.	BI Service Administrator	▪ "Administration: Manage Privileges page" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Using the Analyzer for Excel" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Publisher*
Views	Add/Edit Column SelectorView	Allows users to create and edit column selector views.	BI Content Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Compound LayoutView	Allows users to create and edit compound layout views.	BI Content Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Compound Layout" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit GraphView	Allows users to create and edit graph views.	BI Service Administrator	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit FunnelView	Allows users to create and edit funnel graph views.	BI Content Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit GaugeView	Allows users to create and edit gauge views.	BI Content Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Micro Chart View	Allows users to create and edit microcharts.	BI Content Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit FiltersView	Allows users to create and edit filter views.	BI Content Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Dashboard PromptView	Allows users to create and edit dashboard prompt views.	BI Content Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Performance TileView	Allows users to create and edit performance tile views.	BI Content Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Static TextView	Allows users to create and edit static text views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Static Text editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Legend View	Allows users to create and edit legend views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Legend editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit MapView	Allows users to create and edit map views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit NarrativeView	Allows users to create and edit narrative views.	BI Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Results tab: Narrative editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit No ResultsView	Allows users to create and edit no result views.	BI Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Analysis Properties dialog: Results Display tab" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Pivot TableView	Allows users to create and edit pivot table views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Using Fusion Middleware Control to Set Configuration Options for Data in Tables and Pivot Tables" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Report PromptView	Allows users to create and edit prompt views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Create SegmentView	Allows users to create and edit segment views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Create Segment editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Selection StepsView	Allows users to create and edit selection steps views.	BI Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Logical SQLView	Allows users to create and edit logical SQL views.	BI Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "What Types of Logical SQL View Are Available?" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit TableView	Allows users to create and edit table views.	BI Author	▪ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Using Fusion Middleware Control to Set Configuration Options for Data in Tables and Pivot Tables" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* ▪ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Create Target ListView	Allows users to create and edit target list views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Create Target List editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit TickerView	Allows users to create and edit ticker views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Ticker editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit TitleView	Allows users to create and edit title views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: Title editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit TrellisView	Allows users to create and edit trellis views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit View SelectorView	Allows users to create and edit view selector views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: View Selector editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Table D–1 (Cont.) Privileges and Default Settings for the Oracle Business Intelligence Infrastructure

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit TreemapView	Allows users to create and edit treemap views.	BI Author	■ "Adding Views for Display in Dashboards" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Results tab: *Data View* editor" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring and Managing Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Write Back	Write Back to Database	Grants the right to write data into the data source.	Denied: BI Consumer	■ "Modifying Values and Performing Write Back" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "About Handling Errors for Write Back" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring for Write Back in Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Write Back	Manage Write Back	Grants the right to manage write back requests.	BI Service Administrator	■ "Modifying Values and Performing Write Back" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "About Handling Errors for Write Back" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* ■ "Configuring for Write Back in Analyses and Dashboards" in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

D.2.3.3.1 Access to Oracle BI Enterprise Edition Actions You must set the Action privileges, which determine whether the Actions functionality is available to users and specify which user types can create Actions. The following list describes these privileges:

- **Create Navigate Actions** — Determines which users can create a Navigate action type. The sessions of users who are denied this privilege do not contain any of the user interface components that allow them to create Navigate Actions. For example, if a user is denied this privilege and chooses to create an action from the Oracle BI Enterprise Edition global header, the dialog where the user selects an action type does not include the Navigate Actions options (Go to BI Content, Go to a Web Page, and so on). However, users who are denied this privilege can add saved actions to analyses and dashboards. And, users who are denied this privilege can execute an action from an analysis or dashboard that contains an action.
- **Create Invoke Actions** — Determines which users can create an Invoke action type. The sessions of user who are denied this privilege do not contain any of the user interface components that allow them to create Invoke Actions. For example, if a user is denied this privilege and chooses to access the agent editor's Actions tab and clicks the **Add New Action** button, the dialog where the user selects the action type does not include the Invoke Actions options (Invoke a Web Service, Invoke an HTTP Request, and so on). However, users who are denied this privilege can add saved actions to analyses and dashboards. And, users who are denied this privilege can execute an action from an analysis or dashboard that contains an action.
- **Save Actions Containing Embedded HTML** — Determines which users can embed HTML code in the customization of web service action results. Use care in assigning this privilege, because it poses a security risk to allow users to run HTML code.

D.2.3.3.2 Access to Oracle BI for Microsoft Office Privilege

The Access to Oracle BI for Microsoft Office privilege shows the following option for the **Download BI Desktop Tools** link in the Get Started area of the Oracle BI EE Home page:

- **Oracle BI for MS Office**: Downloads the installation file for the Oracle BI Add-in for Microsoft Office.

The Access to Oracle BI for Microsoft Office privilege does not affect the display of the **Copy** link for analyses. The link is always available there.

The location of the installation file to download for Oracle BI for Microsoft Office is specified by default in the BIforOfficeURL element in the instanceconfig.xml file. For more information on using Oracle BI for Microsoft Office and the **Copy** option, see *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*.

D.2.3.3.3 Save Content with HTML Markup Privilege

By default, Presentation Services is secured against cross-site scripting (XSS). Securing against XSS escapes input in fields in Presentation Services and renders it as plain text. For example, an unscrupulous user can use an HTML field to enter a script that steals data from a page.

By default, end users cannot save content that is flagged as HTML; instead only administrators who have the Save Content with HTML Markup privilege can save content that contains HTML code. Users that have the Save Content with HTML Markup privilege can save an image with the "fmap" prefix. If users try to save an image with the "fmap" prefix when they do not have this privilege assigned, then they see an error message.

Users with this privilege can also save mission and vision statements in Oracle Scorecard and Strategy Management.

D.2.3.3.4 Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding

The ability to perform certain tasks when building KPIs, and KPI watchlists, or within Oracle

Scorecard and Strategy Management (such as, viewing or creating scorecards or contacting owners) generally requires a combination of privileges. Table D–2, Table D–3, and Table D–4 list the following information for KPIs, KPI watchlists, and Oracle Scorecard and Strategy Management, respectively:

- Task Object (for example, Action link or KPI chart)
- Task (for example, "Contact owner from a dashboard" or "Follow a link in the Scorecard editor")
- Privileges required to perform the task (for example, "Delivers - Create Agents" or "Access - Access to Dashboards"). You must have each privilege listed to perform the specific task.

The privileges required to perform these tasks have been grouped into sets where applicable, and the set name has been included (rather than the individual privileges) along with any additional required privileges. The set names and privileges included within each set are:

- **Edit_scorecard_set1**

  Privileges include:

  - Access - Access to Scorecard
  - Scorecard - Create/Edit Scorecards

- **View_or_edit_scorecard_set2**

  Privileges include:

  - Access - Access to Scorecard
  - Scorecard - Create/Edit Scorecards or Scorecard - View Scorecards

- **View_KPI_watchlist_on_dashboard_set3**

  Privileges include:

  - Access - Access to Dashboards
  - Access - Access to Scorecard

- **Edit_KPI_with_KPI_Builder_set4**

  Privileges include:

  - Access - Access to KPI Builder
  - Scorecard - Create/Edit KPIs
  - Subject Area - *<name of subject area>*

- **Edit_KPI_watchlist_with_standalone_KPI_watchlist_editor_set5**

  Privileges include:

  - View_or_edit_scorecard_set2
  - Access - Access to KPI Builder
  - Scorecard - Create/Edit KPIs

- **View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6**

  Privileges include:

  - Access - Access to Scorecard
  - Scorecard - Create/Edit Scorecards or Scorecard - View Scorecards

Table D–2 lists the combination of privileges that are required for KPI tasks.

Table D–2 Privileges Required for KPI Tasks

Task Object	Task	Privileges Required to Perform the Task
Action link	**Create**, **edit**, or **delete** on a KPI within the Scorecard editor using the KPI editor[1] tab	▪ Actions - Create Navigate Actions ▪ Edit_scorecard_set1 ▪ Edit_KPI_with_KPI_Builder_set4
Action link	**Create**, **edit**, or **delete** from within the KPI editor	▪ Actions - Create Navigate Actions ▪ Edit_KPI_with_KPI_Builder_set4
Agent	**Create** an agent for a KPI within the Scorecard editor	▪ Access - Access to Access to Delivers ▪ Delivers - Create Agents ▪ Edit_scorecard_set1
Business owner	**Modify** within the Scorecard editor using the KPI editor tab	▪ Admin: Security - User Population - Can List Users ▪ Edit_KPI_with_KPI_Builder_set4
Business owner	**Modify** from within the KPI editor	▪ Admin: Security - User Population - Can List Users ▪ Edit_KPI_with_KPI_Builder_set4
KPI	**Create** or **edit** within the Scorecard editor using the KPI editor tab	▪ Edit_scorecard_set1 ▪ Edit_KPI_with_KPI_Builder_set4 Note that you must have read/write permission on the folder for which you create the KPI, and at least read permission on all ancestor directories.
KPI	**Create**, **edit**, or **view** from within the KPI editor Note that there is no read-only mode in the KPI editor.	▪ Edit_KPI_with_KPI_Builder_set4 Note that you must have read/write permission on the folder for which you create the KPI and at least read permission on all ancestor directories.
KPI	**Open** to see an Answers analysis from the Oracle BI EE Home page, Favorites list, or Catalog browser	No specific Access, Scorecard, or Subject area privileges are required.
KPI dimensioned target value (target setting)	**Edit** within the KPI watchlist on a dashboard	▪ Scorecard - Write Back to Database for KPI ▪ View_KPI_watchlist_on_dashboard_set3

Table D–2 (Cont.) Privileges Required for KPI Tasks

Task Object	Task	Privileges Required to Perform the Task
KPI dimensioned target value (target setting)	**Edit** within a scorecard view[2] on a dashboard	▪ Access - Access to Dashboards ▪ Scorecard - Write Back to Database for KPI ▪ View_or_edit_scorecard_set2
Related document	**Add**, **edit**, or **delete** a related document from within the KPI editor	▪ Edit_KPI_with_KPI_Builder_set4
Related document	**Add**, **edit**, or **delete** a related document within the Scorecard editor using the KPI editor tab	▪ Edit_scorecard_set1 ▪ Edit_KPI_with_KPI_Builder_set4

Table D–3 lists the combination of privileges that are required for KPI watchlist tasks.

Table D–3 Privileges Required for KPI Watchlist Tasks

Task Object	Task	Privileges Required to Perform the Task
<*Device*> (for example, email, pager, or digital phone)	**Contact owner** from a KPI watchlist on a dashboard	▪ Access - Access to Delivers ▪ Admin: Security - User Population - Can List Users ▪ Delivers - Create Agents ▪ View_KPI_watchlist_on_dashboard_set3
<*Device*>	**Contact owner** from within the standalone KPI watchlist editor[3]	▪ Access - Access to Delivers ▪ Admin: Security - User Population - Can List Users ▪ Delivers - Create Agents ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Action link	**Invoke** from a KPI watchlist on a dashboard	▪ View_KPI_watchlist_on_dashboard_set3 Note that you must enable pop-ups in your browser.
Action link	**Invoke** from within the standalone KPI watchlist editor	▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Analyze link	**Follow** an analyze link from a KPI watchlist view on a dashboard	▪ Access - Access to Answers ▪ View_KPI_watchlist_on_dashboard_set3 Note that you must enable pop-ups in your browser.

Table D–3 (Cont.) Privileges Required for KPI Watchlist Tasks

Task Object	Task	Privileges Required to Perform the Task
Analyze link	**Follow** an analyze link from within the standalone KPI watchlist editor	▪ Access - Access to Answers ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6 Note that you must enable pop-ups in your browser.
Annotation	**Add** from a KPI watchlist on a dashboard	▪ Scorecard - Add Annotations ▪ View_KPI_watchlist_on_dashboard_set3
Annotation	**Add** from within the standalone KPI watchlist editor	▪ Scorecard - Add Annotations ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Annotation	**View** from a KPI watchlist on a dashboard	▪ View_KPI_watchlist_on_dashboard_set3
Annotation	**View** from within the standalone KPI watchlist editor	▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Business owner	**Modify** the business owner of a KPI watchlist from within the standalone KPI watchlist editor	▪ Admin: Security - User Population - Can List Users ▪ Edit_KPI_watchlist_with_standalone_KPI_watchlist_editor_set5
Business owner	**View** the business owner in a KPI watchlist from within the standalone KPI watchlist editor	▪ Admin: Security - User Population - Can List Users ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
KPI chart	**View** a KPI chart from a KPI watchlist on a dashboard	▪ Access - Access to Answers ▪ View_KPI_watchlist_on_dashboard_set3
KPI chart	**View** a KPI chart from within the standalone KPI watchlist editor	▪ Access - Access to Answers ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
KPI dimensioned target value (target setting)	**Edit** a KPI's dimensioned target value in the KPI watchlist within the Scorecard editor	▪ Scorecard - Write Back to Database for KPI ▪ View_or_edit_scorecard_set2
KPI dimensioned target value (target setting)	**Edit** a KPI's dimensioned target value in the KPI watchlist from within the standalone KPI watchlist editor	▪ Scorecard - Write Back to Database for KPI ▪ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6

Table D–3 (Cont.) Privileges Required for KPI Watchlist Tasks

Task Object	Task	Privileges Required to Perform the Task
KPI watchlist	**Add** to a dashboard	■ Access - Access to Dashboards ■ Scorecard - Add Scorecard Views to Dashboards ■ View_or_edit_scorecard_set2
KPI watchlist	**Create** or **edit** within the Scorecard editor	■ Scorecard - Create Views ■ View_or_edit_scorecard_set2
KPI watchlist	**Create** or **edit** from within the standalone KPI watchlist editor	■ Edit_KPI_watchlist_with_standalone_KPI_watchlist_editor_set5 Note that you must have read/write permission on the folder under which you create the KPI watchlist and at least read permission on all ancestor directories.
KPI watchlist	**Open in read-only** from within the standalone KPI watchlist editor	■ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
KPI watchlist	**View** on a dashboard	■ View_KPI_watchlist_on_dashboard_set3
Related document	**Follow** a related document link from within the standalone KPI watchlist editor	■ View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Related document	**Add**, **edit**, or **delete** a related document from within the standalone KPI watchlist editor	■ Edit_KPI_watchlist_with_standalone_KPI_watchlist_editor_set5 ■ Actions - Create Navigate Actions
Related document	**Add**, **edit**, or **delete** a related document for a KPI watchlist	■ Edit_scorecard_set1 ■ Actions - Create Navigate Actions

Table D–4 lists the combination of privileges that are required for scorecard and scorecard object tasks.

Table D–4 Privileges Required for Scorecard and Scorecard Object Tasks

Task Object	Task	Privileges Required to Perform the Task
<*Device*> (for example, email, pager, or digital phone)	**Contact owner** in a scorecard view on a dashboard	■ Access - Access to Dashboards ■ Access - Access to Delivers ■ Admin: Security - User Population - Can List Users ■ Delivers - Create Agents ■ View_or_edit_scorecard_set2

Table D–4 (Cont.) Privileges Required for Scorecard and Scorecard Object Tasks

Task Object	Task	Privileges Required to Perform the Task
<Device>	**Contact owner** within the Scorecard editor	▪ Access - Access to Delivers ▪ Admin: Security - User Population - Can List Users ▪ Delivers - Create Agents ▪ View_or_edit_scorecard_set2
Action link	**Invoke** in a scorecard view on a dashboard	▪ Access - Access to Dashboards ▪ View_or_edit_scorecard_set2 Note that you must enable pop-ups in your browser.
Action link	**Invoke** within the Scorecard editor	▪ View_or_edit_scorecard_set2
Action link on an object in the Strategy or Initiatives panes	**Create**, **edit**, or **delete** within the Scorecard editor	▪ Actions - Create Navigate Actions ▪ View_or_edit_scorecard_set2
All scorecard nodes[4], views, and documents (excludes KPI editor)	**View in read-only** within the Scorecard editor	▪ View_or_edit_scorecard_set2
Analyze link	**Follow** an analyze link in a scorecard view on a dashboard	▪ Access - Access to Answers ▪ Access - Access to Dashboards ▪ View_or_edit_scorecard_set2 Note that you must enable pop-ups in your browser.
Analyze link	**Follow** an analyze link within the Scorecard editor	▪ Access - Access to Answers ▪ View_or_edit_scorecard_set2 Note that you must enable pop-ups in your browser.
Annotation	**Add** in a scorecard view on a dashboard	▪ Access - Access to Dashboards ▪ Scorecard - Add Annotations ▪ View_or_edit_scorecard_set2
Annotation	**Add** in a scorecard view within the Scorecard editor	▪ Scorecard - Add Annotations ▪ View_or_edit_scorecard_set2
Annotation	**View** in a scorecard view on a dashboard	▪ Access - Access to Dashboards ▪ View_or_edit_scorecard_set2
Annotation	**View** within the Scorecard editor	▪ View_or_edit_scorecard_set2
Business owner	**Modify** within the Scorecard editor	▪ Admin: Security - User Population - Can List Users ▪ Edit_scorecard_set1
Business owner	**View** within the Scorecard editor	▪ Admin: Security - User Population - Can List Users ▪ View_or_edit_scorecard_set2

Table D–4 (Cont.) Privileges Required for Scorecard and Scorecard Object Tasks

Task Object	Task	Privileges Required to Perform the Task
Causal linkage	**Create**, **edit**, or **delete** within the Scorecard editor	■ Scorecard - Create/Edit Cause and Effects Linkages ■ Edit_scorecard_set1
Dimensioned status override of a scorecard node	**Override** a KPI's dimensioned status (or cancel an override) from a scorecard view on a dashboard	■ Access - Access to Dashboards ■ Scorecard - Override Status ■ View_or_edit_scorecard_set2 Note that you must also be the KPI's business owner to override the status that is set in the KPI editor.
Dimensioned status override of a scorecard node	**Override** a KPI's dimensioned status (or cancel an override) within the Scorecard editor	■ Scorecard - Override Status ■ View_or_edit_scorecard_set2 Note that you must also be the KPI's business owner to override the status that is set in the KPI editor.
Dimensioned status override of a scorecard node	**View** a KPI's dimensioned status in a scorecard view on a dashboard	■ Access - Access to Dashboards ■ View_or_edit_scorecard_set2
Dimensioned status override of a scorecard node	**View** a KPI's dimensioned status in a scorecard view within the Scorecard editor	■ View_or_edit_scorecard_set2
Filter	**Add a user** to the filter in a scorecard smart watchlist within the Scorecard editor	■ Admin: Security - User Population - Can List Users ■ Edit_scorecard_set1
Filter	**Filter on a user** in the scorecard smart watchlist on a dashboard	■ Access - Access to Dashboards ■ Admin: Security - User Population - Can List Users ■ View_or_edit_scorecard_set2
Filter	**Filter on a user** in the scorecard smart watchlist within the Scorecard editor	■ Admin: Security - User Population - Can List Users ■ View_or_edit_scorecard_set2
Initiatives node[5]	**Create**, **edit**, or **delete** within the Scorecard editor using the Initiatives tab or KPI Details tab	■ Scorecard - Create/Edit Initiatives ■ Edit_scorecard_set1
KPI chart	**View** in a scorecard view on a dashboard	■ Access - Access to Answers ■ Access - Access to Dashboards ■ View_or_edit_scorecard_set2
KPI chart	**View** within the Scorecard editor	■ Access - Access to Answers ■ View_or_edit_scorecard_set2

Table D–4 (Cont.) Privileges Required for Scorecard and Scorecard Object Tasks

Task Object	Task	Privileges Required to Perform the Task
Mission or vision statement	Create or edit within the Scorecard editor	▪ Access - Access to Answers ▪ Answers - Save Content with HTML Markup ▪ Scorecard - Create Views ▪ Edit_scorecard_set1
Permissions dialog	**Modify** within the Scorecard editor	▪ Admin: Catalog - Change Permissions ▪ Edit_scorecard_set1 ▪ Security: Access to Permissions Dialog
Perspective	**Create**, **edit**, or **delete** within the Scorecard editor	▪ Scorecard - Create/Edit Perspectives ▪ Edit_scorecard_set1
Related document	**Add**, **edit**, or **delete** for a scorecard node or scorecard view within the Scorecard editor	▪ Edit_scorecard_set1 ▪ Actions - Create Navigate Actions ▪ Scorecard - Create/Edit <*object*> (where <*object*> is the specific object type, such as objective, initiative, or KPI)
Related document	**Follow** a related document link within the Scorecard editor	▪ View_or_edit_scorecard_set2
Scorecard	**Create**	▪ Edit_scorecard_set1 Note that you must have read/write permission on the scorecard folder and at least read permission on all ancestor directories.
Scorecard	**Edit** using the Scorecard editor	▪ Edit_scorecard_set1 Note that you must have read/write permission on the scorecard folder and at least read permission on all ancestor directories.
Scorecard view	**Add** to a dashboard	▪ Access - Access to Dashboards ▪ Scorecard - Add Scorecard Views to Dashboards ▪ View_or_edit_scorecard_set2
Scorecard view (excludes mission and vision statements and KPI watchlists)	**Create**, **edit**, or **delete** within the Scorecard editor	▪ Scorecard - Create Views ▪ Edit_scorecard_set1
Scorecard view	**View** on a dashboard	▪ Access - Access to Dashboards ▪ View_or_edit_scorecard_set2
Settings dialog	**Modify** (or **view**) settings	▪ Edit_scorecard_set1

Table D–4 (Cont.) Privileges Required for Scorecard and Scorecard Object Tasks

Task Object	Task	Privileges Required to Perform the Task
Strategy node[6]	**Create**, **edit**, or **delete** within the Scorecard editor using the Objective tab or KPI Details tab	▪ Scorecard - Create/Edit Objectives ▪ Edit_scorecard_set1

1. The KPI editor is also known as the KPI Builder.
2. A scorecard view (also known as a "scorecard document") is an Oracle BI EE catalog object which meets the following criteria:
   - Displays in the **Scorecard Documents** pane within the Scorecard editor. See *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* for additional information.
   - Is tied to and can only be edited in the specific scorecard where it was created.
   - Displays the scorecard's strategy and initiative information.
   - Consists of the following view types:
     - Cause and effect map
     - Custom view
     - Mission statement
     - Smart watchlist
     - Strategy map
     - Strategy tree
     - Strategy contribution wheel
     - Vision statement
3. The standalone KPI watchlist editor is the KPI watchlist editor used outside of the Scorecard editor. In other words, it is not embedded within a Scorecard editor tab.
4. Scorecard node is an objective or initiative that belongs to the Strategy pane tree or Initiatives pane tree of a scorecard, or a KPI belonging to an initiative or objective within these panes, respectively.
5. Initiatives node is an initiative or KPI within the **Initiatives** pane. See Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition for additional information.
6. Strategy node is an objective or KPI within the **Strategy** pane. See Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition for additional information.

D.2.4 Managing Sessions in Presentation Services

Using the Session Management page in Presentation Services Administration, you can view information about active users and running analyses, cancel requests, and clear the cache.

To manage sessions in Presentation Services:

1. From the Home page in Presentation Services, select **Administration**.

2. Click the **Manage Sessions** link.

   The Session Management screen is displayed with the following tables:

   – The Sessions table, which gives information about sessions that have been created for users who have logged in:

   – The Cursor Cache table, which shows the status of analyses:

To cancel all running requests:

1. Click **Cancel Running Requests**.
2. Click **Finished**.

To cancel one running analysis:

- In the Cursor Cache table, identify the analysis and click the **Cancel** link in the **Action** column.

  The user receives a message indicating that the analysis was canceled by an administrator.

To clear the web cache:

1. In the Cursor Cache table, identify the analysis and click **Close All Cursors**.
2. Click **Finished**.

To clear the cache entry associated with an analysis:

- In the Cursor Cache table, identify the analysis and click the **Close** link in the **Action** column.

To view the query file for information about an analysis:

- In the Cursor Cache table, identify the analysis and click the **View Log** link.

> **Note:** Query logging must be turned on for data to be saved in this log file.

D.3 Determining a User's Privileges and Permissions in Oracle BI Presentation Services

Oracle BI Presentation Services privileges and Oracle BI Presentation Services Catalog item permissions, use an Access Control List (ACL) to control who has privilege to access Presentation Services functionality and what permissions any given user can have on Presentation Services Catalog items. Privileges are set using the Administration pages in Oracle BI Presentation Services. Permissions are set for Presentation Services Catalog objects through the Analytics user interface, or the Catalog Manager user interface.

When you try to access functionality in Presentation Services, the appropriate privilege is checked; for example, to view the Oracle Business Intelligence page you must have the Access to Answers privilege. Also, when you try to perform any action on a Presentation Services Catalog item, that item's permissions are checked; for example, to view an item in Oracle Business Intelligence, the item's permissions are checked to see if you have read access.

There are 3 types of records that may be added to an ACL:

- Individual user records

It is difficult to administer individual user records especially when there might be thousands of users, and hundreds of thousands of Catalog items.

- 10*g* Catalog group records

  Catalog groups exist purely for backwards compatibility, and are not recommended. They should not be used, instead you should change to using application roles.

- 11g application roles records

  These are the recommended way of managing ACLs.

Oracle Business Intelligence determines user access by sequentially checking 3 types of records. A user's effective privileges or permissions are deduced using the ACL records, looking for an explicit record for the user (if there is one); then looking for any records with the Catalog groups, of which the user is directly and indirectly a member; and then looking for any records with application roles granted to the user either explicitly or implicitly.

This section contains the following topics:

D.3.1 Rules for Determining a User's Privileges or Permissions

The following tasks describe the sequential checks completed to determine a user's effective privileges and permissions.

Note: Step 1 takes precedence over Step 2, which takes precedence over Step 3, which takes precedence over Step 4, which takes precedence over Step 5.

Note: Within an individual step, a privilege ACL record that is Denied always takes precedence over any other grants. Similarly, within an individual step, a permission ACL record that has No Access always takes precedence over any access grant.

Semantically, the privilege Denied is the same as the permission No Access, and so the term deny will be used interchangeably for both privileges and permissions.

D.3.1.1 Task 1 - Check for an explicit record for this user

The following sequence represents the checks completed for a user record.

1. If there is an explicit record for this user, then return that access. Done.

2. If there is no explicit record for this user. Go to Task 2 - Check for records for this user's Catalog groups (deprecated behavior for 10g backwards compatibility only).

D.3.1.2 Task 2 - Check for records for this user's Catalog groups (deprecated behavior for 10g backwards compatibility only)

The following sequence represents the checks completed for a user's Catalog groups.

1. Get the set of all Catalog groups this user is directly, explicitly in.

   This set does not include Catalog groups that this user is implicitly in.

   This set includes:

   - Catalog groups assigned through the Presentation Services Administration Page.
   - Catalog groups assigned through the WEBGROUPS BI session variable.
   - Any Catalog group that has an application role as a member, where that application role has been granted (either explicitly or implicitly) to this user.

   Note: This functionality was initially provided to help migration of 10*g* Catalog groups to 11*g* application roles, rather than force immediate conversion of all Catalog groups to application roles.

2. Check for any ACL record that matches any of the current set of Catalog groups as follows:

   - If there are any records that deny access, then return access denied. Done.
   - Else, if there are any records that grant access, return the union of all those access grants. For example, if one Catalog group has read access, and another Catalog group has write access, then the user has read and write access. Done.
   - Else, no records matched the current set of Catalog groups.

3. Get the parent set of all Catalog groups of the current set of Catalog groups. In other words, get all Catalog groups that the current set of Catalog groups are themselves members of explicitly. This parent set becomes the new current set of Catalog groups.

4. If the parent set is not empty, go to "Check for any ACL record that matches any of the current set of Catalog groups as follows:".

   - Thus, explicit Catalog groups take precedence over (override) implicit Catalog groups.
   - Similarly, implicit "parent" Catalog groups take precedence over implicit "grandparent" Catalog groups; implicit "grandparent" Catalog groups take precedence over implicit "great-grandparent" Catalog groups; and so on.

   Note: The logic for permission inheritance for Catalog groups is different to the logic for permission inheritance for application roles.

5. Else there were no records for this user's Catalog groups. Go to Task 3 - Check records for this user's application roles.

D.3.1.3 Task 3 - Check records for this user's application roles

The following sequence represents the checks completed for a user's application roles.

1. Get all the application roles for this user, including both direct, explicit application roles and indirect, implicit application roles.

   For example, if a user is explicitly granted the BI Author application role, then the user also implicitly has the BI Consumer application role too.

2. Check for any ACL record that matches any of the set of application roles.
   - If any records deny access, then return access denied. Done.
   - Else, if any records grant access, return the union of all those access grants. So if one application role had read access, and another application role had write access, then the user has read and write access. Done.
   - Else there are no records for this user's application roles.
3. Else there were no records for this user's application roles. Go to Task 4 - Fall back default behavior.

D.3.1.4 Task 4 - Fall back default behavior

The following sequence represents the checks completed for a specific application role called Authenticated User.

1. If there is a record for the authenticated user application role, return that record's access. Done.

   Note: The Authenticated User application role is deliberately not included in the list of application roles for a user in Task 3 - Check records for this user's application roles, even though that user does technically have this application role too.

2. Else there is no record for the special application role. Go to Task 5 - No matching records at all.

D.3.1.5 Task 5 - No matching records at all

Return access denied. Done.

D.3.2 Example of Determining a User's Privileges with Application Roles

Figure D–1 shows an example of how privileges are determined with application roles. At the top of the diagram is a rectangle labelled User1, which specifies that User1 has been explicitly given the application roles Executive and BI Author. Attached beneath the User1 rectangle are two more rectangles - one on the left that represents the Executive role and one on the right that represents the BI Author role.

- The Executive role rectangle specifies that Executive is granted the Access to Administration privilege, and that the application roles Finance and Sales have in turn been given to Executive.
- The BI Author role rectangle specifies that BI Author is granted the Catalog privilege, is Denied the Agents privilege, and that the application role BI Consumer has in turn been given to BI Author.

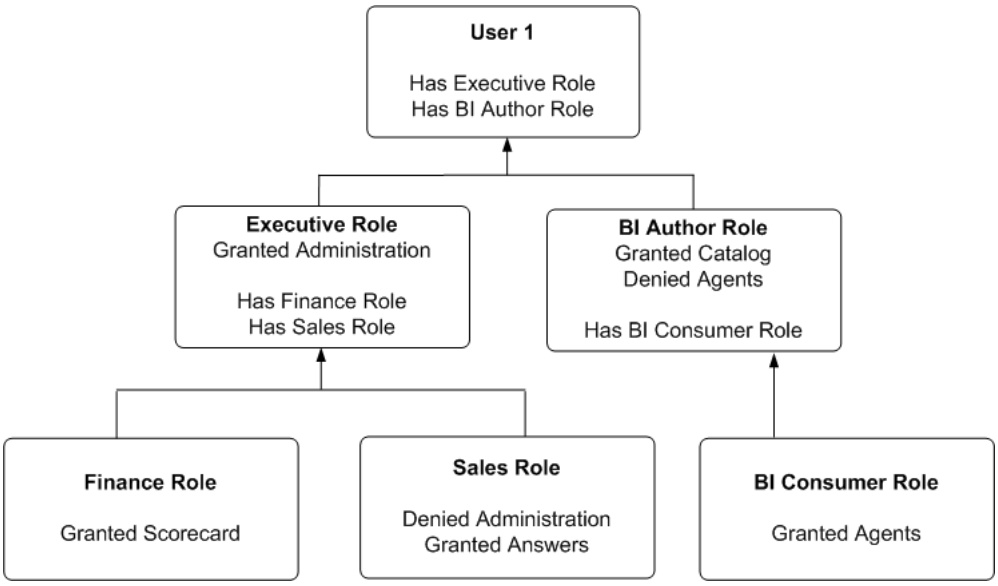
Attached beneath the Executive Role rectangle are two more rectangles - one on the left that represents the Finance role and one on the right that represents the Sales role:

- The Finance Role rectangle specifies that the Finance role is granted the Scorecard privilege.
- The Sales Role rectangle specifies that Sales is Denied the Access to Administration privilege and granted the Access to Answers privilege.

And finally, attached beneath the BI Author Role rectangle is a rectangle that represents the BI Consumer role:

- The BI Consumer Role rectangle specifies that BI Consumer is granted the Catalog privilege and is granted the Agents privilege.

Figure D–1 Example of Determining a User's Privileges Using Application Roles



In this example:

- User1 explicitly has the Executive role, and thus implicitly has Finance role and also Sales role.
- User1 also explicitly has the BI Author role, and thus also implicitly has BI Consumer role.
- So User1's flattened list of application roles is Executive, BI Author, Finance, Sales and BI Consumer.
- The effective privileges from Executive Role are Denied Administration privilege, granted Scorecard privilege, and granted Answers privilege. The Sales' Denied Administration privilege takes precedence over Executive's granted privilege, as Deny always takes precedence.
- The effective privileges from the BI Author role are granted Catalog privilege, and Denied Agents privilege. The BI Author's Denied Agents privilege takes precedence over BI Consumer's granted, as deny always takes precedence.

The total privileges granted to User1 are as follows:

- Denied Administration privilege, because the privilege is specifically denied for Sales.
- Granted Scorecard privilege.
- Granted Answers privilege.

- Granted Catalog privilege.
- Denied Agents privilege, because the privilege is specifically denied for BI Author.

D.3.3 Example of Determining a User's Permissions with Application Roles

Figure D–2 shows an example of how permissions are determined with application roles. At the top of the diagram is a rectangle labelled User1, which specifies that User1 has been explicitly given the application roles Executive and BI Author. Attached beneath the User1 rectangle are two more rectangles - one on the left that represents Executive Role and one on the right that represents BI Author Role.

- The Executive Role rectangle specifies that Executive has no access to DashboardA, and that the application roles Finance and Sales have in turn been given to Executive.
- The BI Author Role rectangle specifies that BI Author role has open access to DashboardD, has no access to DashboardE, and that the BI Consumer role has in turn been given to BI Author.

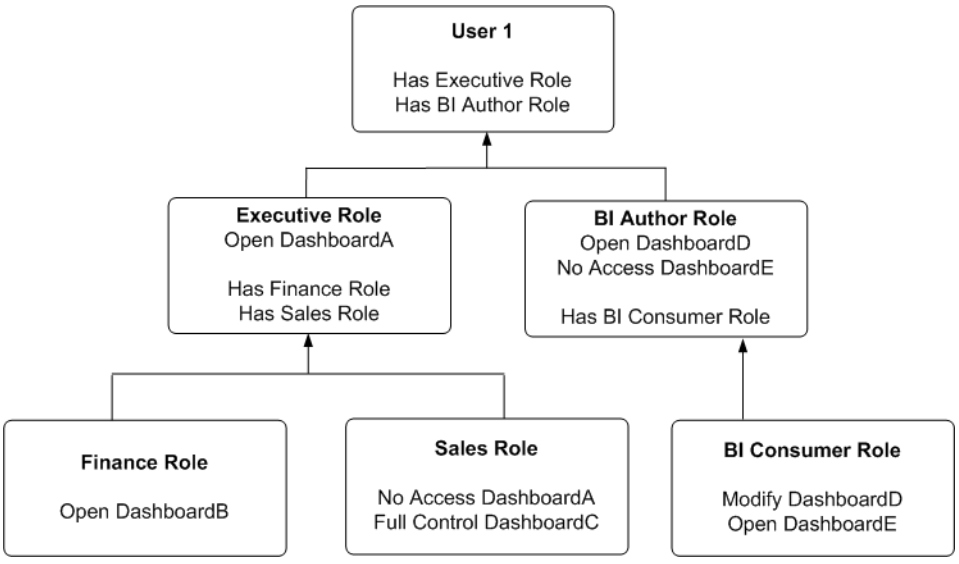
Attached beneath the Executive Role rectangle are two more rectangles - one on the left that represents Finance role and one on the right that represents Sales role:

- The Finance Role rectangle specifies that Finance role has open access to DashboardB.
- The Sales Role rectangle specifies that Sales role has no access to DashboardA and full control of DashboardC.

And finally, attached beneath the BI Author Role rectangle is a rectangle that represents BI Consumer role:

- The BI Consumer Role rectangle specifies that BI Consumer role has modify access to DashboardD and open access to DashboardE.

Figure D–2 Example of Determining a User's Permissions Using Application Roles



In this example:

- User1 explicitly has Executive role, and thus implicitly has Finance role and also Sales role.

- User1 also explicitly has BI Author role, and thus also implicitly has BI Consumer role.
- So User1's flattened list of application roles is Executive, BI Author, Finance, Sales and BI Consumer.
- The effective permissions from Executive role are no access to DashboardA, open access to DashboardB, and full control for DashboardC. Note Sales role's No Access to DashboardA takes precedence over Executive role's Open, as Deny always takes precedence.
- The effective privileges from BI Author role are Open&Modify access to DashboardD, and No Access to DashboardE. Note BI Author role's No Access to DashboardE takes precedence over BI Consumer role's Open, as Deny always takes precedence.

The total permissions and privileges granted to User1 are as follows:

- No Access to DashboardA, because access is specifically denied for Sales role.
- Open Access to DashboardB.
- Full Control for DashboardC.
- Open&Modify access to DashboardD, the union of Role2's and Role5's access.
- No Access to DashboardE, because access is specifically denied for BI Author role.

D.3.4 Example of Determining a User's Privileges with Deprecated Catalog Groups

Figure D–3 shows an example of how privileges are determined with Catalog groups. At the top of the diagram is a rectangle labelled User1, which specifies that User1 is an explicit member of the Catalog groups, Manager Group and Canada Group. Attached beneath the User1 rectangle are two more rectangles - one on the left that represents Manager Group and one on the right that represents Canada Group.

- The Manager Group rectangle specifies that Manager Group is granted the Access to Administration privilege, and that the Manager Group is in turn itself a member of both Marketing Group and Sales Group.
- The Canada Group rectangle specifies that Canada Group is granted the Catalog privilege, is denied the Agents privilege, and that the Canada Group is in turn itself a member of the Americas Group.

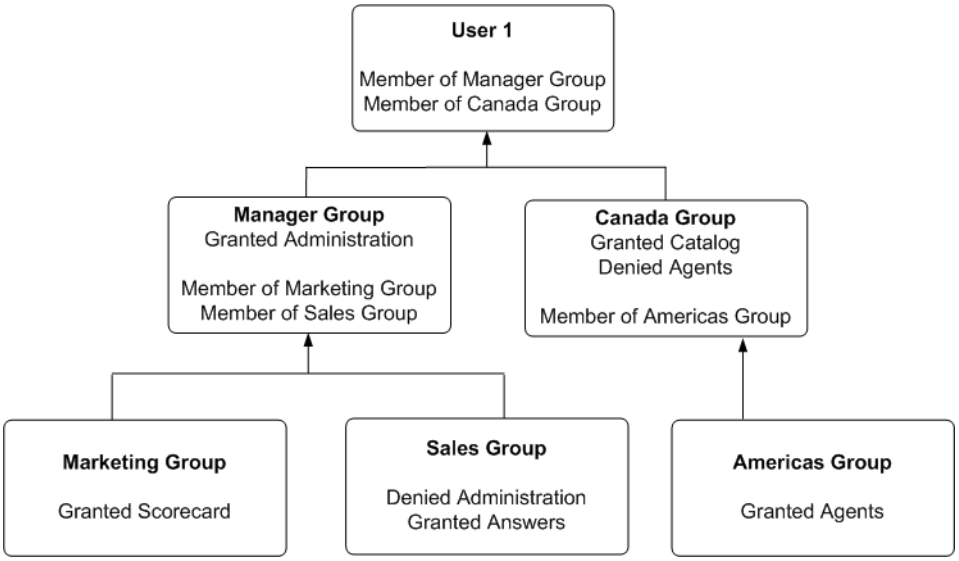
Attached beneath the Manager Group rectangle are two more rectangles - one on the left that represents Marketing Group and one on the right that represents Sales Group:

- The Marketing Group rectangle specifies that Marketing Group is granted the Scorecard privilege.
- The Sales Group rectangle specifies that Sales Group is denied the Access to Administration privilege and granted the Access to Answers privilege.

And finally, attached beneath the Canada Group rectangle is a rectangle that represents the Americas Group:

- The Americas Group rectangle specifies that Americas Group is granted the Catalog privilege and is granted the Agents privilege.

Figure D–3 Example of Determining a User's Privileges Using Deprecated Catalog Groups



In this example:

- User1 is explicitly in the Manager Group, and thus is implicitly in the Marketing Group and Sales Group too.
- User1 also is explicitly in the Canada Group, and thus is also implicitly in the Americas Group too.
- So User1's initial list of Catalog groups is Manager Group and Canada Group. If required, User1's parent list of Catalog groups is Marketing Group, Sales Group and Americas Group. The grandparent list of Catalog groups is empty, as the Catalog group hierarchy is only two levels deep.
- The effective privileges from the Manager Group are granted the Administration privilege, granted Scorecard privilege, and granted the Answers privilege. Note explicit Manager Group's record for Administration takes precedence over implicit Sale Group's record, as the more immediate ancestor Catalog group always takes precedence over more distant ancestor Catalog group.
- The effective privileges from the Canada group are granted the Catalog privilege, and denied Agents privilege. Note explicit Canada Group's records for both Catalog and Agents takes precedence over implicit Americas Group's records, as the more immediate ancestor Catalog group always takes precedence over more distant ancestor Catalog group.

The total privileges granted to User1 are as follows:

- Granted Access to Administration privilege, because the Manager Group takes precedence over Sales group.
- Granted Scorecard privilege.
- Granted Answers privilege.
- Granted Catalog privilege, because Canada Group takes precedence over Americas Group.
- Denied Agents privilege, because the Canada Group takes precedence over Americas.

D.3.5 Example of Determining a User's Permissions with Deprecated Catalog Groups

Figure D–4 shows an example of how permissions are determined with Catalog groups. At the top of the diagram is a rectangle labelled User1, which specifies that User1 is an explicit member of Catalog groups Manager Group and Canada Group. Attached beneath the User1 rectangle are two more rectangles - one on the left that represents Manager Group and one on the right that represents Canada Group.

- The Manager Group rectangle specifies that Manager Group has open access to DashboardA, and that the Manager Group is in turn itself a member of both Marketing Group and Sales Group.
- The Canada Group rectangle specifies that Canada Group has open access to DashboardD, has no access to DashboardE, and that the Canada Group is in turn itself a member of the Americas Group.

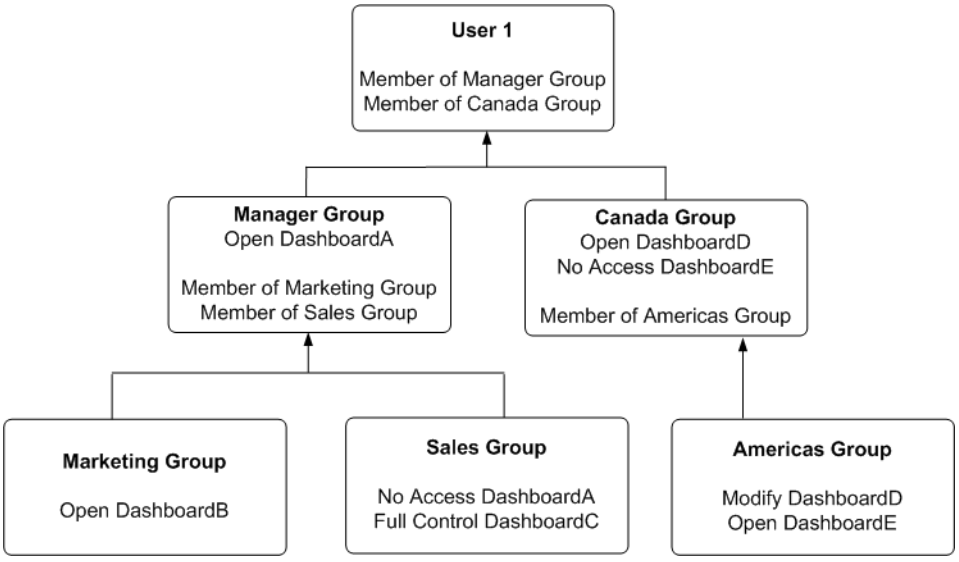
Attached beneath the Manager Group rectangle are two more rectangles - one on the left that represents Marketing Group and one on the right that represents Sales Group:

- The Marketing Group rectangle specifies that Marketing Group has open access to DashboardB.
- The Sales Group rectangle specifies that Sales Group has full control of DashboardC and no access to DashboardA.

And finally, attached beneath the Canada Group rectangle is a rectangle that represents the Americas Group:

- The Americas Group rectangle specifies that Americas Group has Modify access to DashboardD and Open access to DashboardE.

Figure D–4 Example of Determining a User's Permissions Using Deprecated Catalog Groups



In this example:

- User1 is explicitly in the Manager Group, and thus is implicitly in the Marketing Group and Sales Group too.
- User1 also is explicitly in the Canada Group, and thus is also implicitly in the Americas Group too.

- So User1's initial list of Catalog groups is Manager Group and Canada Group. If required, User1's parent list of Catalog groups is Marketing Group, Sales Group and Americas Group. The grandparent list of Catalog groups is empty, as the Catalog group hierarchy is only two levels deep.
- The effective permissions from the Manager Group are open access to DashboardA, open access to DashboardB, and full control of DashboardC. Note explicit Manager Group's record for DashboardA takes precedence over implicit Sale Group's record, as the more immediate ancestor Catalog group always takes precedence over more distant ancestor Catalog group.
- The effective permissions from the Canada group are open access to DashboardD, and no access to DashboardE. Note explicit Canada Group's records for both DashboardD and DashboardE takes precedence over implicit Americas Group's records, as the more immediate ancestor Catalog group always takes precedence over more distant ancestor Catalog group.

The total privileges granted to User1 are as follows:

- Open access to DashboardA, because the Manager group takes precedence over Sales group.
- Open access to DashboardB.
- Full control of DashboardC.
- Open access to DashboardD, because the Canada group takes precedence over Americas group.
- No access to DashboardE, because the Canada group takes precedence over Americas group.

D.4 Providing Shared Dashboards for Users

This section contains the following topics on providing shared dashboards for users:

- Section D.4.1, "Understanding the Catalog Structure for Shared Dashboards"
- Section D.4.2, "Creating Shared Dashboards"
- Section D.4.3, "Testing the Dashboards"
- Section D.4.4, "Releasing Dashboards to the User Community"

D.4.1 Understanding the Catalog Structure for Shared Dashboards

The Oracle BI Presentation Catalog has two main folders:

- **My Folders** — Contains the personal storage for individual users. Includes a Subject Area Contents folder where you save objects such as calculated items and groups.
- **Shared Folders** — Contains objects and folders that are shared across users. Dashboards that are shared across users are saved in a Dashboards subfolder under a common subfolder under the /Shared Folders folder

---

Note: If a user is given permission to an analysis in the Oracle BI Presentation Catalog that references a subject area to which the user does not have permission, then the BI Server still prevents the user from executing the analysis.

D.4.2 Creating Shared Dashboards

After setting up the Oracle BI Presentation Catalog structure and setting permissions, you can create shared dashboards and content for use by others.

One advantage to creating shared dashboards is that pages that you create in the shared dashboard are available for reuse. Users can create their own dashboards using the pages from your shared dashboards and any new pages that they create. You can add pages and content as described in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*.

If you plan to allow multiple users to modify a shared default dashboard, then consider putting these users into an application role. For example, suppose that you create an application role called Sales and create a default dashboard called SalesHome. Of the 40 users that have been assigned the Sales application role, suppose that there are three who must have the ability to create and modify content for the SalesHome dashboard. Create a SalesAdmin application role, with the same permissions as the primary Sales application role. Add the three users who are allowed to make changes to the SalesHome dashboard and content to this new SalesAdmin application role, and give this role the appropriate permissions in the Oracle BI Presentation Catalog. This allows those three users to create and modify content for the SalesHome dashboard. If a user no longer requires the ability to modify dashboard content, then you can change the user's role assignment to Sales. If an existing Sales role user must have the ability to create dashboard content, then the user's role assignment can be changed to SalesAdmin.

For more information about creating shared dashboards, see 'Managing Dashboards' in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

D.4.3 Testing the Dashboards

Before releasing dashboards and content to the user community, perform some tests.

To test the dashboard:

1. Verify that users with appropriate permissions can correctly access it and view the intended content.
2. Verify that users without appropriate permissions cannot access the dashboard.
3. Verify that styles and skins are displayed as expected, and that other visual elements are as expected.
4. Correct any problems you find and test again, repeating this process until you are satisfied with the results.

D.4.4 Releasing Dashboards to the User Community

After testing is complete, notify the user community that the dashboard is available, ensuring that you provide the relevant network address.

D.5 Controlling Access to Saved Customization Options in Dashboards

This section provides an overview of saved customizations and information about administering saved customizations. It contains the following topics:

- Section D.5.1, "Overview of Saved Customizations in Dashboards"
- Section D.5.2, "Administering Saved Customizations"

D.5.1 Overview of Saved Customizations in Dashboards

Saved customizations allow users to save and view later dashboard pages in their current state with their most frequently used or favorite choices for items such as filters, prompts, column sorts, drills in analyses, and section expansion and collapse. By saving customizations, users need not make these choices manually each time that they access the dashboard page.

Users and groups with the appropriate permissions and dashboard access rights can perform the following activities:

- Save various combinations of choices as saved customizations, for their personal use or use by others.
- Specify a saved customization as the default customization for a dashboard page, for their personal use or use by others.
- Switch between their saved customizations.

You can restrict this behavior in the following ways:

- Users can view only the saved customizations that are assigned to them.
- Users can save customizations for personal use only.
- Users can save customizations for personal use and for use by others.

For information about end users and saved customizations with dashboards, see *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition*.

D.5.2 Administering Saved Customizations

This section describes the privileges and permissions that are required to administer saved customizations. It also describes the relevant portions of the Oracle BI Presentation Catalog that relate to storing and administering saved customizations.

D.5.2.1 Privileges for Saved Customizations

In Oracle BI Presentation Services Administration, the following privileges in the Dashboards area, along with permission settings for key dashboard elements, control whether users or groups can save or assign customizations:

- Save Customizations
- Assign Default Customizations

You can set neither privilege, one privilege, or both privileges for a user or group, depending on the level of access desired. For example, a user who has neither privilege can view only the saved customization that is assigned as his or her default customization.

D.5.2.2 Permissions for Saved Customizations

This section describes the permissions that are required for users to administer saved customizations of dashboard pages, and the relevant portions of the Oracle BI Presentation Catalog structure for setting permissions on shared and personal saved customizations.

D.5.2.2.1 Assigning Permissions to Dashboards

You set permissions for dashboards and pages, such as Full Control or No Access, in the Permission dialog in Oracle BI EE. You assign these permissions in the same manner as for other objects in the catalog.

D.5.2.2.2 Assigning Permissions for Customizations on a Dashboard Page

You set permissions for working with saved customizations on a particular dashboard page in the Dashboard Properties dialog, which is available in the Dashboard Builder. After selecting a page in the list in the dialog, click one of the following buttons:

- **Specify Who Can Save Shared Customizations** displays the Permission dialog in which you specify who can save shared customizations for that dashboard page.
- **Specify Who Can Assign Default Customizations** displays the Permission dialog in which you specify who can assign default customizations for that dashboard page.

Catalog objects and permissions scenarios are described in the following sections.

D.5.2.2.3 Catalog Folder Structure for Saved Customizations

In addition to the privileges that you set in Oracle BI Presentation Services Administration, the level of control that users and groups have over saved customizations depends on their access rights to key elements. For example, users and groups that can create and edit underlying dashboards, save dashboard view preferences as customizations, and assign customizations to other users as default customizations require Full Control permission to the key elements in shared storage, while users and groups that can view only their assigned default saved customizations need only View access to the key elements in shared storage.

Key elements in the catalog include the following folders:

- Shared Storage Folders.

  Shared storage folders for dashboards are typically located within the Dashboards sub-folder of a parent shared folder. Dashboards are identified by their assigned names. You can save a dashboard anywhere in the Oracle BI Presentation Catalog. If you save a dashboard within a subfolder called "Dashboards", then that dashboard's name is displayed in the list of dashboards that is displayed from the Dashboards link in the global header.

  Permission settings control access to a specific dashboard for editing. Typically, if permissions are inherited down to the _selections and Dashboards sub-folders, then users who can edit dashboards can also save customizations and set defaults. Access to a specific dashboard folder controls whether a user or group can edit the dashboard.

  The _selections folder contains a page identifier folder for each dashboard page. Shared saved customizations are located within this folder. Access to the page identifier folder controls whether a user or group can display, save, or edit customizations for that page.

  The _defaults folder within a _selections folder contains assigned default customizations. Each group that has an assigned default is displayed here. Access to this folder controls whether a user or group can assign defaults.

- Personal Storage Folders.

  Within a user's personal folder, the _selections folder contains an individual user's saved customizations. Like the shared _selections folder, a personal _selections folder contains a page identifier folder for each dashboard page. The page identifier folder contains personal saved customizations and a _defaultlink file that specifies a user's preference for the personal defaulted customization.

A personal saved customization default overrides an assigned shared customization default.

Note: If a dashboard page with saved customizations is deleted, then the saved customizations are also deleted from the catalog. If the underlying dashboard structure changes such that a saved customization is no longer valid when a user accesses it, then the default content is displayed on the dashboard.

D.5.3 Permission and Privilege Settings for Creating Saved Customizations

Table D–5 describes typical user roles and specific permission settings that can be granted to users for creating saved customizations. The folder names listed in the Permission and Privilege Settings column are described in the preceding section.

Table D–5 User Roles and Permission Settings for Saved Customizations

User Role	Permission and Privilege Settings
Power users such as IT users who must perform the following tasks: ■ Create and edit underlying dashboards. ■ Save dashboard view preferences as customizations. ■ Assign customizations to other users as default customizations.	In the Shared section of the catalog, requires Full Control permission to the following folders: ■ dashboard_name ■ _selection ■ _defaults Typically, no additional privileges must be assigned.
Technical users such as managers who must perform the following tasks: ■ Save customizations as customizations for personal use. ■ Save customizations for use by others. Users cannot create or edit underlying dashboards, or assign view customizations to others as default customizations.	In the Shared section of the catalog, requires View permission to the following folders: ■ dashboard_name In the Shared section of the catalog, requires Modify permission to the following folders: ■ _selections ■ _defaults Typically, no additional privileges must be assigned.
Everyday users who must save customizations for personal use only.	In Oracle BI Presentation Services Administration, requires the following privilege to be set: ■ Save Customizations In the dashboard page, requires that the following option is set: ■ Allow Saving Personal Customizations In the catalog, no additional permission settings are typically required.

Table D–5 (Cont.) User Roles and Permission Settings for Saved Customizations

User Role	Permission and Privilege Settings
Casual users who must view only their assigned default customization.	In the Shared section of the catalog, the user needs View permission to the following folders: ■ dashboard_name ■ _selections ■ _defaults In the catalog, no additional permission settings are typically required.

D.5.4 Example Usage Scenario for Saved Customization Administration

Depending on the privileges set and the permissions granted, you can achieve various combinations of user and group rights for creating, assigning, and using saved customizations.

For example, suppose a group of power users cannot change dashboards in a production environment, but they are allowed to create saved customizations and assign them to other users as default customizations. The following permission settings for the group are required:

- Open access to the dashboard, using the Catalog page.
- Modify access to the _selections and _defaults subfolders within the dashboard folder in the Oracle BI Presentation Catalog, which you assign using the Dashboard Properties dialog in the Dashboard Builder. After selecting a page in the list in the dialog, click **Specify Who Can Save Shared Customizations** and **Specify Who Can Assign Default Customizations**.

D.6 Enabling Users to Act for Others

This section contains the following topics on enabling users to act for others:

- Section D.6.1, "Why Enable Users to Act for Others?"
- Section D.6.2, "What Are the Proxy Levels?"
- Section D.6.3, "Process of Enabling Users to Act for Others"

D.6.1 Why Enable Users to Act for Others?

You can enable one user to act for another user in Oracle BI Presentation Services. When a user (called the proxy user) acts as another (called the target user), the proxy user can access the objects in the catalog for which the target user has permission.

Enabling a user to act for another is useful, for example, when a manager wants to delegate some of his work to one of his direct reports or when IT support staff wants to troubleshoot problems with another user's objects.

See *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Enterprise Edition* for information on how users enable others to act for them.

D.6.2 What Are the Proxy Levels?

When you enable a user to be a proxy user, you also assign an authority level (called the proxy level). The proxy level determines the privileges and permissions granted to

the proxy user when accessing the catalog objects of the target user. The following list describes the proxy levels:

- **Restricted** — Permissions are read-only to the objects to which the target user has access. Privileges are determined by the proxy user's account (not the target user's account).

  For example, suppose a proxy user *has not* been assigned the Access to Answers privilege, and the target user *has*. When the proxy user is acting as the target user, the target user *cannot* access Answers.

- **Full** — Permissions and privileges are inherited from the target user's account.

  For example, suppose a proxy user *has not* been assigned the Access to Answers privilege, and the target user *has*. When the proxy user is acting as the target user, the target user *can* access Answers.

When you have enabled a user to act as a proxy user, that user can display the **Act As** option in the global header of Presentation Services to select the target user to act as, provided the Act As Proxy privilege has been set.

> **Tip:** Before a proxy user can act as a target user, the target user must have signed into Presentation Services at least once and accessed a dashboard.

> **Note:** If you are a user who can be impersonated by a proxy user, you can see the users with the permission to proxy (Act As) you. To see these users, log in to Oracle Business Intelligence, go to the My Account dialog box and display the extra tab called Delegate Users. This tab displays the users who can connect as you, and the permission they have when they connect as you (Restricted or Full).

D.6.3 Process of Enabling Users to Act for Others

To enable users to act for others, perform the following tasks:

- Section D.6.3.1, "Defining the Association Between Proxy Users and Target Users"
- Section D.6.3.2, "Creating Session Variables for Proxy Functionality"
- Section D.6.3.3, "Modifying the Configuration File Settings for Proxy Functionality"
- Section D.6.3.4, "Creating a Custom Message Template for Proxy Functionality"
- Section D.6.3.5, "Assigning the Proxy Privilege"

D.6.3.1 Defining the Association Between Proxy Users and Target Users

You define the association between proxy users and target users in the database by identifying, for each proxy user/target user association, the following:

- ID of the proxy user
- ID of the target user
- Proxy level (either full or restricted)

For example, you might create a table called Proxies in the database that looks like this:

proxyId	targetId	proxyLevel
Ronald	Eduardo	full
Timothy	Tracy	restricted
Pavel	Natalie	full
William	Sonal	restricted
Maria	Imran	restricted

After you define the association between proxy users and target users, you must import the schema to the physical layer of the BI Server. For information on importing a schema, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

D.6.3.2 Creating Session Variables for Proxy Functionality

To authenticate proxy users, you must create the following two session variables along with their associated initialization blocks. For both variables, you must modify the sample SQL statement according to the schema of the database.

- **PROXY** — Use this variable to store the name of the proxy user.

  Use the initialization block named ProxyBlock and include code such as the following:

  ```
  select targetId
  from Proxies
  where UPPER(targetid) = UPPER('VALUEOF(NQ_SESSION.RUNAS)')
  and UPPER(proxyid) = UPPER('VALUEOF(NQ_SESSION.RUNASORIGUSER)')
  ```

- **PROXYLEVEL** — Use this optional variable to store the proxy level, either Restricted or Full. If you do not create the PROXYLEVEL variable, then the Restricted level is assumed.

  Use the initialization block named ProxyLevel and include code such as the following:

  ```
  select proxyLevel
  from Proxies
  where UPPER(targetid) = UPPER('VALUEOF(NQ_SESSION.RUNAS)')
  and UPPER(proxyid) = UPPER('VALUEOF(NQ_SESSION.RUNASORIGUSER)')
  ```

For more information on creating session variables, see *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

D.6.3.3 Modifying the Configuration File Settings for Proxy Functionality

Use various elements in the instanceconfig.xml file to configure the proxy functionality.

Before you begin this procedure, ensure that you are familiar with the information in 'Using a Text Editor to Update Oracle Business Intelligence Configuration Settings' in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

To manually configure for proxy functionality:

1. Open the instanceconfig.xml file for editing, as described in 'Where are Configuration Files Located' in *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

2. Locate the section in which you must add the elements that are described in the following list:

   - LogonParam: Serves as the parent element for the TemplateMessageName and MaxValues elements.
   - TemplateMessageName: Specifies the name of the custom message template in the Custom Messages folder that contains the SQL statement to perform tasks related to displaying proxy and target users. The default name is LogonParamSQLTemplate.

     The name that you specify in the TemplateMessageName element must match the name that you specify in the WebMessage element in the custom message file. For more information, see Section D.6.3.4, "Creating a Custom Message Template for Proxy Functionality."
   - MaxValues: Specifies the maximum number of target users to be listed in the **User** box in the Act As dialog box. If the number of target users for a proxy user exceeds this value, then an edit box, where the proxy user can enter the ID of a target user, is shown rather than a list of target users. The default is 200.

3. Include the elements and their ancestor elements as appropriate, as shown in the following example:

```
<LogonParam>
     <TemplateMessageName>LogonParamSQLTemplate</TemplateMessageName>
     <MaxValues>100</MaxValues>
</LogonParam>
```

4. Save your changes and close the file.
5. Restart Oracle Business Intelligence.

D.6.3.4 Creating a Custom Message Template for Proxy Functionality

You must create a custom message template for the proxy functionality that contains the SQL statement to perform the following tasks:

- Obtain the list of target users that a proxy user can act as. This list is displayed in the User box in the Act As dialog box.
- Verify whether the proxy user can act as the target user.
- Obtain the list of proxy users that can act as the target user. This list is displayed on the target user's My Account screen.

In the custom message template, you place the SQL statement to retrieve this information in the following XML elements:

Element	Description
getValues	Specifies the SQL statement to return the list of target users and corresponding proxy levels. The SQL statement must return either one or two columns, where the: - First column returns the IDs of the target users - (Optional) Second column returns the names of the target users

Element	Description
verifyValue	Specifies the SQL statement to verify if the current user can act as the specified target user. The SQL statement must return at least one row if the target user is valid or an empty table if the target user is invalid.
getDelegateUsers	Specifies the SQL statement to obtain the list of proxy users that can act as the current user and their corresponding proxy levels. The SQL statement must return either one or two columns, where the: ■ First column returns the names of the proxy users ■ (Optional) Second column returns the corresponding proxy levels

You can create the custom message template in one of the following files:

- The original custom message file in the directory
- A separate XML file in the directory

To create the custom message template:

1. To create the custom message template in the original custom message file:
   a. Make a backup of the original custom message file in a separate directory.
   b. Make a development copy in a different directory and open it in a text or XML editor.
2. To create the custom message template in a separate XML file, create and open the file in the *BI_DOMAIN*/bidata/components/OBIPS/customMessages directory.

   You must also configure a folder (for example, customMessages) as an application in WebLogic Server, to make Oracle BI Presentation Services aware of it. For more information, see, "Install applications and modules" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* in:

   http://docs.oracle.com/cd/E23943_01/apirefs.1111/e13952/taskhelp/deployment/InstallApplicationsAndModules.html
3. Start the custom message template by adding the WebMessage element's begin and end tags. For example:

```
<WebMessage name="LogonParamSQLTemplate">
</WebMessage>
```

> **Note:** The name that you specify in the WebMessage element must match the name that you specify in the TemplateMessageName element in the instanceconfig.xml file. For information, see Section D.6.3.3, "Modifying the Configuration File Settings for Proxy Functionality."

4. After the </WebMessage> tag:
   a. Add the <XML> and </XML> tags
   b. Between the <XML> and </XML> tags, add the <logonParam name="RUNAS"> and </logonParam> tags.

c. Between the <logonParam name="RUNAS"> and </logonParam> tags, add each of the following tags along with its corresponding SQL statements:

   * <getValues> and </getValues>
   * <verifyValue> and </verifyValue>
   * <getDelegateUsers> and </getDelegateUsers>

The following entry is an example:

```
<?xml version="1.0" encoding="utf-8" ?>
<WebMessageTables xmlns:sawm="com.example.analytics.web.messageSystem">
 <WebMessageTable system="SecurityTemplates" table="Messages">
  <WebMessage name="LogonParamSQLTemplate">
   <XML>
    <logonParam name="RUNAS">
     <getValues>EXECUTE PHYSICAL CONNECTION POOL "01 - Sample App Data
(ORCL)"."Sample Relational Connection" select targetId from SAMP_USERS_PROXIES
where proxyId='@{USERID}'</getValues>
     <verifyValue>EXECUTE PHYSICAL CONNECTION POOL "01 - Sample App Data
(ORCL)"."Sample Relational Connection" select targetId from SAMP_USERS_PROXIES
where proxyId='@{USERID}' and targetId='@{VALUE}'</verifyValue>
     <getDelegateUsers>EXECUTE PHYSICAL CONNECTION POOL "01 - Sample App Data
(ORCL)"."Sample Relational Connection" select proxyId, proxyLevel from SAMP_
USERS_PROXIES where targetId='@{USERID}'</getDelegateUsers>
    </logonParam>
   </XML>
  </WebMessage>
 </WebMessageTable>
</WebMessageTables>
```

Note that you must modify the example SQL statement according to the schema of the database. In the example, the database and connection pool are both named Proxy, the proxyId is PROXYER, and the targetId is TARGET.

5. If you created the custom message template in the development copy of the original file, then replace the original file in the customMessages directory with the newly edited file.
6. Test the new file.
7. (Optional) If you created the custom message template in the development copy of the original file, then delete the backup and development copies.
8. Load the custom message template by either restarting the server or by clicking the **Reload Files and Metadata** link on the Presentation Services Administration screen. For information on the Administration page, see Section D.2.1, "Understanding the Administration Pages."

D.6.3.5 Assigning the Proxy Privilege

For each user whom you want to enable as a proxy user or for each application role or Catalog group whose members you want to enable as proxy users, you must grant the Act As Proxy privilege. For information on how to assign privileges, see Section D.2.3.2, "Setting Presentation Services Privileges for Application Roles."