Oracle® Fusion Middleware

Security Guide for Oracle Business Intelligence Enterprise Edition

12*c* (12.2.1.3.0)
E80929-03
October 2018

Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition, 12*c* (12.2.1.3.0)

E80929-03

Copyright © 2015, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Helen Gilmore

Contributing Authors: Nick Fry, Kate Price

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

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

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

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

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

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

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

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

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

Contents

Preface

Audience x

Documentation Accessibility x

Related Documents and Other Resources x

System Requirements and Certification xi

Conventions xi

New Features in Oracle Business Intelligence Security

New Features for 12c (12.2.1.3.0) xii

New Features for 12c (12.2.1.2.0) xii

New Features for 12c (12.2.1.1.0) xiii

New Features for 12c (12.2.1.0) xiii

1 Introduction to Security in Oracle Business Intelligence

High-Level Roadmap for Setting Up Security in Oracle Business Intelligence 1-1

Overview of Security in Oracle Business Intelligence 1-2

About Authentication 1-2

About Authorization 1-3

- About Application Roles 1-3
- About the Security Policy 1-4

About Users, Groups, and Application Roles 1-5

Using Tools to Configure Security in Oracle Business Intelligence 1-5

- Using Oracle WebLogic Server Administration Console 1-6
- Using Oracle Fusion Middleware Control 1-7
- Using Oracle BI Administration Tool 1-8
- Using Presentation Services Administration Page 1-8

Process for Setting Up Security in Oracle Business Intelligence 1-8

Terminology 1-10

2 Managing Security Using a Default Security Configuration

Working with Users, Groups, and Application Roles 2-1

Example of Users, Groups, and Application Roles Security Setup 2-3

Managing Users and Groups in the Embedded WebLogic LDAP Server 2-4

- Assigning a User to a New Group, and a New Application Role 2-4
- Creating a New User in the Embedded WebLogic LDAP Server 2-5
- Creating a New Group in the Embedded WebLogic LDAP Server 2-5
- Assigning a User to a Group in the Embedded WebLogic LDAP Server 2-6
- Deleting a User 2-6
- Changing a User Password in the Embedded WebLogic LDAP Server 2-7

Managing Application Roles and Application Policies Using Fusion Middleware Control 2-7

- Displaying Application Policies and Application Roles Using Fusion Middleware Control 2-8
- Creating and Deleting Application Roles Using Fusion Middleware Control 2-9
  - Creating Application Roles 2-9
  - Creating Application Roles from Existing Roles 2-10
  - Assigning a Group to an Application Role 2-11
  - Deleting Application Roles 2-11
- Creating Application Policies Using Fusion Middleware Control 2-12
- Modifying Application Roles Using Fusion Middleware Control 2-12
  - Adding an Application Role to an Application Policy 2-13
  - Adding or Removing Members from an Application Role 2-13
  - Renaming an Application Role 2-14

Managing Metadata Repository Privileges Using the Oracle BI Administration Tool 2-14

- Setting Metadata Repository Privileges for an Application Role 2-15
- Managing Application Roles in the Metadata Repository - Advanced Security Configuration Topic 2-15

Managing Presentation Services Privileges Using Application Roles 2-16

- Setting Presentation Services Privileges for Application Roles 2-17
- Encrypting Credentials in BI Presentation Services - Advanced Security Configuration Topic 2-18

Managing Data Source Access Permissions Using BI Publisher 2-18

Enabling High Availability of the Default Embedded Oracle WebLogic Server LDAP Identity Store 2-19

Using runcat to Manage Security Tasks in the Oracle BI Presentation Catalog 2-19

3 Using Alternative Authentication Providers

Introduction 3-1

High-Level Steps for Configuring an Alternative Authentication Provider 3-2

Setting Up Groups and Users in the Alternative Authentication Provider 3-2

Configuring Oracle Business Intelligence to Use Alternative Authentication Providers 3-3
Reconfiguring Oracle Internet Directory as an Authentication Provider 3-4
Oracle Internet Directory Authenticator Provider Specific Reference 3-5
Reconfiguring Microsoft Active Directory as the Authentication Provider 3-6
Configuring User and Group Name Attributes in the Identity Store 3-8
Configuring User Name Attributes 3-9
Configuring Group Name Attributes 3-10
Configuring LDAP as the Authentication Provider and Storing Groups in a Database 3-10
Prerequisites 3-11
Creating a Sample Schema for Groups and Group Members 3-11
Configuring a Data Source and the BISQLGroupProvider Using Oracle WebLogic Server Administration Console 3-12
Configuring the Virtualized Identity Store 3-16
Testing the Configuration by Adding a Database Group to an Application Role 3-20
Correcting Errors in the Adaptors 3-21
Configuring a Database as the Authentication Provider 3-21
Introduction and Prerequisites 3-21
Creating a Sample Schema for Users and Groups 3-22
Configuring a Data Source and SQL Authenticator Using the Oracle WebLogic Server Administration Console 3-22
Configuring the Virtualized Identity Store 3-27
Troubleshooting the SQL Authenticator 3-31
Correcting Database Adapter Errors by Deleting and Recreating the Adapter 3-33
Configuring Identity Store Virtualization Using Fusion Middleware Control 3-34
Configuring Multiple Authentication Providers 3-35
Setting the JAAS Control Flag Option 3-35
Configuring a Single LDAP Authentication Provider as the Authenticator 3-36
Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator 3-36
Troubleshooting 3-41
Resetting the BI System User Credential 3-41

4 Enabling SSO Authentication

SSO Configuration Tasks for Oracle Business Intelligence 4-1
Understanding SSO Authentication and Oracle Business Intelligence 4-2
SSO Implementation Considerations 4-4
Configuring SSO in an Oracle Access Manager Environment 4-5
Configuring an OID Authenticator for Oracle WebLogic Server 4-5

Authentication Provider Source Reference 4-7
Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server 4-7
Configuring Custom SSO Environments 4-8
Configuring Single Sign-On with Smart View 4-8
Enabling Oracle Business Intelligence to Use SSO Authentication 4-10
Enabling and Disabling SSO Authentication Using WLST Commands 4-10
Enabling SSO Authentication Using Fusion Middleware Control 4-11
Enabling the Online Catalog Manager to Connect 4-12

5 Configuring SSL in Oracle Business Intelligence

What is SSL? 5-1
Enabling End-to-End SSL 5-3
Configuring a Standard Non-SSL Oracle BI EE System 5-3
Configuring WebLogic SSL 5-3
Starting Only the Administration Server 5-4
Configuring HTTPS Ports 5-4
Configuring Internal WebLogic Server LDAP to Use LDAPs 5-5
Configuring Internal WebLogic Server LDAP Trust Store 5-6
Disabling HTTP 5-8
Restarting 5-8
Configuring OWSM to Use t3s 5-8
Restarting System 5-9
Enabling Oracle BI EE Internal SSL 5-9
Disabling Internal SSL 5-10
Exporting Trust and Identity for Clients 5-11
Configuring SSL for Clients 5-12
Exporting Client Certificates 5-12
Using SASchInvoke when BI Scheduler is SSL-Enabled 5-12
Configuring Oracle BI Job Manager 5-13
Connecting the Online Catalog Manager to Oracle BI Presentation Services 5-14
Configuring the Oracle BI Administration Tool to Communicate Over SSL 5-15
Configuring an ODBC DSN for Remote Client Access 5-15
Configuring Oracle BI Publisher to Communicate Over SSL 5-15
Checking Certificate Expiry 5-15
Replacing the Certificates 5-16
Update Certificates After Changing Listener Addresses 5-16
Adding New Servers 5-17
Enabling SSL in a Configuration Template Configured System 5-18
Enabling SSL Without Internal Business Intelligence SSL 5-18
Manually Configuring SSL Cipher Suite 5-19

Configuring SSL Connections to External Systems 5-20
Configuring SSL for the SMTP Server Using Fusion Middleware Control 5-20
Configuring SSL when Using Multiple Authenticators 5-20
WebLogic Artifacts Reserved for Oracle BI EE Internal SSL Use 5-21

A Legacy Security Administration Options

Lightweight SSO and Legacy Authentication Options A-1
Legacy Authentication Options A-1
Setting Up LDAP Authentication Using Initialization Blocks A-2
Setting Up an LDAP Server A-3
Defining a USER Session Variable for LDAP Authentication A-4
Setting the Logging Level A-5
Setting Up External Table Authentication A-6
About Oracle BI Delivers and External Initialization Block Authentication A-7
Order of Authentication A-8
Authenticating by Using a Custom Authenticator Plug-In A-8
Managing Session Variables A-9
Managing Server Sessions A-9
Using the Session Manager A-9
Alternative Authorization Options A-11
Changes Affecting Security in Presentation Services A-11
Setting Up Authorization Using Initialization Blocks A-12

B Understanding the Default Security Configuration

About Securing Oracle Business Intelligence B-1
About the Security Framework B-2
Oracle Platform Security Services B-2
Oracle WebLogic Server B-2
Key Security Elements B-3
Security Configuration Using the Sample Application B-4
Default Authentication Provider B-5
Policy Store Provider B-6
Granting Permissions To Users Using Groups and Application Roles B-7
Permission Inheritance and Role Hierarchy B-8
Common Security Tasks After Installation B-9

C Troubleshooting Security in Oracle Business Intelligence

Resolving User Login Authentication Failure Issues C-1
Authentication Concepts C-1

Authentication Defaults on Install C-2
Using Oracle WebLogic Server Administration Console and Fusion Middleware Control to Configure Oracle Business Intelligence C-2
WebLogic Domain and Log Locations C-2
WebLogic Server Administrator User Account C-3
Oracle Business Intelligence Login Overview C-3
Identifying Causes of User Login Authentication Failure C-4
Resolving User Login Authentication Failures C-6
Single User Cannot Log in to Oracle Business Intelligence C-7
Users Cannot Log in to Oracle Business Intelligence Due to Misconfigured Authenticators C-7
Users Cannot Log in to Oracle Business Intelligence When Oracle Web Services Manager is not Working C-9
Users Cannot Log in to Oracle Business Intelligence - Is the External Identity Store Configured Correctly? C-12
Users Can Log in With Any or No Password C-12
Have Removed Default Authenticator and Cannot Start WebLogic Server C-12
Resolving Inconsistencies with the Identity Store C-13
User Is Deleted from the Identity Store C-13
User Is Renamed in the Identity Store C-14
Group Associated with User Name Does Not Exist in the Identity Store C-14
Resolving Inconsistencies with the Policy Store C-15
Application Role Was Deleted from the Policy Store C-16
Application Role Is Renamed in the Policy Store C-16
Resolving SSL Communication Problems C-16
Resolving Custom SSO Environment Issues C-17
Resolving RSS Feed Authentication When Using SSO C-17

D Managing Security for Dashboards and Analyses

Managing Security for Users of Oracle BI Presentation Services D-1
Security Settings in Oracle BI Presentation Services D-1
What Are the Security Goals in Oracle BI Presentation Services? D-2
How Are Permissions and Privileges Assigned to Users? D-3
Using Oracle BI Presentation Services Administration Pages D-3
Understanding the Administration Pages D-3
Managing Presentation Services Privileges D-4
What Are Presentation Services Privileges? D-4
Default Presentation Services Privilege Assignments D-4
Managing Sessions in Presentation Services D-44
Determining a User's Privileges and Permissions in Oracle BI Presentation Services D-44
Rules for Determining a User's Privileges or Permissions D-45

Task 1 - Check for an explicit record for this user D-46

Task 2 - Check for records for this user's Catalog groups D-46

Task 3 - Check records for this user's application roles D-47

Task 4 - Fall back default behavior D-48

Task 5 - No matching records at all D-48

Example of Determining a User's Privileges with Application Roles D-48

Example of Determining a User's Permissions with Application Roles D-50

Example of Determining a User's Privileges with Removed Catalog Groups D-51

Example of Determining a User's Permissions with Removed Catalog Groups D-53

Providing Shared Dashboards for Users D-54

Understanding the Catalog Structure for Shared Dashboards D-54

Creating Shared Dashboards D-55

Testing the Dashboards D-55

Releasing Dashboards to the User Community D-56

Controlling Access to Saved Customization Options in Dashboards D-56

Overview of Saved Customizations in Dashboards D-56

Administering Saved Customizations D-57

Permission and Privilege Settings for Creating Saved Customizations D-57

Example Usage Scenario for Saved Customization Administration D-58

Enabling Users to Act for Others D-58

Why Enable Users to Act for Others? D-58

What Are the Proxy Levels? D-58

Process of Enabling Users to Act for Others D-59

Defining the Association Between Proxy Users and Target Users D-59

Creating Session Variables for Proxy Functionality D-60

Modifying the Configuration File Settings for Proxy Functionality D-60

Creating a Custom Message Template for Proxy Functionality D-61

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:

- *Securing Applications with Oracle Platform Security Services*

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 section lists the changes to security features in Oracle Business Intelligence release 12*c*.

If you are upgrading to Oracle BI EE from a previous release, read the following information carefully. There are significant differences in features, tools, and procedures. See *Upgrade Guide for Oracle Business Intelligence*.

This section contains the following topics:

- New Features for 12*c* (12.2.1.3.0)
- New Features for 12*c* (12.2.1.2.0)
- New Features for 12*c* (12.2.1.1.0)
- New Features for 12*c* (12.2.1.0)

New Features for 12*c* (12.2.1.3.0)

New security features in Oracle BI EE 12*c* (12.2.1.3.0) include:

- This release uses OpenSSL version 1.0.2h.
- Lightweight Single Sign-On (SSO)

Lightweight Single Sign-On (SSO)

Users can log in to Oracle Business Intelligence once and navigate between the Classic (Analytics) Home page, Visual Analyzer, and the new Home page.

Lightweight SSO is enabled by default in Oracle Business Intelligence for new installations only. If you patched Oracle BI EE to the latest release, lightweight SSO is not enabled by default.

If external SSO is configured, lightweight SSO defers to the external SSO configuration. Oracle BI EE uses the same mechanism to enable internal lightweight SSO and external SSO.

If you need to disable lightweight SSO, use the WSLT disable SSO command. See Enabling and Disabling SSO Authentication Using WLST Commands.

New Features for 12*c* (12.2.1.2.0)

This section contains information about new security features.

There are no new security features in Oracle BI EE 12*c* (12.2.1.2.0).

New Features for 12*c* (12.2.1.1.0)

New security features in Oracle BI EE 12*c* (12.2.1.1.0) include:

- See Catalog Groups are Not Supported

Catalog Groups are Not Supported

In this release Catalog groups are not supported and you must use application roles.

See the *Upgrading Oracle Business Intelligence*.

New Features for 12*c* (12.2.1.0)

New security features in Oracle BI EE 12*c* (12.2.1.0) include:

- BISystemUser and BISystem Removed
- User GUIDs Removed
- Database Security Store
- Easier SSL Configuration
- Migrating Catalog Groups to Application Roles

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 virtual and represented by the `oracle.bi.system/system.user` credential. The values are securely and randomly generated by the Configuration Assistant. Oracle BI components use this credential for internal communication, backed by Oracle BI Security. The BISystem application role is no longer available in the Policy Store, and is removed from any environment upgraded from 11*g*.

User GUIDs Removed

In this release user GUIDs are 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.

See 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.

See *Installing and Configuring 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.

See 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.

See Migrating Catalog Groups in *Upgrading Oracle Business Intelligence*.

1

Introduction to Security in Oracle Business Intelligence

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

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

This chapter contains the following sections:

- High-Level Roadmap for Setting Up Security in Oracle Business Intelligence
- Overview of Security in Oracle Business Intelligence
- About Authentication
- About Authorization
- About Users, Groups, and Application Roles
- Using Tools to Configure Security in Oracle Business Intelligence
- Process for Setting Up Security in Oracle Business Intelligence
- Terminology

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

Use this high level roadmap to understand typical sequence of actions to maintain security in Oracle Business Intelligence.

See Working with Users, Groups, and Application Roles.

1. Read the rest of this chapter to get an overview of security concepts, tools, and terminology.
2. Decide which authentication provider to use to authenticate users.
3. Set up the required users and groups.
4. Set up the required application roles.
5. Assign each group to an appropriate application role.
6. Fine-tune the permissions that users and groups have in the Oracle BI repository.

7. Fine-tune the permissions that users and groups have in the Oracle BI Presentation Catalog.
8. If required, configure Single Sign-On (SSO).
9. If required, configure Secure Sockets Layer (SSL).

See Process for Setting Up Security in Oracle Business Intelligence.

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 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. There are certain scenarios where this is not possible or where certain aspects of the legacy approach to authentication and authorization are required. Using 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 Legacy Security Administration Options. Application roles are used with alternative authentication and authorization mechanisms.

About Authentication

You manage users and groups within the authentication provider.

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.

See Managing Security Using a Default Security Configuration.

To learn about Oracle WebLogic Server domains and authentication providers, see *Administering Security for Oracle WebLogic Server*.

About Authorization

Authorization is about ensuring users can do and see what they are authorized to do and see.

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.

About Application Roles

Application roles define the security policy for users.

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.

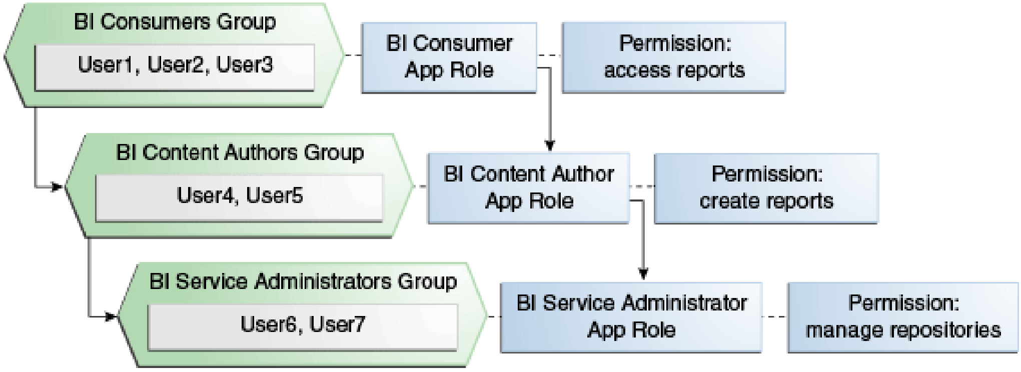
Application roles represent a functional role that a user has giving the user the privileges required to perform that role. For example, the Sales Analyst application role might grant a user access to view, edit and create reports on a company's sales pipeline.

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 moving the artifacts of a business intelligence system between development, test and production environments.

No change to the security policy is needed as a result of the environment moves, and all that is required is to assign the application roles to the users and groups available in the target environment.

The diagram below shows an example set of groups, users, application roles, permissions, and inheritance.


BI Consumers Group
User1, User2, User3
BI Consumer App Role
Permission: access reports
BI Content Authors Group
User4, User5
BI Content Author App Role
Permission: create reports
BI Service Administrators Group
User6, User7
BI Service Administrator App Role
Permission: manage repositories

The diagram 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 repositories.

About the Security Policy

The security policy is split across Oracle BI Presentation Services, the metadata repository, and the policy store.

The security policy definition is split across the following components:

- Oracle BI Presentation Services

  Oracle BI Presentation Services defines the specific catalog objects and functionality that users can access with specific application roles. Access to functionality is defined in the Managing Privileges page for Oracle BI Presentation Services privileges and access to Oracle BI Presentation Catalog objects is defined in the Permission dialog.
- Repository

  The repository defines the metadata items in the repository that user can access with assignment to specific application roles. You can define the security policy using the Oracle BI Administration Tool.
- Policy Store

> The Policy Store defines the BI Server and Oracle BI Publisher functionality that user can access with specific application roles. In the default Oracle Business Intelligence configuration, the policy store is managed using Oracle Enterprise Manager Fusion Middleware Control or by using Oracle WebLogic Scripting Tool (WLST). See *Securing Applications with Oracle Platform Security Services*.

See Using Tools to Configure Security in Oracle Business Intelligence.

About Users, Groups, and Application Roles

Oracle Business Intelligence application authors can define and name the application roles and permission grants for their applications.

Oracle Business Intelligence application authors do not have to use the default application roles and permission grants that existed in previous versions. However, you can use the default application roles and permission set grants.

When you initially configure Oracle Business Intelligence, you can create the business intelligence service instance using a supplied BI Archive (BAR) file, see *Installing and Configuring Oracle Business Intelligence*.

The set of application roles and memberships available in your service instance depend on the BAR file that you import into the service instance. The imported security policy includes the application role definitions, the application role memberships, permission set definitions, permission definitions, permission set grants, permission grants, plus Oracle BI Presentation Services and repository security policy.

If you create the initial BI service instance using the Sample App Lite BAR file or the Starter BAR file, your initial service instance imports the sample application roles and application policies for that application.

If you create the initial service instance without using the sample or starter files, the system imports an empty BAR file into your service instance that adds a minimal set of application roles and policies to your service instance. The minimal set is only the *BIServiceAdministrator* application role. You can create your own security policy specific to your BI application.

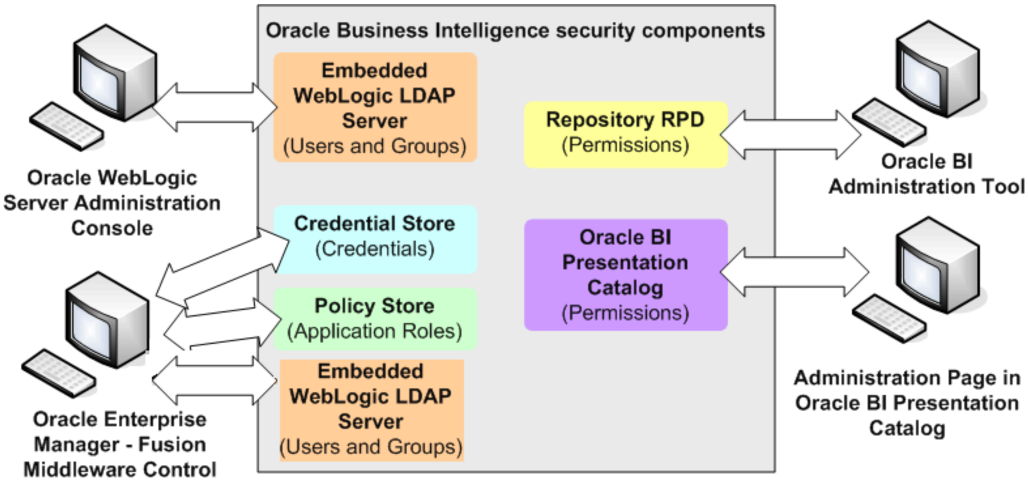
Using Tools to Configure Security in Oracle Business Intelligence

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

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

See Example of Users, Groups, and Application Roles Security Setup.

The diagram summarizes the tools used to configure security in an example installation of Oracle Business Intelligence that uses the embedded WebLogic LDAP Server.


Oracle Business Intelligence security components
Embedded WebLogic LDAP Server (Users and Groups)
Repository RPD (Permissions)
Credential Store (Credentials)
Oracle BI Presentation Catalog (Permissions)
Policy Store (Application Roles)
Embedded WebLogic LDAP Server (Users and Groups)
Oracle WebLogic Server Administration Console
Oracle Enterprise Manager - Fusion Middleware Control
Oracle BI Administration Tool
Administration Page in Oracle BI Presentation Catalog

See Managing Security Using a Default Security Configuration.

Using Oracle WebLogic Server Administration Console

You use Oracle WebLogic Server Administration Console to manage the WebLogic LDAP Server that enables you 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.

When you configure Oracle Business Intelligence, the initial security configuration uses the embedded WebLogic LDAP directory, the default authenticator, as the Identity Store. In 11*g*, the BI installation added some specific users and groups into the LDAP directory. In 12*c*, the installation does not add default BI groups into the LDAP directory. If your application expects LDAP groups such as the BIConsumers, BIContentAuthors, and BIServiceAdministrators to exist in the Identity Store, you 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 can 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 port number as used for the Administration server. The default port number is 9500. See *Oracle WebLogic Server Administration Console Online Help*.

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.

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. 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.

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.

The components consist of Oracle WebLogic Server domains, one Administration Server, one or more Managed Servers, clusters, and the Fusion Middleware Control 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.

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

See *Administering Oracle Fusion Middleware*.

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.

- See Managing Application Roles and Application Policies Using Fusion Middleware Control.
- Configure Secure Sockets Level (SSL), see:
  - Configuring HTTPS Ports
  - Configuring SSL for the SMTP Server Using Fusion Middleware Control

1. Enter the Fusion Middleware Control URL in a web browser.

   Use the format:

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

   For example:

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

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

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.

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. The best practice is to assign metadata repository permissions to application roles rather than directly to users.

1. Log in to the Administration Tool, and open a repository in **Online Mode**.
2. (Optional) Select **Manage**, then **Identity**.
3. In the Identity Manager dialog, double-click an application role.
4. In the Application Role <Name> dialog, click **Permissions**.
5. In the **Object Permissions** tab view or configure the **Read** and **Write** permissions for that application role, in relation to objects and folders in the Oracle BI Presentation Catalog.
6. In the Presentation pane, expand a folder, then right-click an object to display the Presentation Table <Table name> dialog.
7. Click **Permissions** to display the Permissions <Table name> dialog.

Using Presentation Services Administration Page

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

As a best practice, you should assign Presentation Services permissions to application roles rather than directly to users.

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.
4. Select a link for a particular privilege to display the Privilege <*Privilege name*> dialog.
5. Click the **Add users/roles** icon (+) to display the Add Application Roles and Users dialog.

   Use the Add Application Roles and Users dialog to assign application roles to this privilege.

Process for Setting Up Security in Oracle Business Intelligence

Use this process to set up security in a new Oracle Business Intelligence installation.

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

Read:

- Using Tools to Configure Security in Oracle Business Intelligence
- Working with Users, Groups, and Application Roles

> **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. See About the SampleApp.rpd Demonstration Repository in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

Oracle recommends that you complete these post installation tasks in the following order:

- Decide which authentication provider to use to authenticate users:
  - Use the default embedded WebLogic LDAP Server

    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.

    See System Requirements and Certification.
  - Use an alternative authentication provider such as Oracle Internet Directory (OID)
- When using the embedded WebLogic LDAP Server as the authentication provider, do the following:
  - Set up the users that you want to deploy, see Creating a New User in the Embedded WebLogic LDAP Server.
  - Create groups and set up the groups that you want to use, see Creating a New Group in the Embedded WebLogic LDAP Server.
  - Assign your users to appropriate groups, seeAssigning a User to a Group in the Embedded WebLogic LDAP Server.
  - Assign groups of users to application roles, see Assigning a User to a New Group, and a New Application Role.
- When using Oracle Internet Directory (OID) as the authentication provider, do the following:
  - Configure OID as the authentication provider, see High-Level Steps for Configuring an Alternative Authentication Provider.
    Use your authentication provider tools, for example, OID Console to create your users and groups as required.
- Set up the application roles that you want to deploy, see 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.

- Assign each group to an appropriate application role, see Assigning a Group to an Application Role.
- Use the Administration Tool to update the permissions that users and groups have in the Oracle BI repository, see Managing Metadata Repository Privileges Using the Oracle BI Administration.

  For example, you can enable an application role, *BISuperConsumer*, to create analyses. You use the Administration Tool to change the access from *Read* to *Read/Write* access to the specific subject area.
- To change the permissions for users and groups have in the Presentation Services, see Managing Presentation Services Privileges Using Application Roles.

  For example, you can prevent the application role, *BISuperConsumer*, from viewing scorecards, so you use Presentation Services Administration page to change the Scorecard\View Scorecard privileges for *BISuperConsumer* from *Granted* to *Denied*.
- If you want to deploy Single Sign-On, see Enabling SSO Authentication.
- To deploy secure sockets layer (SSL), see Configuring SSL in Oracle Business Intelligence. Oracle Business Intelligence is installed with SSL disabled.

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
Catalog groups are not supported in Oracle Business Intelligence Release 12.2.1.1 and higher. See *Oracle Fusion Middleware Migration Guide for Oracle Business Intelligence*.

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 Oracle BI 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, see Oracle WebLogic Server.

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, 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 such as 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

These topic explain how to deploy Oracle Business Intelligence security using the embedded WebLogic LDAP Server with the sample application.

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.

- Working with Users, Groups, and Application Roles
- Example of Users, Groups, and Application Roles Security Setup
- 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 BI Publisher
- Enabling High Availability of the Default Embedded Oracle WebLogic Server LDAP Identity Store
- Deleting a User
- Using runcat to Manage Security 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. See Exporting and Importing Information in the Embedded LDAP Server in *Administering Security for Oracle WebLogic Server*.

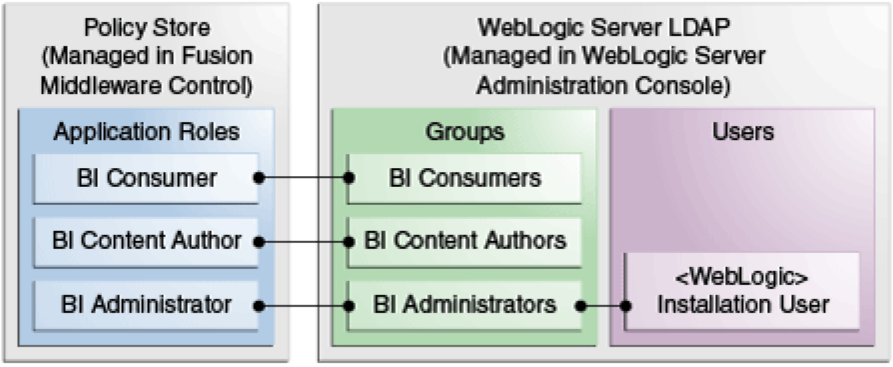
Working with Users, Groups, and Application Roles

When you configure Oracle Business Intelligence with the Sample Application that is made available with the BI installation, a number of application roles are provided for you to use in order to provision users and groups that enable you to use BI functionality and access BI folders, reports, data columns and other objects.

For example, following a new installation of Oracle Business Intelligence, 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 is assigned to the BIServiceAdministrator application role. In addition, the Sample Application provides the BIContentAuthor and BIConsumer application roles, these application roles are preconfigured to work together. For example, a user who is a member of the BIServiceAdministrator application role automatically inherits the BIContentAuthor and BIConsumer application roles and is therefore provisioned with all the privileges and permissions associated with all of these application roles. See Understanding the Default Security Configuration for this 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.

The screen below shows application roles, groups and users that are preconfigured in the sample and starter applications installation.


Policy Store (Managed in Fusion Middleware Control)
Application Roles
BI Consumer
BI Content Author
BI Administrator
WebLogic Server LDAP (Managed in WebLogic Server Administration Console)
Groups
BI Consumers
BI Content Authors
BI Administrators
Users
<WebLogic> Installation User

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 administrator specifies an owner (a user) for the service instance. The system assigns 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 automatically tags the BIAdministrator application role as the administration application role.

See *Installing and Configuring Oracle Business Intelligence* and importServiceInstance in *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 to assign Fred as a Sales dashboard author, 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, create a new application role called *BIManager* that has both BIContentAuthors privileges and Sales_Dashboard_Author privileges.

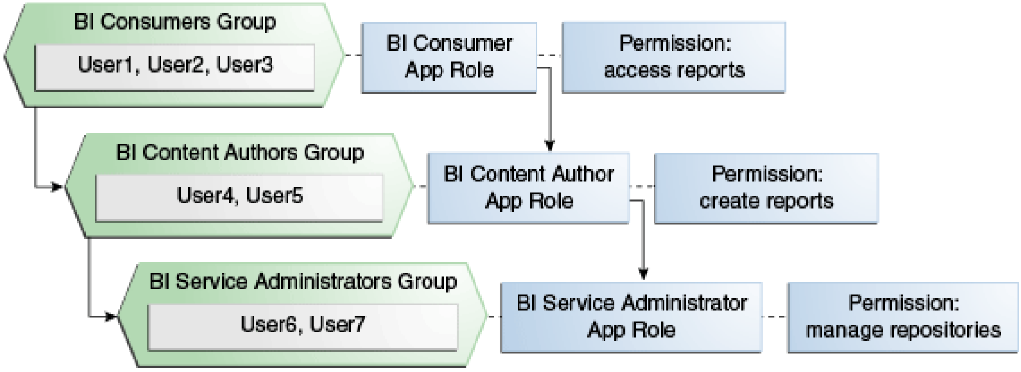
See Understanding the Default Security Configuration.

Example of Users, Groups, and Application Roles Security Setup

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.

The diagram shows the users, groups, and application roles that you would deploy to implement this example security model.


BI Consumers Group
User1, User2, User3
BI Consumer App Role
Permission: access reports
BI Content Authors Group
User4, User5
BI Content Author App Role
Permission: create reports
BI Service Administrators Group
User6, User7
BI Service Administrator App Role
Permission: manage repositories

The diagram 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.

See:

- Creating a New User in the Embedded WebLogic LDAP Server
- Creating a New Group in the Embedded WebLogic LDAP Server
- Assigning a User to a Group in the Embedded WebLogic LDAP Server

1. Create seven users named User1 to User 7.
2. Create the groups BIConsumers and BIContentAuthors and BIServiceAdministrators.
3. Assign the users to the default groups, as follows:
    a. Assign User1, User2, and User3 to the group named BIConsumers.
    b. Assign User4 and User5 to the group named BIContentAuthors.
    c. Assign User6 and User7 to the group named BIServiceAdministrators
4. Assign the groups to the sample application roles as follows:
    a. Make the BIConsumers group a member of the BIConsumer application role.
    b. Make the BIContentAuthors group a member of the BIContentAuthor application role.
    c. Make the BIServiceAdministrators group a member of the BIServiceAdministrator application role.

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:

- Assigning a User to a New Group, and a New Application Role
- Creating a New User in the Embedded WebLogic LDAP Server
- Creating a New Group in the Embedded WebLogic LDAP Server
- Assigning a User to a Group in the Embedded WebLogic LDAP Server
- Deleting a User
- Changing a User Password in the Embedded WebLogic LDAP Server

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

You can extend the security model by creating users, and assigning the users to new groups, and application roles.

For example, you can create a user named, Jim, and assign Jim to the BIMarketingGroup group that is assigned to an application role named BIMarketingRole.

The process for assigning a user to a group, and an application role is as follows:

1. Launch WebLogic Administration Console.
2. Create a new user.
3. Create a new group.

4. Assign the user to the group.
5. Create an application role and assign it to the new group.
6. Edit the Oracle BI repository and set up the privileges for the new application role.
7. Edit the Oracle BI Presentation Catalog and set up the privileges for the new user and group.

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.

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 might have designed the security policy so that all authenticated users are members of an application role that grants privileges in the BI application. See Security Configuration Using the Sample Application

DefaultAuthenticator is the name for the default authentication provider.

1. Log in to the Oracle WebLogic Server Administration Console.
2. In Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane, and then click the realm you are configuring, for example, **myrealm**.
3. Select **Users and Groups** tab, then **Users**. Click **New**.
4. In Create a New User, in **Name**, type the name of the user.
5. (Optional) In **Description**, provide additional information about the user.
6. From the **Provider** list, select the authentication provider that corresponds to the identity store where the user information is contained.
7. In **Password**, type a password for the user that is at least 8 characters long.
8. In **Confirm Password**, retype the user password.
9. Click **OK**.

Creating a New Group in the Embedded WebLogic LDAP Server

You can create a separate group for each functional type of business user in your Oracle Business Intelligence environment.

A typical deployment might require three groups: *BIConsumers*, *BIContentAuthors*, and *BIServiceAdministrators*. You could create groups with those names and configure the group to use with Oracle Business Intelligence, or you might create your own custom groups.

See Example of Users, Groups, and Application Roles Security Setup.

DefaultAuthenticator is the default authentication provider.

1. Launch 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. Click the **Users and Groups** tab, and then click **Groups**.
4. Click **New**.
5. In **Create a New Group**, in the **Name** field, type a group names that is unique.
6. (Optional) In the **Description** field, type a brief note about the composition of the group.
7. From the **Provider** list, select the authentication provider that corresponds to the identity store where the group information is contained.
8. Click **OK**

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.

See Example of Users, Groups, and Application Roles Security Setup and Using Oracle WebLogic Server Administration Console.

1. Launch 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.
7. Click **Save**.

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 the user from the policy store, the Oracle BI Presentation Catalog, the metadata repository, and the identity store.

See Delete Users Command in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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

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

1. Delete the user from the policy store.
2. Delete the user from the Oracle BI Presentation Catalog, and the metadata repository using the `deleteusers` command.
3. Log in to the Oracle WebLogic Server Administration Console.
4. Select **Security Realms**, and select the realm containing the user, for example, **myrealm**.
5. Click **Users and Groups** tab, then click **Users**.
6. Select a user, click **Delete**.
7. In Delete Users, click **Yes**.
8. Click **OK**.

Changing a User Password in the Embedded WebLogic LDAP Server

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

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

1. In Oracle WebLogic Server Administration Console, select **Security Realms**, and click the realm you are configuring, for example, *myrealm*.
2. Select the **Users and Groups** tab, and then click **Users**.
3. In the Users table, select the user receiving the changed password.
4. In the user's Settings page, select the **Passwords** tab.
5. Type the password in the **New Password** and **Confirm Password** fields.
6. Click **Save**.

Managing Application Roles and Application Policies Using Fusion Middleware Control

Application roles and application policies provide permissions for users and groups.

After creating a service instance or importing a BI application archive (BAR) file into a service instance, you should check the security policy in the service instance to ensure that 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. As a best practice, check the security policy on your service instance after importing a BI application archive file.

A BI application archive file that has the BI metadata for an application contains pre-defined application roles that you can use to provision users with permissions. For example, the sample application contains the application roles, BIConsumer, BIContentAuthor, and BIServiceAdministrator. To provision users with permissions and privileges, you map users and groups from the Identity Store, usually an LDAP directory, to the defined application roles.

> **Important:**
>
> You use Oracle Enterprise Manager Fusion Middleware Control to manage operations on permission grants. You must use Oracle WebLogic Scripting Tool (WLST) commands to perform operations on permission set grants. See `grantEntitlement` and `revokeEntitlement`. See OPPS Security Store WLST Commands in Oracle Fusion Middleware *WLST Command Reference for Infrastructure Security* guide.

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

See:

- Creating and Deleting Application Roles Using Fusion Middleware Control.

  You can create application roles based on preconfigured Application policies, or you can create your own Application policies. See Working with Users, Groups, and Application Roles.
- Creating Application Policies Using Fusion Middleware Control.
- Modifying Application Roles Using Fusion Middleware Control.

Displaying Application Policies and Application Roles Using Fusion Middleware Control

You can display application policies and application roles that are assigned to permission set grants in Fusion Middleware Control.

Fusion Middleware Control displays permission grants and permission set grants. You can only carry out operations on the permission grants. If you add a permission grant to your application role using Fusion Middleware Control, you can delete the application role through Fusion Middleware Control.

You need to use WLST commands to manage permission set grants. See OPSS Security Store WLST Commands in *Fusion Middleware WLST Command Reference for Infrastructure Security*.

1. Log in to 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. Select one of the following options:
   - Right-click **biinstance**, select**Security**, and then select **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. Select **Application Policies** or **Application Roles** to display either the Application Policies page or the Application Roles page.

Creating and Deleting Application Roles Using Fusion Middleware Control

Use Fusion Middleware Control to create, delete, and manage application roles.

In a new Oracle Business Intelligence deployment, you create an application role for each type of business user activity in your Oracle Business Intelligence environment. For example, a deployment based on the sample application or the starter application might include the BIConsumer, BIContentAuthor, and BIServiceAdministrator application roles. 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 is assigned to a user. For example, the Sales Analyst application role might grant a user access to view, edit and create reports on a company's sales pipeline. The service instance administrator can create and modify application roles. 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 changing the groups defined in the corporate directory server. To control authorization requirements, you can then assign existing groups of users from the directory server to application roles.

Before creating a new application role and adding the application role 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. See Granting Permissions To Users Using Groups and Application Roles.

See Managing the Policy Store in *Securing Applications with Oracle Platform Security Services*.

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

- Creating Application Roles
- Creating Application Roles from Existing Roles
- Assigning a Group to an Application Role
- Deleting Application Roles

Creating Application Roles

Create application roles in Fusion Middleware Control using these steps.

You can also add members to the application role. See Characters in Application Role Names in *Securing Applications with Oracle Platform Security Services*.

You can create application roles by copying an existing role, see Creating Applications Roles From Existing Roles.

Valid members of an application role are users, groups, and other application roles.

Membership for an application role is controlled using the Application Roles 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, see Creating Application Policies Using Fusion Middleware Control. Permission and permission set grants are displayed in the Application Policies page in Fusion Middleware Control.

1. Log in to Fusion Middleware Control, and select the Application Roles page.
2. In Application Roles, verify that the value in the **Application Stripe** field is *obi*, and click the search icon next to **Role Name**.
3. Click **Create**.
4. In Application Role, in **Role Name**, type a name for the application role without invalid special characters and spaces.
5. In **Display Name**, type the name for the application role that displays in the user interface.
6. (Optional) In **Description** , type a explanation for the use of the application role.
7. In the **Members** section, click **Add**.
8. In **Add Principal**, from the **Type** list, select *Application Role*, *Group*, or *Users*.
9. (Optional) In the **Principal Name** and **Display Name** fields, enter search criteria, and click **Search**.
10. In the **Searched Principals**, select a result, and click **OK**.

Creating Application Roles from Existing Roles

You can create 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. You can make modifications to customize the new application role.

See Characters in Application Role Names in *Securing Applications with Oracle Platform Security Services*.

1. Log in to Fusion Middleware Control, and display the Application Roles page.
2. From the list **Application Stripe** list, select *obi*.
3. Click the search icon next to **Role Name**.
4. Select the application role you want to copy from the list.
5. Click **Create Like**.
6. In the **General** section, in **Role Name**, type the name of the application role without using any invalid characters or spaces.
7. (Optional) In **Display Name**, type the display name for the application role
8. (Optional) In **Description**, type a description for the use of the application role.
9. In the **Members** section, click **Add**.

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

10. In Add Principal, from the **Type** list, select an *Application Role*.
11. (Optional) In the **Principal Name** and **Display Name** fields, type your search criteria, and click **Search**.
12. In **Searched Principals**, select a result, and click **OK**.
13. Modify the members as appropriate, and click **OK**.

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.

See 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.

1. Log in to Fusion Middleware Control, and display the Application Roles page.
2. If necessary, select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.
3. Select an application role in the list and click **Edit** to display the Edit Application Role dialog.
4. From **Role Name**, select an application role to use.
5. (Optional) In **Display Name**, type the application role name to display in the user interface.
6. (Optional) In **Description**, type a brief description for the use of the application role.
7. 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.
8. Click **OK** to return to the Application Roles page.

Deleting Application Roles

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

See Displaying Application Policies and Application Roles Using Fusion Middleware Control.

1. Log in to Fusion Middleware Control, and display the Application Roles page.
2. Select the application role you want to delete.

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

Creating Application Policies Using Fusion Middleware Control

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

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

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. InFusion Middleware Control, you can modify permission grants against application roles. In Oracle BI EE 12*c*, if you need to update permission set grants against an application role you need to use the WLST command line, see Managing Policies with WLST in *Securing Applications with Oracle Platform Security Services*.

You can create an application policy using on an existing application policy.

The Principal represents the name of the policy grantee.

1. Log in to Fusion Middleware Control, and display the Application Policies page.
2. Select **obi** from the **Application Stripe** list, then click the search icon next to **Name**.
3. Select an existing policy from the table.
4. Click **Create Like** to display the Create Application Grant Like page.
5. Click **Add Application Role** in the **Grantee** area to display the Add Application Role dialog and add application roles to a policy.
6. Complete the **Search** area and click the blue search button next to the **Display Name** field.
7. Select from the **Searched Principals** list and click **OK**.

   The Create Application Grant Like page displays with the selected application role added as *Grantee*.
8. Click **OK** to return to the Application Policies page.

Modifying Application Roles Using Fusion Middleware Control

You can modify an application role by changing permission set 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:

- Adding an Application Role to an Application Policy
- Adding or Removing Members from an Application Role
- Renaming an Application Role

See Managing Policies with Fusion Middleware Controlin *Securing Applications with Oracle Platform Security Services*.

Adding an Application Role to an Application Policy

Use this procedure to change the permission grants for an application role by adding the application role to an application policy using Fusion Middleware Control.

For permission grant changes, you can perform these tasks in Fusion Middleware Control. To change permission set grants, you must use Oracle WebLogic Server Administration Console.

1. Log in to Fusion Middleware Control
2. Click **Target Navigation**.
3. In Target Navigation, expand **Business Intelligence**, and select the **biinstance**.
4. From the **biinstance** list, select **Security**, and then select **Application Policies**.
5. In Application Policies, from the **Application Stripe**, select *obi*.
6. Click the arrow next to **Principle Role** to search the associated application roles.
7. From the **Principal** column, select an application role, and click **Edit**.
8. In Grantee, click **Add**.
9. In the Add Principal, search for an application role.
10. After adding an application role, in Permissions, click **Add**.
11. In Add Permission, select the permissions that you want to grant the application role.

Adding or Removing Members from an Application Role

You can add or delete members 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.

Assign groups instead of individual users to application roles as a best practice, and then assign users to the groups.

> **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.

See Displaying Application Policies and Application Roles Using Fusion Middleware Control.

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

2. If not already displayed, select **Application Stripe** and **obi** from the list, then click the search icon next to **Role Name**.
3. Select the cell next to the application role name and click **Edit** to display the Edit Application Role page.
4. To delete a member, select the **Name** of the member to activate the **Delete** button, then click **Delete**.
5. Click the **Add** to add a member.
   a. Select Application Role, Group, or Users from the **Type** field list.
   b. (Optional) Enter search details into **Principal Name** and **Display Name** fields.
   c. Click Search.
   d. From the **Searched Principals**, make your selection from the results.
   e. Click **OK**.
6. Click **OK** in the Edit Application Role page to return to the Application Role page.

See Managing Application Roles in *Securing Applications with Oracle Platform Security Services*.

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 *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

Managing Metadata Repository Privileges Using the Oracle BI Administration Tool

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.

Use the Oracle BI Administration Tool to configure security in the Oracle BI repository:

- Setting Metadata Repository Privileges for an Application Role
- Managing Application Roles in the Metadata Repository - Advanced Security Configuration Topic

Setting Metadata Repository Privileges for an Application Role

The data model for your service instance includes a security policy that defines permissions for accessing different parts of the data model, such as 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.

See Setting Presentation Services Privileges for Application Roles, and Setting Permissions Using Command-Line Tools in *XML Schema Reference for Oracle Business Intelligence Enterprise Edition*.

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

To view the 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 the permissions for the selected object.

1. Open the repository in the Oracle BI Administration Tool in Online mode.
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.
4. Click *Permissions*.
5. In Permissions <*subject area name*> properties, click the **Show all users/ application roles** if the check box is not checked.
6. In the Permissions <*subject area name*> dialog, update **User/Application Role** permissions to match your security policy.

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

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.

Managing Presentation Services Privileges Using Application Roles

The catalog for your service instance includes a security policy for Presentation Services 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.

You use application roles to manage privileges.

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.

About Presentation Services Privileges

Presentation Services privileges are managed 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.

- Setting Presentation Services Privileges for Application Roles
- Encrypting Credentials in BI Presentation Services - Advanced Security Configuration Topic

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:**
>
> You can assign Presentation Services privileges to a new application role programmatically, see SecurityService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

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

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.

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.

1. Log in to Oracle BI Presentation Services as a user with Administrator privileges.
2. From the Home page in Presentation Services, select **Administration**.
3. In the Security area, click Manage 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.
7. Save your changes.

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 a 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) to prevent 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. Proprietary key-based encryption provides security to prevent unauthorized users from accessing the metadata repository.

Managing Data Source Access Permissions Using BI Publisher

You manage the data source access permissions stored in BI Publisher, using the 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 that 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.

See Granting Data Access in *Administrator's Guide for Oracle Business Intelligence Publisher*.

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

Use this procedure to enable high availability in a clustered environment when using the default WebLogic LDAP identity store.

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

Use lowercase for the property name `virtualize` . Use uppercase for the property name `OPTIMIZE_SEARCH`.

1. Log in to 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`*
6. Click **OK** to save the changes.
7. Restart the Administration server, any Managed servers, and Oracle BI EE components.

Using runcat to Manage Security 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>
```

See Opening an Oracle BI Presentation Catalog in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

See Renaming an Application Role.

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
```

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.

For a detailed list of security setup steps, see Process for Setting Up Security in Oracle Business Intelligence.

This chapter contains the following sections:

- Introduction
- High-Level Steps for Configuring an Alternative Authentication Provider
- Setting Up Groups and Users in the Alternative Authentication Provider
- Configuring Oracle Business Intelligence to Use Alternative Authentication Providers
- Resetting the BI System User Credential

Introduction

When you use an alternative authentication provider, you 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.

See 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. See System Requirements and Certification.

You can configure one or more supported authentication providers, see 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.

High-Level Steps for Configuring an Alternative Authentication Provider

Use these steps as a general guide for configuring an alternative authentication provider.

See Setting Up Groups and Users in the Alternative Authentication Provider, Configuring Oracle Business Intelligence to Use Alternative Authentication Providers, and see Adding or Removing Members from an Application Role.

1. Ensure your external Identity Store has all the users and groups setup for use with Oracle Business Intelligence.
2. Configure the necessary authentication provider(s).
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.

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. Follow these steps to set up an alternative authentication provider.

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 Example of Users, Groups, and Application Roles Security Setup.

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 created groups. 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.

Configuring Oracle Business Intelligence to Use Alternative Authentication Providers

Follow these options to configure Oracle Business Intelligence to use one or more authentication providers instead of the default Oracle WebLogic Server LDAP directory.

This section contains the following topics:

- Reconfiguring Oracle Internet Directory as an Authentication Provider
- Reconfiguring Microsoft Active Directory as the Authentication Provider
- Configuring User and Group Name Attributes in the Identity Store
- Configuring LDAP as the Authentication Provider and Storing Groups in a Database
- Configuring a Database as the Authentication Provider
- Configuring Identity Store Virtualization Using Fusion Middleware Control
- Configuring Multiple Authentication Providers
- Setting the JAAS Control Flag Option
- 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 an *Identity Store Virtualization*, see Configuring Identity Store Virtualization Using Fusion Middleware Control.

> **Note:**
>
> If you are configuring Oracle Unified Directory as the alternative LDAP authentication provider, see Accessing Other LDAP Servers and Configuring an Authentication Provider for Oracle Unified Directory in *Administering Security for Oracle WebLogic Server*

Reconfiguring Oracle Internet Directory as an Authentication Provider

Use these steps to reconfigure the Oracle Internet Directory (OID) LDAP as the authentication provider.

> **Note:**
>
> 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. The LDAP authenticators, including the `OracleInternetDirectoryAuthenticator` and the `ActiveDirectoryAuthenticator`, default to *cn* as the user name and group name attributes. You can use alternative attributes for the user name such as *uid* or *mail*.
>
> See Oracle Internet Directory Authenticator Provider Specific Reference to learn about the values for the Provider Specific tab.

See the following:

- Configuring User and Group Name Attributes in the Identity Store.
- Setting the JAAS Control Flag Option.
- About Configuring the Authentication Providers in WebLogic Server in *Administering Security for Oracle WebLogic Server*.

1. Log in to Oracle WebLogic Server Administration Console.
2. In the Change Center, click **Lock & Edit** .
3. In Domain Structure, select **Security Realms**, and click **myrealm**.
4. Click the **Providers** tab, then click the **Authentication** tab.
5. Click **New** .
6. In Create a New Authentication Provider, in the **Name** field, type a name for the authentication provider such as *MyOIDDirectory*.
7. From the **Type** list, select *OracleInternetDirectoryAuthenticator*.
8. Click **OK** to save the changes and display the authentication providers list updated with the new authentication provider.
9. In the **Authentication Providers** table, under the **Name** column, click *MyOIDDirectory*.
10. In Settings for *MyOIDDirectory*, click the **Configuration** tab and then click the **Common** tab.
11. From the **Control Flag** list, select *SUFFICIENT*, and then click **Save**.
12. Click the **Provider Specific** tab, in the Connection properties, type your values for **Host**, **Port**, **Principal**, and **Credential**.
13. In the Provider Specific tab, Group area, specify value for the **Group Base DN** (distinguished name).
14. In the Provider Specific tab, Users area, specify the following:

- **User Base DN**
- **All Users Filter**
- **User From Name Filter**
- **Use Retrieved User Name as Principal**
- **User Name Attribute**

15. Click **Save**.

You must also complete these tasks:

- Configuring the Default Authenticator Control Flag
- Reordering Authentication Providers

After completing the above tasks, in the Change Center, click **Activate Changes**, and then restart Oracle WebLogic Server.

Oracle Internet Directory Authenticator Provider Specific Reference

Review the table to complete the values required in the Oracle Internet Directory (OID) Authenticator.

Use this table to get the details about the fields in the Provider Settings page of the Settings for MyOIDDirectory, see Reconfiguring Oracle Internet Directory as an Authentication Provider.

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, because it is the default value for the Active Directory authenticator. 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 such as cn, uid, or mail. For example, to authenticate using a user's email address you set this value to `mail`. The value that you specify must match the User Name Attribute that you are using in the authentication provider.
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. 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.

Reconfiguring Microsoft Active Directory as the Authentication Provider

Follow this procedure 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)

See About Configuring the Authentication Providers in WebLogic Server in *Administering Security for Oracle WebLogic Server*.

See Setting the JAAS Control Flag Option and Configuring User Name Attributes.

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.
2. Select **Security Realms** from the left pane and click **myrealm**.

   myrealm is the default Security Realm.
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**.
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. 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.
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.

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.

> **Note:**
>
> The LDAP authenticators provided by WebLogic including `OracleInternetDirectoryAuthenticator` and `ActiveDirectoryAuthenticator`, use *cn* as the default user name and group name attributes. You can use alternative attributes for the user name, for example *uid* or *mail*.

13. Click **Save**.
14. In Settings for myrealm page, click the **Providers** tab, then click the **Authentication** tab.
15. Click **Reorder**.
16. In the Reorder Authentication Providers page, 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.

Configuring User and Group Name Attributes in the Identity Store

The LDAP authenticators provided by WebLogic, including OracleInternetDirectoryAuthenticator and ActiveDirectoryAuthenticator, default to using cn as the user name and group name attributes.

You might need to use alternative attributes for the user name, for example *uid* or *mail*. The need to use different group name attributes is less common. This section explains how to reconfigure user names and group names.

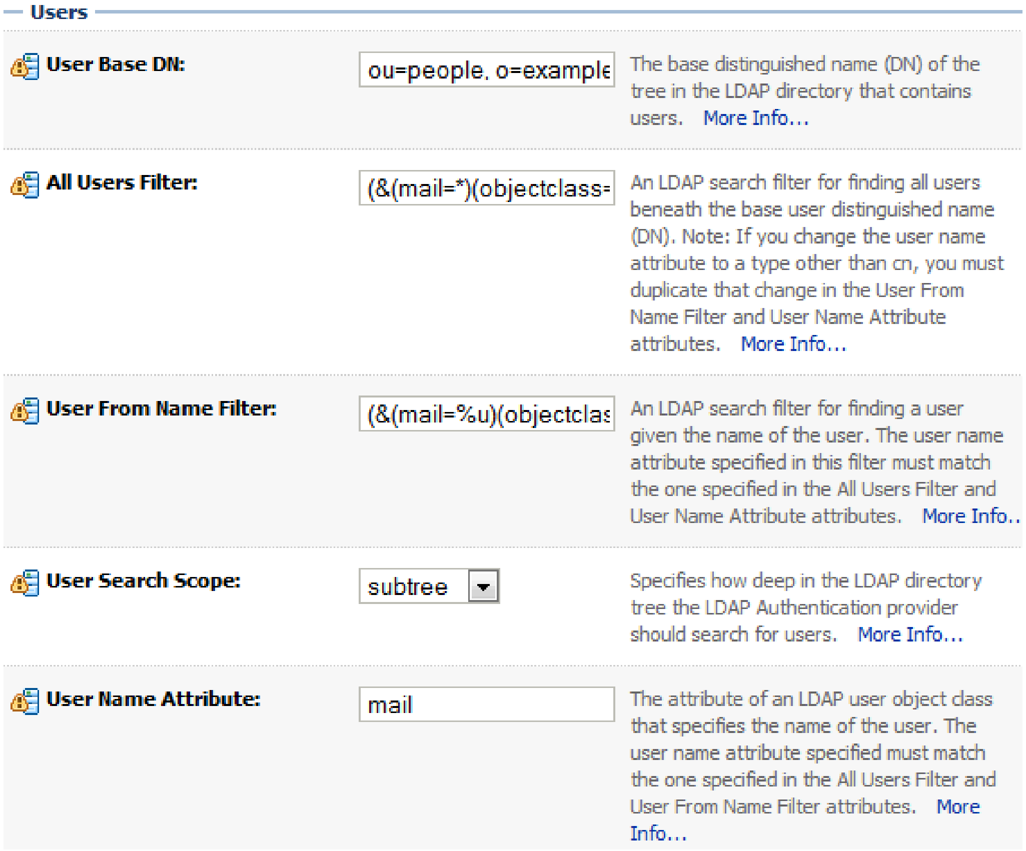
This topic contains the following sections:

- Configuring User Name Attributes
- Configuring Group Name Attributes

Configuring User Name Attributes

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

The **Users** section shows the **User Name Attribute** configured with the value *mail*.



Users

User Base DN: ou=people, o=example
The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...

All Users Filter: (&(mail=*)(objectclass=
An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a type other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. More Info...

User From Name Filter: (&(mail=%u)(objectclas
An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes. More Info..

User Search Scope: subtree
Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. More Info...

User Name Attribute: mail
The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in the All Users Filter and User From Name Filter attributes. More Info...

The `UserNameAttribute` in the alternative authentication provider is usually set to the value *cn*. If the `UserNameAttribute` is not set to *cn*, you must make sure the settings for AllUsersFilter and UserFromNameFilter are configured correctly as shown in the table. The table illustrates the default setting using the value *cn*, and a required new setting using a new value in the attribute `AnOtherUserAttribute`.

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, substitute the AnOtherGroupAttribute setting with your own value. See Configuring Oracle Business Intelligence to Use Alternative Authentication Providers.

Configuring Group Name Attributes

You can configure the ActiveDirectoryAuthenticator to use a group name other than *cn*.

If the group name for Active Directory server is set to anything other than the default value *cn*, you must change the group name. If you change the value, you must also change the values of *AllGroupsFilter* and *GroupFromNameFilter* as in the *AnOtherGroupAttribute* attribute.

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 the values in the table, substitute the *AnOtherGroupAttribute* setting with your own value. To display the Provider Specific tab, see Reconfiguring Microsoft Active Directory as the Authentication Provider.

Configuring LDAP as the Authentication Provider and Storing Groups 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:

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

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 Oracle 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.

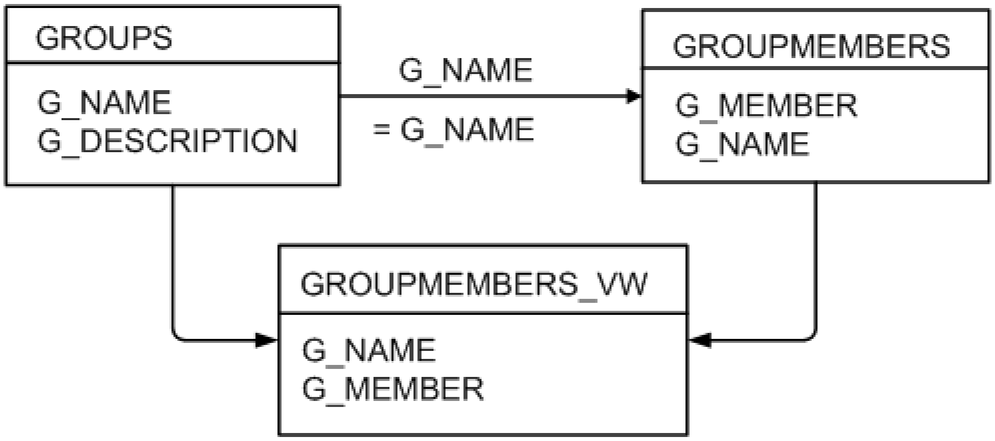
    You cannot have a group with the same name in both LDAP and database groups table. If you do, the security code invoked by Oracle BI Delivers cannot resolve application role membership.

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

An advantage of defining tables or views identical to those shown in the diagram is that the configuration of the `BISQLGroupProvider` can use the default SQL outlined in the table in Configuring the BISQLGroupProvider SQL Authenticator.



You must map the users in your LDAP store to groups in your database table by login name. In the diagram, 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. You should not, for example, map the database groups by *uid* if the login attribute is *mail*. Create a GROUPMEMBERS_VW view with an outer join between the GROUPMEMBERS and GROUPS tables.

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:

- Configuring Oracle Internet Directory as the Primary Identity Store for Authentication Using Oracle WebLogic Server
- Installing the BISQLGroupProvider
- Configuring the Data Source Using Oracle WebLogic Server Administration Console
- Configuring the BISQLGroupProvider SQL Authenticator

Configuring Oracle Internet Directory as the Primary Identity Store for Authentication Using Oracle WebLogic Server

Use the instructions in the link to configure WebLogic to authenticate your user population against OID LDAP.

See 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 for use later. See Configuring a Database Adaptor to Retrieve Group Information.

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 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.

Configuring the Data Source Using Oracle WebLogic Server Administration Console

These steps enable you 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.
2. Click **Services**, and click **Data Sources**.
3. In Summary of Data Sources, click **New**, and select **Generic Data Source**.
4. In JDBC Data Sources Properties , enter or select values for the following properties:
   - **Name**, for example, enter `BIDatabaseGroupDS`.

     The name used in the `config.xml` configuration file 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 where the JDBC data source is 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** list.

> **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 local host 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 Creating a Sample Schema for Groups and Group Members.

     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 Select Targets, choose the servers or clusters as deployment targets for your data source.

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

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

Configuring the BISQLGroupProvider SQL Authenticator

Follow these steps to create a BISQLGroupProvider against the BIDatabaseGroupDS data source using an example table structure.

This task explains how to create a BISQLGroupProvider against the BIDatabaseGroupDS data source using the example table structure outlined in 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.

See About Configuring the Authentication Providers in WebLogic Server in *Administering Security for Oracle WebLogic Server*.

1. Log in to Oracle WebLogic Server Administration Console as a WebLogic administrator, and click **Lock & Edit** in the Change Center.
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.
   - From the **Type** list , select *BISQLGroupProvider*.
   - 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`.
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..
    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.

Configuring the Virtualized Identity Store

You configure the virtualized identity store as follows:

- Enabling Virtualization by Configuring the Identity Store
- Configuring SSL Against LDAP
- Configuring a Database Adaptor to Retrieve Group Information

Enabling Virtualization by Configuring the Identity Store

You configure the identity store to enable virtualization enabling the use of multiple identity stores with the identity store service.

You can split the user profile information across different authentication providers (identity stores), see Configuring Identity Store Virtualization Using Fusion Middleware Control.

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.

See Configuring SSL when Using Multiple Authenticators.

Configuring a Database Adaptor to Retrieve Group Information

You configure a database adaptor to make it appear like an LDAP server to enable the virtualized identity store provider to retrieve group information from a database using the database adapter.

In this task you create a file containing the elements for an adapter templates that specifies how to use your database tables as an identity store to map groups. The file describes the mapping of the `GROUPMEMBERS_VW` view to a virtual LDAP store. The view uses an outer join to ensure that you can reference fields from more than one table by the database adaptor.

1. Create a file named *bi_sql_groups_adapter_template.xml*.
2. Adapt the following elements to match your table and column attributes against LDAP server attributes.

> **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.VirtualAttribut
ePlugin</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="groupnameattr" table="GROUPMEMBERS" 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" field="G_NAME"
type=""/>
         </objectClass>
      </mapping>
      <useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
      <connectionWaitTimeout>10</connectionWaitTimeout>
      <oracleNetConnectTimeout>0</oracleNetConnectTimeout>
      <validateConnection>false</validateConnection>
   </dataBase>
</adapters>
```

3. Customize appropriate sections for the following elements:
   - ReplaceAttribute

Specifies how to define the unique member for a group. The `%uniquemember%` is a placeholder for a value that is passed 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 7.

- groupofuniquenenames

  Specifies how group attributes are mapped to database fields.

  You must map the following attributes:

  – *cn* maps to a unique name for your group.

  – **uniquemember** maps 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.

  No other attributes are 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 9500 -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:**
>
> Use the *JNDI* name and not just the *DS* name for the *dataSourceJNDIName*.

> **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, set the root 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 can ignore the following `Warning: BISQLGroupsProvider: Connection pool not usable.`

Log in to WebLogic and Oracle Business Intelligence using credentials stored in the database.

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

You can 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.
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.

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.

See Correcting Database Adapter Errors by Deleting and Recreating the Adapter.

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:

- Introduction and Prerequisites
- Creating a Sample Schema for Users and Groups
- Configuring a Data Source and SQL Authenticator Using the Oracle WebLogic Server Administration Console
- Configuring the Virtualized Identity Store
- Troubleshooting the SQL Authenticator
- Correcting Database Adapter Errors by Deleting and Recreating the Adapter

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.

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.

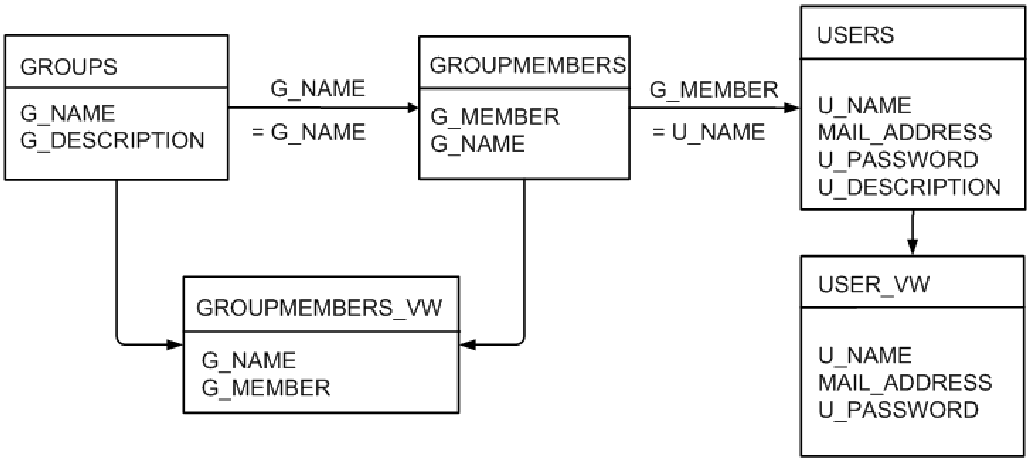
Oracle Business Intelligence Enterprise Edition Releases 11.1.1.5, 11.1.1.6, and 11.1.1.7 (or higher) must be installed and running. However, for Releases 11.1.1.5 and 11.1.1.6, you must also apply Oracle Fusion Middleware patch 13826887. See Patching Oracle Business Intelligence Systems in *System Administrator's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

Creating a Sample Schema for Users and Groups

You have schemas that you were using in an earlier installation of Oracle BI EE. This sample schema is intended to illustrate how to configure the system to use this schema.

> **Note:**
>
> You must use a database schema containing the users, credentials and groups required for authentication that is accessible from the WebLogic Server where Oracle BI EE is running.

The diagram shows 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.



If 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 the diagram to the database adapter, you would need to follow the configuration shown in Configuring a Database Adaptor.

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:

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

- Configuring a SQL Authenticator Using the Oracle WebLogic Server Administration Console
  - SQL Authenticator Select Statement Reference
  - Configuring the Default Authenticator Control Flag
  - Reordering Authentication Providers

Configuring a Data Source Using the Oracle WebLogic Server Administration Console

Use these steps to configure a data source using the Oracle WebLogic Server Administration Console.

The schema owner of the tables is defined in Creating a Sample Schema for Users and Groups.

See Using Oracle WebLogic Server Administration Console.

1. Log in to Oracle WebLogic Server Administration Console, navigate to the Change Center, click **Lock & Edit**.
2. Click **Services** 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 is 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** 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**
- **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.

Configuring a SQL Authenticator Using the Oracle WebLogic Server Administration Console

A user with the appropriate privileges can log in to the Oracle WebLogic Server Administration Console using the WebLogic database authenticator.

When creating the SQL authenticator, select the read-only SQL authenticator. The read-only authentication provider type does not write back to the database.

When entering the SQL statements in the Provider Specific tab, if your password column is in plain text as the result of the query supplied for the **SQL Get Users Password** column was not hashed or encrypted, select the **Plaintext Password Enabled** option.

If the **Plaintext Password Enabled** option is cleared, the `SQLAuthenticator` expects passwords 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.

See SQL Authenticator Select Statement Reference for help in defining the **Provider Specific** SQL statements.
After completing this task, you must Configure the Default Authenticator Control Flag, reorder the authentication providers, and restart the servers.

1. Log in to Oracle WebLogic Server Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. From Domain Structure, select **Security Realms** and click **myrealm**.
4. In Settings for myrealm, click the **Providers** tab, and then click the **Authentication** tab.

5. In **Authentication Provider**s, click **New**.
6. In Create a New Authentication Provider, in **Name** type a name for the authentication providers such as `UserGroupDBAuthenticator`.
7. From the **Type** list, select *ReadOnlySQLAuthenticator*, and click **OK**.
8. From the **Authentication Providers** table, select the provider you just created.
9. In the Settings for <*your new authentication provider name*>, click the **Provider Specific** tab.
10. (Optional) In the **Provider Specific** tab, if your password column is in plain text, select **Plaintext Password Enabled**.
11. In the **Data Source Name** field, type the name of an existing data source, for example, *UserGroupsDS*, to use this authentication provider.

    The data source name must match the existing data sources defined in Oracle WebLogic Server Administration Console.
12. In the **Provider Specific** tab, specify the SQL statements used to authenticate user access and to query your database tables.
13. After entering all of the required SQL statements for your authenticator, click **Save**.

You must configure the authentication provider control flag when using multiple authentication providers. See Configuring the Default Authenticator Control Flag.

SQL Authenticator Select Statement Reference

Learn options available for creating SQL statements when implementing a SQL authentication provider.

When you create a SQL Authenticator in the **Provider Specific** tab, you specify the SQL statements used to query, and authenticate against, your database tables. See Configuring a SQL Authenticator Using the Oracle WebLogic Server Administration Console.

The table shows SQL statements for the sample schema outlined in Creating a Sample Schema for Users and Groups.

If you are using a different table structure, you might need to adapt these SQL statements with the table or column names of your schema. You should use the question mark (?) as a runtime query placeholder rather than hard coding a user or group name.

Query	SQL	Notes
SQL Get Users Password	`SELECT U_PASSWORD FROM USERS WHERE U_NAME = ?`	This SQL statement looks 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 = ?`	This SQL statement looks 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.

Query	SQL	Notes
SQL List Users	`SELECT U_NAME FROM USERS WHERE U_NAME LIKE ?`	This SQL statement retrieves users that match a specific 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 ?`	This SQL statement retrieves 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 = ?`	This SQL statement looks 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 ?`	This SQL statement looks up members of a group. The SQL statement requires two parameters, a group name and a member or group name. This SQL statement must return a `resultSet`.
SQL List Member Groups	`SELECT G_NAME FROM GROUPMEMBERS WHERE G_MEMBER = ?`	This SQL statement looks up the group membership of a user or group. 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 the criteria.
SQL Get User Description	`SELECT U_DESCRIPTION FROM USERS WHERE U_NAME = ?`	This SQL statement retrieves the description of a specific user. The SQL statement is valid only if `Descriptions Supported` is enabled. 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.
SQL Get Group Description	`SELECT G_DESCRIPTION FROM GROUPS WHERE G_NAME = ?`	This SQL statement retrieves the description of a group. The SQL statement 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.

Configuring the Default Authenticator Control Flag

Use a JAAS Control Flag for each provider to control how the authentication providers are used in the login sequence.

You must complete this task if you are using multiple authentication providers.

1. From the *myrealm* Settings page, click the **Providers** tab, and then click the **Authentication** tab.
2. From the Authentication Providers table, select **DefaultAuthenticator**.

3. In Settings for DefaultAuthenticator on the **Configuration** page in the **Common** tab, from the **Control Flag** list, select *SUFFICIENT*.
4. Click **Save**.

See Reordering Authentication Providers to complete the next task in defining a SQL Authenticator process.

Reordering Authentication Providers

After adding a new authenticator, you can reorder the Authentication Providers table.

1. From the *myrealm* Settings page, click the **Providers** tab, and then click the **Authentication** tab.
2. In the **Authentication Providers** table, click **Reorder**.
3. In Reorder Authentication Providers, from **Available**, select the provider to use as the default, click the up arrow, and then click **OK**.
4. In the Change Center, click **Activate Changes**.

After restarting the Administration Server, use the Fusion Middleware Control to restart the Oracle Business Intelligence components, Oracle WebLogic Server, and managed servers.

Configuring the Virtualized Identity Store

Configure the virtualized identity store as follows:

- Enabling Virtualization by Configuring the Identity Store
- Configuring a Database Adaptor

Configuring a Database Adaptor

Follow these steps to configure a database adaptor to make the database appear like an LDAP server. This enables the virtualized identity store provider to retrieve user profile information from a database using the database adapter.

This task shows how to edit and apply adapter templates that specify how to use your database tables as an identity store. The example given here is for the sample schema that is used throughout Configuring a Database as the Authentication Provider.

When customizing the `adapter_template_usergroup1.xml` file, map the elements by matching the classes and attributes used in a virtual LDAP schema with the columns in your database. The virtual schema is the same as that of WebLogic Embedded LDAP, you can map database columns to any of the attributes shown in the table.

The following is the schema file 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>DBGUID</name>

<class>oracle.ods.virtualization.engine.chain.plugins.dbguid.DBGuidPlugin</class>
               <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="GUID"
type=""/>
                        </objectClass>
      </mapping>
      <useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
      <connectionWaitTimeout>10</connectionWaitTimeout>
      <oracleNetConnectTimeout>0</oracleNetConnectTimeout>
      <validateConnection>false</validateConnection>
   </dataBase>
</adapters>
```

In the `<objectClass>` element:

- The `name="person"` and `rdn="cn"` values declare the mapping of the LDAP `person` object class.
- The `cn` attribute is used as its Relative Distinguished Name (RDN).
- The child elements declare the LDAP attributes mapping to tables and columns in the database, for example:

  The line `<attribute ldap="uid" table="USER_VW" field="USER_ID" type=""/>` maps the `USER_ID` field of the `USER_VW` table to the standard LDAP attribute `uid`, a unique user id for each user.
- The `USER_VW` view should have a `GUID` column to match the `orclguid` attribute mapped to `GUID` column in `adapter_template_usergroup1.xml`, for example:

  You could CREATE or REPLACE VIEW USER_VW as the following:

  ```
  SELECT U_NAME, MAIL_ADDRESS, U_PASSWORD, U_DESCRIPTION, RPAD(U_NAME, 16, '0') AS
  GUID FROM USERS;
  ```

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

Attribute	Example
homepostaladdress	123 Main St., Anytown 12345

You map groups using the same method as you used for mapping a person. When mapping groups, in the `<objectClass name="groupofuniquenames" ...>` element, define the unique member for a group. The `%uniquemember%` value is a placeholder for a value that is passed in at runtime during the look up to determine if the user is a member of a group. The only aspect of this element you might want to change is the specification of the root for your users. The `%uniquemember%` value matches the root of your user population when you run the `libovdadapterconfig` script.

The `groupofuniquenames` object class 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` maps to a unique name for your group.
- `uniquemember` maps 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 `description` attribute is optional.

1. Create a file named `adapter_template_usergroup1.xml` that maps the user table to a virtual LDAP store.
2. In the `<mapping>` element, add the `<objectclass>` element with attributes similar to the following example:

```
<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="GUID" type=""/>
      </objectClass>
      </mapping>
```

3. Create a file, named `adapter_template_usergroup2.xml`, to map the group table to a virtual LDAP store.
4. In the `<objectClass name="groupofuniquenames">` element map the group table to the virtual LDAP store, as shown in the example:

```
  <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_MEMBER" type=""/>
```

```
                        </objectClass>
        </mapping>
```

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

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

6. Open a command prompt/terminal from within:

   ORACLE_HOME/oracle_common/bin

7. Verify that the environment variables are set:

   - ORACLE_HOME=*ORACLE_HOME*/oraclehome
   - WL_HOME=*ORACLE_HOME*/wlserver
   - JAVA_HOME=*ORACLE_HOME*/jdk/jre

8. Run the libovdadapterconfig script to create each of the two adapters from the template files using the syntax as follows:

```
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 9500 -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 9500 -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
```

9. Restart WebLogic Administration Server and Managed servers.

10. Sign in to WebLogic and Oracle WebLogic Server using credentials stored in the database.

Troubleshooting the SQL Authenticator

This section provides troubleshooting information on the SQL authenticator in the following topics:

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

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

You can use this diagnostic test if you are unable to login to Oracle Business Intelligence using a database user.

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.

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 Configuring Identity Store Virtualization Using Fusion Middleware Control and that your DBAdapter templates are correct in Configuring a Database Adaptor.

1. Log in to Oracle WebLogic Server Administration Console, and click **Lock & Edit** in the Change Center.
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** 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 match your user, directly or by membership in a group.

   For example, a possible condition is 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`.

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 are included in the log files for Administration Server and Managed Servers.

The following is an example of an error written to the log files.

```
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 Configuring a Data Source Using the Oracle WebLogic Server Administration Console.

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)
```

Correcting Database Adapter Errors by Deleting and Recreating the Adapter

Use this procedure to create a replacement adapter.

You cannot modify an existing database adapter, if you make an error in the `libovdadapter` command or the templates, you must delete then recreate the adapter.

1. Log in to the Oracle WebLogic Server console by running the `WLST` script.

   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://myserverexample:9500')
   ```

3. Delete the poorly configured adapter using the following syntax:

   ```
   deleteAdapter(adapterName='<AdapterName>')
   ```

   For example:

   ```
   deleteAdapter(adapterName='userGroupAdapter2')
   ```

4. Exit the WLST console using the `exit()` command.

Recreate the adapter with the correct settings by following the steps outlined in Configuring a Database Adaptor.

Configuring Identity Store Virtualization Using Fusion Middleware Control

Use these steps to configure identity store virtualization using Fusion Middleware Control.

If you are communicating with LDAP over SSL (one-way SSL only), see Configuring SSL when Using Multiple Authenticators.

Configure supported authentication providers as described in Configuring Oracle Business Intelligence to Use Alternative Authentication Providers.

1. Log in to 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**, 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:**
>
> Use lowercase for the Property Name `virtualize` , and use uppercase for `OPTIMIZE_SEARCH`.

> **Note:**
>
> If you are using multiple authentication providers, go to 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

6. Click **OK** to save the changes.
7. Restart the Administration Server and Managed Servers.

Configuring Multiple Authentication Providers

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.

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.

See 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 an one authenticator, from multiple configured authenticators, is unavailable and is not critical, use the following procedure to enable users from other authenticators to log in to Oracle Business Intelligence.

1. Open the `adapters.os_xml` file for editing 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* 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.

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.

See Set the JAAS control flag in the *Oracle WebLogic Server Administration Console Online Help*. You can also use the Oracle 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.

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 automatically generates the required users and groups in WebLogic Server LDAP. If you may have your own LDAP directory, for example, Oracle Internet Directory, that you want to use as the default authenticator, you must disable the WebLogic Server default authenticator. A single source authentication provider prevents deriving user names and passwords from multiple authentication sources which could lead to multiple points of attack, or entry from unauthorized users.

This topic contains the following sections:

- Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator
- Troubleshooting

Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator

Use the examples for configuring Oracle Internet Directory (OID LDAP). You can apply these examples to other LDAP authentication providers with minor changes.

- 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

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, you keep copies of this file.

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.

See 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.

Task 3 - Identify or Create Essential Users Required in OID LDAP

You must ensure that the essential users shown in the table are migrated from WebLogic Server LDAP to OID LDAP.

Standard WebLogic Server Users	New Users Required in OID LDAP
LCMManager,User	OID_LCMManagerUser; you can use any existing OID LDAP user.
For example, weblogic	OID_Weblogic; you can use 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.

Task 4 - Associate OID LDAP Groups with Global Roles in the WebLogic Console

Configure the global roles by mapping to OID LDAP groups.

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 the table, displayed in the Oracle WebLogic Server Administration Console, with your replacement OID LDAP groups, before you can disable the default WebLogic Server authenticator.

The default Security Realm is named *myrealm*.

Do not do add a new condition for the Anonymous and Oracle System roles, which can both remain unchanged.

1. Log in to Oracle WebLogic Server Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Select **Security Realms** from the left pane and click **myrealm**.
4. Click **Realm Roles**.
5. Click **Global Roles** and expand **Roles**.
6. Add a new condition for each Role.
7. Click **View Role Conditions**.
8. Select group from the **Predicate steps**.
9. Enter your newly-associated OID LDAP group, for example, assign the Admin role to the *OID_Administrators* role.
10. Save your changes.

After disabling the Default WebLogic Server Authentication, you can remove the old WebLogic Server groups, see Task 8 - Remove WebLogic Server Roles

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 the table.

New OID LDAP User	Is A Member Of These New OID LDAP Groups
OID_Weblogic	OID_Administrators OID_BIServiceAdministrators
OracleSystemUser A user with this exact name must exist in OID LDAP.	OracleSystemGroup A group with this exact name must exist in OID LDAP

> **Note:**
>
> In order to achieve the user and group membership shown in the table, you must have suitable access to update your OID LDAP server, or someone else must be able to update group membership on your behalf.

Task 6 - Remove the Default Authenticator

You are now ready to remove the Default Authenticators.

You must create an LDAP authenticator that maps to your LDAP source before performing this task, see Task 2 - Configure the System to use WebLogic Server and an Alternative Authentication Provider.

See Setting the JAAS Control Flag Option.

1. Change the **Control Flag** from *SUFFICIENT* to *REQUIRED* in the Oracle WebLogic Server Administration Console.
2. Save the changes.
3. Delete any other authenticators so that your *OID LDAP* authenticator is the single source.

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 Oracle 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.

Task 8 - Remove WebLogic Server Roles

Complete this task if everything is working correctly.

The following are examples of WebLogic Server roles to remove using this procedure:

- Admin
- AdminChannelUsers
- AppTester
- CrossDomainConnector
- Deployer
- Monitor
- Operator

See Task 4 - Associate OID LDAP Groups with Global Roles in the WebLogic Console.

Back up your `config.xml` file, before performing this step, see Task 1 - Enable Backup and Recovery.

1. Edit global roles.
2. Remove all WebLogic Server roles that were automatically created, from the `OR` clause.
3. Save your changes.

Task 9 - Stop Alternative Methods of Authentication

You must remove the USER variable and may need to update initialization blocks in the metadata repository.

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.

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 *USER* system session variable.

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 *PROXY* and *PROXYLEVEL* system session variables do not allow users to bypass security.

   The *PROXY* and *PROXYLEVEL* system variables 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.

If you disable an initialization block, then any dependent initialization blocks is also 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.

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, 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.

Resetting the BI System User Credential

Follow these steps to reset 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.

1. From the Fusion Middleware Control target navigation pane, expand the farm, then expand **WebLogic Domain**, and select **bi**.
2. From the WebLogic Domain menu, select **Security**, then **Credentials**
3. Expand the **oracle.bi.system** credential map, select **system.user** and click **Edit**.
4. In the Edit Key dialog, update the user name or password using values that do not match the credentials of a user in your Identity Store.

   > **Note:**
   >
   > `system.user` must not be set to an actual user. It is used for internal authentication between various Business Intelligence components. You must provide a unique, random user name and password that aren’t used by an actual system user.

5. Click **OK**.
6. Restart the system.

4

Enabling SSO Authentication

These topics provide guidelines for configuring single sign-on (SSO) authentication for 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 Single Sign-On with Smart View
- 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. You can assume that Oracle Access Manager is the SSO authentication provider.

SSO Configuration Tasks for Oracle Business Intelligence

The table contains SSO authentication configuration tasks and provides links for obtaining more information.

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.	Configuring SSO in an Oracle Access Manager Environment Configuring Single Sign-On in Oracle Fusion Middleware in *Securing Applications with Oracle Platform Security Services*
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 *Securing Applications with Oracle Platform Security Services*

Task	Description	For More Information
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.	Configuring an OID Authenticator for Oracle WebLogic Server Configuring Oracle Business Intelligence to Use Alternative Authentication Providers *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.	Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server Configuring Oracle Business Intelligence to Use Alternative Authentication Providers *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.	Configuring Custom SSO Environments
Enable Oracle Business Intelligence to accept SSO authentication.	Enable the SSO provider configured to work with Oracle Business Intelligence.	Enabling Oracle Business Intelligence to Use SSO Authentication

Note:

For an example of an Oracle Business Intelligence SSO installation scenario, see *Enterprise Deployment Guide for Oracle Business Intelligence*.

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.

You can configure Oracle Business Intelligence to trust incoming HTTP requests authenticated by a SSO solution that is configured for use with Oracle Fusion Middleware and Oracle WebLogic Server. See Configuring Single Sign-On in Oracle Fusion Middleware in *Securing Applications with Oracle Platform Security Services*.

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, the user identity and SSO cookie, is specified and configured.

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.

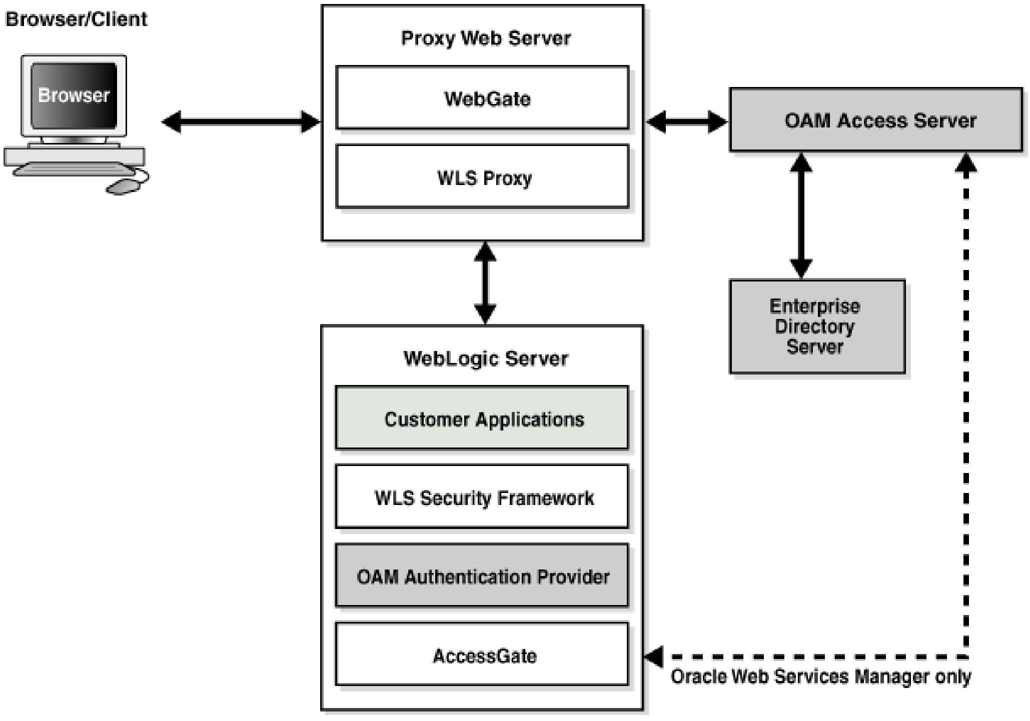
After the authentication provider for Oracle Access Manager is configured as the Identity Asserter for single sign-on, the web resources are protected. Perimeter authentication is performed by WebGate on the web tier and by the *appropriate token* to assert the identity of users who attempt access to 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.

The diagram 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.



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.

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, you must secure the machines that communicate directly with Presentation Services. In the `instanceconfig.xml` file, specify the list of HTTP Server or servlet container IP addresses in the `Listener\Firewall` node. The `Firewall` node must include the IP addresses of all Oracle BI Scheduler instances, Oracle Presentation Services instances, and Oracle Business Intelligence *JavaHost* instances.

If any of these components are co-located with Oracle BI Presentation Services, you must add the 127.0.0.1 address in `Firewall` node. Setting the list of HTTP Server or servlet container IP addresses 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.

Configuring SSO in an Oracle Access Manager Environment

Review the overview about how to configure SSO in an Oracle Access Manager environment, and these additional references.

After the Oracle Fusion Middleware environment is configured, you must do the following 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 the Presentation Services to the SSO provider.
- Configure the new identity store as the main authentication source for the Oracle WebLogic Server domain whereOracle Business Intelligence has been installed. See Configuring an OID Authenticator for Oracle WebLogic Server.
- Configure the Oracle WebLogic Server domain where Oracle Business Intelligence is installed to use an Oracle Access Manager identity asserter. See Configuring Oracle Access Manager as a New Identity Asserter for Oracle WebLogic Server.
- After the SSO environment configuration is complete, enable SSO authentication for Oracle Business Intelligence. See Enabling SSO Authentication Using Fusion Middleware Control .

See Configuring Single Sign-On in Oracle Fusion Middleware in *Securing Applications with Oracle Platform Security Services*.

See Configuring BI Publisher to Use Oracle Access Manager (OAM) Single Sign-On in *Administrator's Guide for Oracle Business Intelligence Publisher*.

Configuring an OID 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 such as Oracle Internet Directory (OID) as the main authentication source, you must configure the Oracle WebLogic Server domain, where Oracle Business Intelligence is installed.

See *Administering Security for Oracle WebLogic Server* and Using Oracle WebLogic Server Administration Console.

See Setting the JAAS Control Flag Option.

For the field details to complete the Provider Specific tab, see Authentication Provider Specific Reference.

1. Click the newly added authenticator in the **authentication providers** table.
2. Navigate to **Settings**, then select the **Configuration\Common** tab:

- Select **SUFFICIENT** from the **Control Flag** list.
- Click **Save**.

3. Display the **Provider Specific** tab and specify the following settings using appropriate values for your environment:
4. Click **Save**.
5. 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** tab, then select **DefaultAuthenticator** to display its configuration page.
   b. Display the **Configuration\Common** tab, from the **Control Flag** list, select *SUFFICIENT*.
   c. Click **Save**.
6. 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.
7. In the Change Center, click **Activate Changes**.
8. Restart Oracle WebLogic Server.

1. Log in to Oracle WebLogic Server Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. From Domain Structure, select **Security Realms** and click **myrealm**.
4. In Settings for myrealm, click the **Providers** tab, and then click the **Authentication** tab.
5. In **Authentication Providers**, click **New**.
6. In Create a New Authentication Provider, type the **Name** for the authentication providers such as `OID Provider`.
7. From the **Type** list, select *OracleInternetDirectoryAuthenticator*, and click **OK**.
8. From the **Authentication Providers** table, select the provider you just created.
9. Click the **Common** tab, from the **Control Flag** list, select *Sufficient*, and click **Save**.

Use Reordering Authentication Providers to make the OID authenticator the primary authentication used by Oracle WebLogic Server. Reorder the authenticators as follows:

- OID Authenticator (*SUFFICIENT*)

- OAM Identity Asserter (*REQUIRED*)
- Default Authenticator (*SUFFICIENT*)

Authentication Provider Source Reference

This table provides a reference for adding an authentication provider.

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 asterisk (*) filters for all users. Click **More Info...** for details.
Users	User From Name Filter	The LDAP search filter. Click **More Info...** for details.
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*. 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 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 You should not change this default value, in most cases the default value here is sufficient.

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.

See Enabling Oracle Business Intelligence to Use SSO Authentication.

1. Log in to 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 **Providers**.
4. Click **New**. Complete the fields as follows:
   - **Name**: *OAM Provider*, or a name of your choosing.
   - **Type**: OAMIdentityAsserter.
5. Click **OK**.
6. Click **Save**.
7. 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 reorder the list of providers as follows:
      - OID Authenticator (SUFFICIENT)
      - OAM Identity Asserter (REQUIRED)
      - Default Authenticator (SUFFICIENT)
   c. Click **OK** to save your changes.
8. In the Change Center, click **Activate Changes**.
9. 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.
10. Enable SSO authentication.
    .

Configuring Custom SSO Environments

This section contains references to information about setting up custom SSO environments.

For information about configuring Oracle Business Intelligence to participate in custom SSO environments, for example, setting up SSO using SiteMinder, see article 1287479.1 on My Oracle Support at:

`https://support.oracle.com`

Configuring Single Sign-On with Smart View

This topic describes the steps required to configure Single Sign-On (SSO) with Smart View. It applies to Smart View clients that are integrated with an Oracle Business Intelligence Enterprise Edition server that is SSO-enabled with Microsoft Active Directory and Native Authentication.

These steps allow Smart View users to launch Smart View on their Windows PCs and connect to Oracle Business Intelligence analytics without being prompted for a login username and password. The SSO login information is passed seamlessly from Microsoft Active Directory to Oracle Business Intelligence to Smart View.

Before you begin, you must have configured Oracle Business Intelligence to use Windows Server Active Directory as an LDAP Authentication source and to use Windows Native Authentication in an SSO environment. This process is described in the white paper *Configuring authentication and SSO with Active Directory and Windows Native Authentication in Oracle Business Intelligence Enterprise Edition* available as part of article 1274953.1 on My Oracle Support.

1. Verify that you can sign in and connect to Oracle Business Intelligence using the Microsoft Active Directory username and password.
2. Install the Smart View client on any Windows machines running Smart View. You can download the most current Smart View version from Oracle Technology Network (OTN).
3. On the Oracle Business Intelligence server, make a backup copy of the existing `jbips.ear` file.
4. Use the `jar` command to unpack the `jbips.ear` file into a temporary directory.

   ```
   jar -xvf jbips.ear
   ```

5. Add the following to the `web.xml` file before the `<welcome-file-list>` section of the document:

   ```
   <security-constraint>
       <web-resource-collection>
           <web-resource-name>JBIPS</web-resource-name>
           <url-pattern>/*</url-pattern>
       </web-resource-collection>
       <auth-constraint>
           <role-name>SSORole</role-name>
       </auth-constraint>
   </security-constraint>
   <login-config>
       <auth-method>CLIENT-CERT</auth-method>
   </login-config>
   <security-role>
       <role-name>SSORole</role-name>
   </security-role>
   ```

6. Modify the `weblogic.xml` file and add the following:

   ```
   <context-root>jbips</context-root>
   <security-role-assignment>
       <role-name>SSORole</role-name>
       <principal-name>BIUsers</principal-name>
       <principal-name>BIAdmins</principal-name>
        <principal-name>Domain Users</principal-name>
       <principal-name>Users</principal-name>
   </security-role-assignment>
   </weblogic-web-app>
   ```

7. Modify the `MANIFEST.MF` file to add the version:

   ```
   Weblogic-Application-Version: 12.2.1
   ```

8. Recreate the `jbips.ear` file using the `jar` command:

   ```
   jar -cfm jbips.ear /META-INF/MANIFEST.MF
   ```

9. Sign in to the WebLogic Server console and delete the existing `jbips.ear` file.

10. Use the WebLogic Server console to deploy the newly created `jbips.ear` file . When deploying, don’t enter the version. The version number is picked up by the changes to the `MANIFEST.MF` file.
11. Restart the servers and retest Smart View to confirm that SSO is working as expected.

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.

- Enabling and Disabling SSO Authentication Using WLST Commands
- Enabling SSO Authentication Using Fusion Middleware Control

Enabling and Disabling SSO Authentication Using WLST Commands

Use WLST commands to enable or disable SSO authentication for Oracle Business Intelligence.

In Oracle Business Intelligence 12.2.1.3.0, lightweight SSO is enabled by default. If you are using legacy authentication methods such as session variables in initialization blocks, you need to disable lightweight SSO using the `disableBISingleSignOn` command.

- You must have file system and WebLogic Administrator permissions.
- You must perform the enable or disable SSO authentication as an offline activity.
- Validation is limited to URL format. Connectivity and WebLogic configuration is not validated.
- Changing the URL for log off requires that you disable, and then re-enable with new URL.
- A logon URL is not required.

Pre-requisites:

- Configure WebLogic security providers, see About Configuring WebLogic Security Providers in *Administering Security for Oracle WebLogic Server*.

See Using the WebLogic Scripting Tool (WLST) in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

See Starting Oracle Business Intelligence Component Processes in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Use the table to learn the arguments appropriate for each command.

Command	Arguments	Return	Description
`enableBISingleSignOn`	*DOMAIN_HOME*, *<logoff-url>*	None	Enable SSO and configure logoff URL.

Command	Arguments	Return	Description
`disableBISingleSignOn`	*DOMAIN_HOME*	None	Disable SSO.

1. Stop the BI system.

   For example on UNIX, use `./stop.sh`

2. Enter a SSO management command from the table using the WLST command line.

   For example, on UNIX change directory to:

   `<Install_Directory>/oracle_common/common/bin`

3. Start WLST using `./wlst.sh` command.

4. (Optional) Run the command `help('BILifecycle')` to display help about `enableBISingleSignOn` and `disableBISingleSignOn` commands and their arguments.

5. Run the `enableBISingleSignOn` or `disableBISingleSignOn` command using the arguments appropriate for each command.

   For example: `enableBISingleSignOn('C:/.../user_projects/domains/bi','/bi-security-login/logout?redirect=/va')` or `disableBISingleSignOn('C:/oracle/Middleware/Oracle_Home/user_projects/domains/bi')`

   The SSO configuration for Oracle Business Intelligence is updated.

6. Restart the Oracle Business Intelligence component processes to consume the changes.

   For example on UNIX, use `./start.sh`.

Enabling SSO Authentication Using Fusion Middleware Control

How you enable SSO authentication for Oracle Business Intelligence using the **Security** tab in Fusion Middleware Control.

See Using Oracle Fusion Middleware Control, and Starting and Stopping the Oracle Business Intelligence Components in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

1. Log in to 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. If required, enter the logoff URL 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.

6. Click **Apply**, then **Activate Changes**.
7. Restart the Oracle Business Intelligence components using Fusion Middleware Control.

Enabling the Online Catalog Manager to Connect

How you enable online Catalog Manager to point to a new URL when analytics becomes protected when using SSO.

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 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).

See Process 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. See SSL Configuration in Oracle Fusion Middleware in *Administering Oracle Fusion Middleware*.

This chapter contains the following sections:

- What is SSL?
- Enabling End-to-End SSL
- Enabling Oracle BI EE Internal SSL
- Disabling Internal SSL
- Exporting Trust and Identity for Clients
- Configuring SSL for Clients
- Checking Certificate Expiry
- Replacing the Certificates
- Update Certificates After Changing Listener Addresses
- Adding New Servers
- Enabling SSL in a Configuration Template Configured System
- Manually Configuring SSL Cipher Suite
- Configuring SSL Connections to External Systems
- WebLogic Artifacts Reserved for Oracle BI EE Internal SSL Use

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.

See How SSL Works in *Administering Oracle Fusion Middleware*.

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. You must configure the following components to enable secure communication 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. See 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.

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.

Scaling Out an SSL-Enabled System

To scale out a system that has internal SSL enabled, see Adding New Computers in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*, where the necessary `ssl.sh bindchannelcerts` call is made.

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:

- Configuring a Standard Non-SSL Oracle BI EE System
- Configuring WebLogic SSL

Configuring a Standard Non-SSL Oracle BI EE System

This section explains how to configure a standard non-SSL Oracle Business Intelligence system.

- Install Oracle BI EE.
- 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`

Configuring WebLogic SSL

These steps configure WebLogic using the provided demo certificates. These are not secure.

Do not use these tasks in a production environment. Using the demo certificates can help you understand how to configure your environment 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 *demoCA* is mentioned in task steps replace *demoCA* with your real CA certificate.

This section contains the following topics:

- Starting Only the Administration Server
- Configuring HTTPS Ports
- Configuring Internal WebLogic Server LDAP to Use LDAPs
- Configuring Internal WebLogic Server LDAP Trust Store
- Disabling HTTP
- Restarting
- Configuring OWSM to Use t3s
- Restarting System

Starting Only the Administration 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 Administration server with:

   ```
   <DomainHome>/bitools/bin/start.sh -i Adminserver
   ```

Configuring HTTPS Ports

Follow these steps to configure the HTTPs ports.

1. Log in to WebLogic Admin console.
2. Click **Lock and Edit**.
3. Select **environment**, **servers**.
4. For each server on the main **Configuration** tab, select **SSL Listen Port Enabled**.
5. Click **Save**.
6. Click **Activate Changes**.
7. If you are using WebLogic demo certificates, go to URL `https://<host>:<AdminServerSSLPort>` and set up a single browser certificate exception.

   The URL `https://<host>:<AdminServerSSLPort>` is the base URL, without Enterprise Manager or the WebLogic Administration 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 Enterprise Manager or the WebLogic Administration console paths, you must setup multiple certificate exceptions.
8. 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. You can ignore the error.

9. Test the secure WebLogic console URL using a URL similar to the following:

   `https://<Host>:<AdminServerSSLPort>/console`

10. Test the secure Fusion Middleware Control URL using a URL similar to the following:

    `https://<Host>:<AdminServerSSLPort>/em`

    Test the HTTPS URL while logged in to Fusion Middleware Control using HTTP.

    Do not disable HTTPS.

11. In WebLogic Administration Console, click **Lock and Edit** to begin Enabling secure replication.
12. Select **Environment**, select **Clusters**, and then select **bi_cluster**.
13. Select **Configuration**, and select the **Replication** tab.
14. Select **secure replication enabled**.

    If you do not select **secure replication enabled**, the managed servers fail to startup and remain in Administration mode preventing the start scripts from running.

15. Click **Save**.
16. Click **Activate Changes**.

Configuring Internal WebLogic Server LDAP to Use LDAPs

If you have configured an external Identity Store, you can skip performing this step. Perform this task if using WebLogic Server LDAP, and the `virtualize` property is not set to *true*.

You can configure an external identity store to use a secure connection. To use an external identity store, you must change the URL in the internal LDAP ID store.

1. Login to Fusion Middleware Control using a URL similar to the following:

   `https://<Host>/<SecureAdminPort>/em`

2. Click **WebLogic Domain**, click **Security**, and click **Security Provider Configuration**.
3. Expand the **Identity Store Provider** segment.
4. Click **Configure**, and click the plus symbol (+) to add a new property.
5. Add a `ldap.url` property using the following format for the *administration server* address rather than the *bi_server1* address:

   `ldaps://<host>:<adminServer HTTPS port>`, for example, `ldaps://myexample_machine.com:9501`.

6. In the Property editor, click **OK**.
7. On the Identity Store Provider page, click **OK**.

8. Open the `jps-config.xml` file located in `<DomainHome>/config/fmwconfig/jps-config.xml`.
9. In the file look for the line, `<property name="ldap.url" value="ldaps://<Host>:<AdminServerSecurePort>"/>` to confirm that the configuration change.

Configuring Internal WebLogic Server LDAP Trust Store

You must now provide a trust keystore.

See One-way SSL in a Multi-LDAP Scenario in *Securing Applications with Oracle Platform Security Services*

> **Note:**
>
> This section only applies when using WebLogic Server LDAP and when `virtualize=true` is set, as you are explicitly pointing the Administration Server.

1. In a terminal window set the *ORACLE_HOME* and *WL_HOME* environment variables .

   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.

   For example:

   ```
   oracle_common/bin/libovdconfig.sh -host myhost -port 9500 -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.
```

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 Administration Server.

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
   ```

Disabling HTTP

After securing the system to use HTTPS, you must also disable HTTP to fully secure the environment.

1. Login to WebLogic Administration 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**.

Restarting

Now you must restart Oracle Business Intelligence.

You cannot login through Analytics since Oracle Web Service Manager (OWSM) is using the disabled HTTP port.

Only the HTTPs one should work.

HTTP should quickly display an error similar to `Unable to connect error`. Do not to mix the protocols and ports. The browser can hang when attempting to connect to a running port with the wrong protocol.

1. Stop the Administration Server from within WebLogic Administration console using the `start.sh` script located in `<DomainHome>/bitools/bin/start.sh` script.
2. Confirm that HTTP is disabled by logging into both the HTTP and HTTPs WebLogic console URLs.

Configuring OWSM to Use t3s

You must now change the Oracle Web Services Manager (OWSM) configuration to use the HTTPs port.

The HTTP(s) OWSM link is not used when using a local OWSM.

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**.
5. Select **Yes** .
6. Confirm by accessing the policy via the validator:

   ```
   https://<host>:<ManagedServerSSLPort>/wsm-pm/validator
   ```

Restarting System

You must stop and restart all servers then test Analytics login with HTTPs.

1. Stop all servers using the `<DomainHome>/bitools/bin/stop.sh script`.
2. Use the `<DomainHome>/bitools/bin/start.sh` script to start everything.
3. Confirm your ability to log in to Analytics using a URL similar to the following:

   ```
   https://<Host>:<SecureManagedServerPort>/analytics
   ```

   The WebLogic tier using HTTPs only for its outward facing ports and all WebLogic infrastructure. The internal BI channel and BI system components use HTTP.

Enabling Oracle BI EE Internal SSL

Follow these steps to enable SSL on internal communication links.

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. Only use this procedure if you have configured security using the configuration assistant.

If you used the Configuration Template for SSL, see Enabling SSL in a Configuration Template Configured System.

You can configure the following advance options:

- Enable server checking of client certificates.
- Specify cipher suite to use.

  See Manually Configuring SSL Cipher Suite.

Post conditions:

1. Stop the system using the following command:

   ```
   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
   ```

4. Restart the domain and BI component processes using the following command:

   ```
   ORACLE_HOME/user_projects/domains/bi/bitools/bin/start.sh
   ```

5. Confirm that WebLogic certificates and the corresponding trust have been correctly configured using the following:

   ```
   ORACLE_HOME/user_projects/domains/bi/bitools/bin/ssl.sh report
   ```

6. Confirm you can login to Oracle BI EE using your environment variables in:

   ```
   https://<host>:<SecureManagedServerPort>/analytics
   ```

> **Note:**
>
> You must perform this login to confirm that the HTTPS listener is enabled on each server before you enable end-to-end SSL. Any communication between internal components is encrypted, and 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:
  - Enable an HTTPS listener on internal channels.
  - The external port configuration is unaltered.
  - 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.

Disabling Internal SSL

Use this task to disable Oracle BI EE SSL on internal communication links.

You must run commands from the master host. To use this option, you configured Oracle Business Intelligence using the configuration assistant, the WebLogic managed servers have been created, and scaling out is complete.

1. Stop the system using:

   ```
   <DomainHome>/bitools/bin/stop.sh
   ```

2. Run the following command to disable SSL on WebLogic internal channels and internal components:

   ```
   <DomainHome>/bitools/bin/ssl.sh internalssl false
   ```

3. Restart the domain using:

   ```
   <DomainHome>/bitools/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.

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.

  See Configuring WebLogic SSL.
- You can perform this task with the system stopped or running.

Use the following command to export client identity and trust to *mydir*:

```
./ssl.sh exportclientcerts mydir
```

Certificates and the zip file are generated.

Post conditions:

- *Mydir* contains *clientcerts.zip* file.
- *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.

Configuring SSL for Clients

Use these topics to configure SSL for clients.

You must configure clients accessing the BIEE components to use BIEE certificates. 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:

- Exporting Client Certificates
- Using SASchInvoke when BI Scheduler is SSL-Enabled
- Configuring Oracle BI Job Manager
- Connecting the Online Catalog Manager to Oracle BI Presentation Services
- Configuring the Oracle BI Administration Tool to Communicate Over SSL
- Configuring an ODBC DSN for Remote Client Access
- Configuring Oracle BI Publisher to Communicate Over SSL
- Configuring SSL when Using Multiple Authenticators

Exporting Client Certificates

Use these steps to create the passphrase for use when exporting client certificates.

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.

1. Run the following command:

   ```
   <DomainHome>/bitools/bin/ssl.sh exportclientcerts <exportDir>
   ```

2. Type the new passphrase at the prompt.

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.

The `SASchInvoke` tool is a command line job invocation tool which allows you to run pre-existing Oracle BI Scheduler jobs. For information about the Oracle BI Scheduler, see Introducing Oracle BI Scheduler.

1. Create a new text file containing on a single line the passphrase you used when running the `./ssl.sh exportclientcerts` command.

   Ensure this file has appropriately restrictive file permissions to protect it. Typically it should only be readable by the owner. See Exporting Client Certificates.

2. Locate the `SASchInvoke` tool.

- Windows: `<Domain_Home>/bitools/bin/saschinvoke.cmd`
- Unix: `<Domain_Home>/bitools/bin/saschinvoke.sh`

3. Use the following syntax to run the `SASchInvoke` command:

```
SASchInvoke -u <Admin Name>  (-j <job id> | -i <iBot path>)
    ([-m <machine name>[:<port>]] | -p <primaryCCS>[:<port>] -s
<secondaryCCS>[:<port>])
    ([[(-r <replace parameter filename> | -a <append parameter filename>)]  | [-x
<re-run instance id>])
    [-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:
-a  File containing additional parameters.
-c  File containing SSL certificate. SSL certificate filename = clientcert.pem
-d  Certificate authority directory.
-e  SSL certificate verification depth.
-f  Certificate authority file.
-h  SSL cipher list
-i  Agent path
-j  Job id
-k  SSL certificate private key filename. SSL certificate private key filename =
clientkey.pem
-l  Use SSL
-m  Machine name:port of scheduler.  Provides direct access to scheduler.
-p  Primary cluster controller name:port.  Provides access to clustered
scheduler.
-q  Location of the passphrase file created in step 1 containing the SSL
passphrase protecting SSL private key (see -k).
-r  File containing replacement parameters.
-s  Secondary cluster controller name:port.  Provides access to clustered
scheduler.
-t  Distinguished names of trusted peers.
-u  Username
-v  Verify peer
-w  SSL passphrase protecting SSL private key (see -k).
-x  Rerun instance id.
-y  Interactively prompt for SSL passphrase protecting SSL private key (see -k).
```

4. The command prompts you to enter the administrator password. Once entered, the `SASchInvoke` tool will get the BI Scheduler to run the specified job.

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. See Exporting Client Certificates.

1. From the **File** menu, select **Oracle BI Job Manager**, then select **Open Scheduler Connection**.
2. In the Secure Socket Layer section, 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*.
5. To provide a secure link you should select the verify server certificate. Without verification the connection works, but a person in the middle attack which impersonates the server is not detectable.
   a. Select the **Verify Server Certificate** 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*.

Connecting the Online Catalog Manager to Oracle BI Presentation Services

For the online Catalog Manager to connect to Oracle BI Presentation Services, you might need to import the SSL server certificate or CA certificate.

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.

The default password for the Java trust store is *changeit*.

1. Navigate to Java's default trust store, named `cacerts`, located at *`ORACLE_HOME/JAVA_HOME`*`/jre/lib/security`.
2. Copy the certificate exported from the web server to the same location as Java's default trust store.
3. Execute the following command to import the certificate to the default trust store:

   ```
   keytool -importcert -trustcacerts -alias bicert -file $WebServerCertFilename -
   keystore cacerts -storetype JKS
   ```

   When the web server certificate file *$WebserverCertFilename* is imported into Java's default trust store, under an alias of `bicert`.

   For example, if using the Oracle WebLogic Server default demonstration certificate, use the full path to the certificate located in *`ORACLE_HOME/`*`wlserver/server/lib/CertGenCA.der`.
4. Restart Catalog Manager using the secure HTTPS URL.

Configuring the Oracle BI Administration Tool to Communicate Over SSL

To successfully connect to an Oracle BI Server configured to use SSL, you must also configure the Oracle BI Administration Tool to communicate over SSL.

The data source name (DSN) for the BI Server data source is required.

1. Determine the BI Server data source DSN in use by logging into the Presentation Services Administration page as an administrative user.
2. Locate the Oracle BI Server **Data Source** field.

   The DSN is listed in the following format, `coreapplication_OH<DSNnumber>`.
3. In the Administration Tool, select **File**, then **Open**, then **Online**.
4. Select the DSN from the list.
5. Enter the repository user name and password.

   The Administration Tool is now connected to the BI Server using SSL.

Configuring an ODBC DSN for Remote Client Access

You can create an ODBC DSN for the BI Server to enable remote client access.

To enable SSL communication for an ODBC DSN, see Integrating Other Clients with Oracle Business Intelligence in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Configuring Oracle BI Publisher to Communicate Over SSL

You can configure Oracle BI Publisher to communicate securely over the internet using SSL.

See Configuring BI Publisher for Secure Socket Layer (SSL) Communication in the *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. See Configuring Integration with Oracle BI Presentation Services in *Administrator's Guide for Oracle Business Intelligence Publisher*.

Checking Certificate Expiry

This task provides a warning if certificates are expired or about to expire.

You must run commands from the master host with the system running or stopped.

- 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.

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 life spans. Once they expire connections using those certificates do not 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.

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.

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.

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.

Adding New Servers

Follow these steps to achieve 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.

1. For each new server run the following:

   ```
   ./ssl.sh channel <new_bi_server> <port>
   ```

2. You can run the following more than once:

   ```
   ./ssl.sh internalssl true
   ```

   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.

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.

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. Do one of the following:
   - Run the command:

     ```
     ./ssl.sh internalssl true
     ```

   - Run the `./ssl.sh internalssl true` repeatedly, and run the <<*other commands*>> 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 runs with SSL and all the WebLogic managed servers using the internal SSL.

Enabling SSL Without Internal Business Intelligence SSL

To support SSL on the external ports without using SSL internally you must decouple the internal communications by creating internal channels. Use the steps in this task to create the internal channels configured to use HTTP.

Oracle Business Intelligence has system components that need to communicate with Java components running inside WebLogic managed servers, for example at login an Oracle BI Server process calls the BI security service. In a default configuration template configured system, the communication links use the external WebLogic ports. You can configure Oracle WebLogic Server to use HTTPS for its external ports.

If you configure WebLogic to use HTTPS for external ports, the internal components attempt to connect to the HTTPS port without the necessary trust setup. To avoid this problem, you need to configure private channels. These private channels are independent of the external WebLogic ports, with their own ports and their own protocol configuration.

Assumptions:

- Run commands from the master host.
- Perform this task as an offline operation.
- Do one of the following:
  - Option A, run the following commands:

    ```
    <domain_home>/bitools/bin/ssl.sh regenerate <days>
    ```

    Regenerate the certificates to allow the subsequent channel commands to work. The certificates aren't used unless you subsequently change your mind and enable internal SSL.

    ```
    <domain_home>/bitools/bin/ssl.sh targetapps bi_cluster
    ```

    For each new server run the following using an unused port:

    ```
    ./ssl.sh channel <new_bi_server> <port>
    ```

    ```
    ./ssl.sh internalssl false
    ```

  - Option B, repeat running the following command using the `internalssl` error checking to prompt you to resolve issues.

    ```
    ./ssl.sh internalssl false
    ```

    Run the other commands as indicated in the `internalssl` command's error messages.

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 coexist with a default SSL configuration.

See Starting and Stopping Oracle Business Intelligence System Components in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

1. Configure SSL.
2. Select the desired Java Cipher Suite.
3. Create an Open SSL Cipher Suite Name that matches the cipher suite.

   For example, the 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
   ```

   Add following child 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
   ```

Configuring SSL Connections to External Systems

Use these links to see topics about configuring SSL connections to external systems:

- Configuring SSL for the SMTP Server Using Fusion Middleware Control
- Configuring SSL when Using Multiple Authenticators

Configuring SSL for the SMTP Server Using Fusion Middleware Control

You must obtain the SMTP server certificate to complete this task.

1. Login to 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**.

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.

In the following procedure you set the values for your 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*

The createKeystore command creates a OVD Keystore password. You have to type a value for the OVD Keystore password.

See Starting and Stopping Components in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Before completing this task, you must configure the custom property, called virtualize, and set the property's value to true, see Configuring Identity Store Virtualization Using Fusion Middleware Control.

1. Set up the keystore by running libovdconfig.sh on UNIX, or libovdconfig.bat on Windows, using the -createKeystore option.
2. On UNIX, open a shell prompt and change the directory to <*OracleHome*>/oracle_common/bin.
3. Type the command to look similar to the following:

   ```
   libovdconfig.bat -createKeystore -host <hostname> -port <Admin_Server_Port> -
   domainPath <OracleHome>/user_projects/domains/bi -userName <BI Admin User>
   ```

4. At the prompt, type the Oracle Business Intelligence administrator user name and password.
5. Type a password for the OVD Keystore password to secure a Keystore file.
6. Export the root certificate from the LDAP directory.
7. Use the following the keytool command to import the root certificate to the libOVD keystore:

   ```
   <OracleHome>/jdk/jre/bin/keytool -import -keystore <OracleHome>/user_projects/
   domains/bi/config/fmwconfig/ovd/default/adapters.jks -storepass <KeyStore
   password> -alias <alias of your choice> -file <Certificate filename>
   ```

8. Restart WebLogic Server and Oracle Business Intelligence processes.

You should see two new credentials in the Credential Store and a new Keystore file, called adapters.jks in the following location, <*OracleHome*>/user_projects/domains/bi/config/fmwconfig/ovd/default.

WebLogic Artifacts Reserved for Oracle BI EE Internal SSL Use

The following WebLogic artifacts are reserved for Oracle BI EE internal use:

- Virtual hosts:

  bi_internal_virtualhost1
- Channels (on each managed server):

  bi_internal_channel1

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.

- Lightweight SSO and Legacy Authentication Options
- 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.

Lightweight SSO and Legacy Authentication Options

If you are using legacy authentication options such as session variables in initialization blocks to get the user ID and group, you must disable lightweight SSO. Legacy authentication cannot use SSO through Oracle WebLogic.

You might need to revert to the previous login page, if you are using the `NQUser` and `NQPassword` query parameters to log in to SSO. `NQUser` and `NQPassword` login parameters were used as optional parameters for the Oracle BI Presentation Services Go URL. If you must continue to use the `NQUser` and `NQPassword` login parameters, you must disable lightweight SSO.

Lightweight SSO is implemented by default in Oracle BI EE release 12.2.1.3.0. Users are not prompted to login when moving between Classic Oracle BI EE and Visual Analyzer, or moving between the Classic Home page to the New Home Page.

To continue to use the `NQUser` and `NQPassword` login parameters, disable lightweight SSO using the WLST `disableSingleSignOn` command. See Enabling and Disabling SSO Authentication Using WLST Commands in *Security Guide for Oracle Business Intelligence Enterprise Edition*. Users are redirected to the Oracle BI security login when lightweight SSO is disabled.

You can implement other SSO options in your environment.

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.

See Introduction to Security in Oracle Business Intelligence and 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:

- Setting Up LDAP Authentication Using Initialization Blocks
- Setting Up External Table Authentication
- About Oracle BI Delivers and External Initialization Block Authentication
- Order of Authentication
- Authenticating by Using a Custom Authenticator Plug-In
- Managing Session Variables
- Managing Server Sessions

Setting Up LDAP Authentication Using Initialization Blocks

You can set up the Oracle 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. See Using Variables in the Oracle BI Repository in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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.
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.

4. If applicable, delete users from the repository file.
5. Associate the USER system variable with the LDAP initialization block.

> **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.

Setting Up an LDAP Server

For instances of Oracle Business Intelligence that use Active Directory Service Interfaces (ADSI) as the authentication method, use the following options 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.

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.

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 are 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.

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 **Session** and **Initialization Blocks** 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** 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**.

Setting the Logging Level

Use the system variable LOGLEVEL to set the logging level for users who are authenticated by an LDAP server.

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. See Using Variables in the Oracle BI Repository in *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. See Setting Up LDAP Authentication Using Initialization Blocks.

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 are assigned to variables. The order of the variables and the order of the columns determine 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.

About Oracle BI Delivers and External Initialization Block Authentication

Oracle BI Scheduler Server runs Oracle BI 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, you must perform all database authentication in only one connection pool. The connection pool is only selectable in an initialization block for the *USER* system session variable. The initialization block is usually called the Authentication initialization block. When impersonation is used, the Authentication initialization block is skipped. All other initialization blocks must use connection pools that do not use database authentication.

> **Important:**
>
> An authentication initialization block is the only initialization block where it is acceptable to use a connection pool with *: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.

See the Oracle BI Delivers examples in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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 *USER* session variable, the server 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 is used.

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. You can use the `authenticator` with the BI Server to perform authentication and other tasks at run time. The authentication module is a BI Server module with a cache layer that uses the authenticator and performs related tasks at run time.

You can find sample custom authenticator code in the Oracle 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 the 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 required *USER* variable and other variables with the initialization blocks.

When a user logs in, if the authentication is successful, a list of variables is populated 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. You can continue to use a custom authenticators.

1. In the Administration Tool, select **Manage**, then **Identity**. Select **Custom Authenticators** from the navigation tree. Select from the following options:

- Right-click in the right pane and select **New Custom Authenticator** to create a new custom authenticator.
- Double-click the name to edit a custom authenticator.

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, pre-allocated 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**.

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. See Using Variables in the Oracle BI Repository in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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**.

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.

The tables describe the columns 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.

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.

See Using Variables in the Oracle BI Repository in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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.
3. To refresh the view, click **Refresh**.
4. To close Session Manager, click **Close**.

Follow these steps 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**.

Follow these steps 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**.

Alternative Authorization Options

For backward capability, this release supports the ability to set application role membership for users using initialization blocks when authentication is performed by initialization blocks.

> **Note:**
>
> You cannot set application role membership using initialization blocks when authentication is performed by Oracle Platform Security Services.

This section contains the following topics:

- Changes Affecting Security in Presentation Services
- Setting Up Authorization Using Initialization Blocks

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.
- 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.

Setting Up Authorization Using Initialization Blocks

Use these steps to set application role membership for users using initialization blocks.

- Initialization blocks to set ROLES or GROUP session variables 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 ROLES or GROUP, enabling the BI Server to make the values of both variables the same.
- When using an initialization block to set ROLES or GROUP session variables, set the values of the variables to match by name against one or more application roles configured using Fusion Middleware Control, for example, BIConsumer. Users are assigned these application roles and associated permissions during authentication.
- See 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.

See Using Variables in the Oracle BI Repository in the *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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** .
4. Right-click in the right pane and select **New Initialization Block**.
5. In Session Variable - Initialization, enter *Authorization* in the **Name** field.
6. Click **Edit Data Source**.
7. Select Database from the **Data Source Type** list.
8. Enter the SQL statement to returns a list of groups, or a single group if row-wise initialization is not used.
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** check box.
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 appendix contains the following sections:

- About Securing Oracle Business Intelligence
- About the Security Framework
- Key Security Elements
- Security Configuration Using the Sample Application
- Granting Permissions To Users Using Groups and Application Roles
- Common Security Tasks After Installation

> **Note:**
>
> Use the tasks in this section to manage privileges 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. See Managing Presentation Services Privileges.

About Securing Oracle Business Intelligence

You can divide securing Oracle Business Intelligence into two areas, system access security and data access security

- System access security controls the access to the components and features that make up Oracle Business Intelligence.

  System access security includes topics such as how to limit system access to authorized users, control software resources based on permission grants, and enable secure communication among components.
- Data access security controls access to business source data and metadata used by Oracle Business Intelligence.

  You can read about data access security in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

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. See Oracle WebLogic Server.

See Introduction to Oracle Platform Security Services in *Securing Applications with Oracle Platform Security Services*. See *Understanding Security for Oracle WebLogic Server* and *Administering Security for Oracle WebLogic Server* to learn about Oracle WebLogic Server domain and security realm.

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 Oracle Application Server Java Authentication and Authorization Service (JAAS) Provider. Oracle Platform Security Services enables the shared security framework to furnish uniform security and identity management across the enterprise.

See Introduction to Oracle Platform Security Services in *Securing Applications with Oracle Platform Security Services*.

Oracle WebLogic Server

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. See Oracle Business Intelligence Components in *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. See System Requirements and Certification.

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.

See Introduction to Oracle Platform Security Services in *Securing Applications with Oracle Platform Security Services*.

Oracle Business Intelligence uses these security platform elements as follows:

Application Policy
See Terminology.
An application stripe defines a subset of policies in the policy store. TheOracle Business Intelligence application stripe is named *obi*.

Application Role
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. See *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. See Managing Presentation Services Privileges Using Application Roles.

Authentication Provider
See About Authentication.

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.

Oracle BI EE 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:

- See 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.

- 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 Fusion Middleware Control.

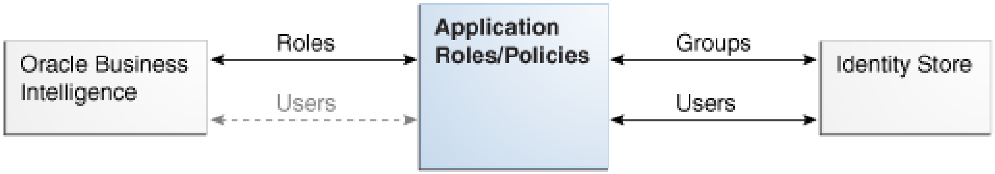
- Credential Store Provider

  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.

The table summarizes the security providers and their initial state after installation.

Security Provider Type	Purpose	Default Provider	Options
Authentication provider	Used to control authentication.	• DefaultAuthenticatior. 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. 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.

The diagram shows the relationship between Oracle Business Intelligence and the authentication and policy store providers.



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.

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.

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 such as BIServiceAdministrator or BIAdministrator.

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 is database-based or LDAP-based. The Oracle Business Intelligence default installation provides a database-based policy store.

Catalog privileges and permissions are not maintained in the policy store provider.

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 are used along with any new permission sets that were not available in 11*g*. You can change permission grants using Fusion Middleware Control.

> **Note:**
>
> You can view only permission set grants in Fusion Middleware Control. You must use WLST commands to change permission set grants.

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.

If you import the sample or starter application into your service instance the preconfigured permission sets are granted to the application roles included in the sample and starter applications. If you import the empty BAR file into your service instance, you must use WLST commands to assign permission sets to the application roles that you create. Application roles have groups as members, and permissions are inherited by users through their membership in 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, permission is granted by membership in the `BIServiceAdministrator` application role. The `BIServiceAdministrator` application policy contains the actual permission grant definitions. The `BIServiceAdministrator` application policy contains the permission set grant that includes the relevant permission. The Oracle Business Intelligence installation does not automatically create any (LDAP) groups. To convey this permission set to a user in your environment, create a suitable group such as a BIAdministrators group in the WebLogic LDAP or the Identity Store that you have configured Oracle Business Intelligence 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.

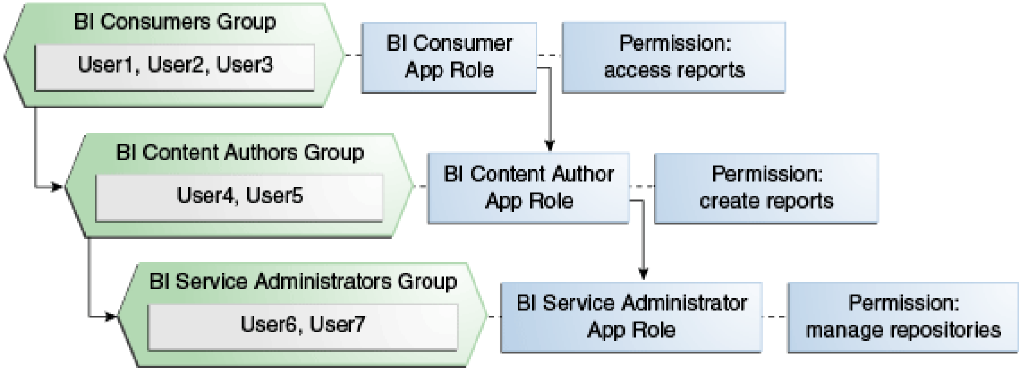
Users can also obtain permissions by inheriting group membership and application roles. For an example of how this is accomplished, see Permission Inheritance and Role Hierarchy.

Permission Inheritance and Role Hierarchy

InOracle 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.

The diagram shows the relationship between application roles and how permissions are granted to members.


BI Consumers Group
User1, User2, User3
BI Consumer App Role
Permission: access reports
BI Content Authors Group
User4, User5
BI Content Author App Role
Permission: create reports
BI Service Administrators Group
User6, User7
BI Service Administrator App Role
Permission: manage repositories

In the diagram, 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. 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:**
>
> Groups and group hierarchies do not provide access rights to application resources. Privileges are conveyed by the permission set 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.

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 lifecycle of using the product in one or more of the following environments:

  - Development
  - Test
  - Production

Common Security Tasks to Evaluate Oracle Business Intelligence

The table contains common security tasks performed to evaluate Oracle Business Intelligence and provides links for more information.

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.	Introduction to Security in Oracle Business Intelligence Security Configuration Using the Sample Application *Securing Applications with Oracle Platform Security Services*
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.	Creating a New User in the Embedded WebLogic LDAP Server *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.	Modifying Application Roles Using Fusion Middleware Control *Securing Applications with Oracle Platform Security Services*
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.	Creating and Deleting Application Roles Using Fusion Middleware Control *Securing Applications with Oracle Platform Security Services*

Common Security Tasks to Implement Oracle Business Intelligence

The table 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 Common Security Tasks to Evaluate 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.	Configuring Oracle Business Intelligence to Use Alternative Authentication Providers Legacy Security Administration Options
Create a new application role.	Create a new application role and make the role a grantee of an application policy.	Creating and Deleting Application Roles Using Fusion Middleware Control
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.	Modifying Application Roles Using Fusion Middleware Control

Task	Description	For Information
Decide whether to use SSL.	Decide whether to use SSL communication and devise a plan to implement.	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.	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.

This appendix 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

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.

This appendix contains the following topics:

- 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.
- 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.
- Resolving User Login Authentication Failures

  This section provides reasons and solutions for login authentication failure.

Authentication Concepts

This section describes authentication concepts and helps to resolve login issues.

This section contains the following topics:

- Authentication Defaults on Install
- Using Oracle WebLogic Server Administration Console and Fusion Middleware Control to Configure Oracle Business Intelligence
- WebLogic Domain and Log Locations

- WebLogic Server Administrator User Account
- Oracle Business Intelligence Login Overview

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 are set up, including a WebLogic Server administrator user account that can use the credentials entered during installation.

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.

See 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 user name 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 WebLogic Server Administrator User Account.

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.

These paths represent the default installation locations. If you specified different installation locations, you must modify your 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/
  ```

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 to enable adding WebLogic Server administrator accounts. The WebLogic Server Admin role is not an Oracle Business Intelligence application role.

Follow these steps to add or remove users to or from the global admin role using the Oracle WebLogic Server Administration Console.

See Using 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.
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, you could use a condition such as `User=myadminaccount` or `Group=Administrators`.
6. If you have made any changes, click **Save**.
7. In the Change Center, click **Activate Changes**.

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. See Configuring Oracle Business Intelligence to Use Alternative Authentication Providers.

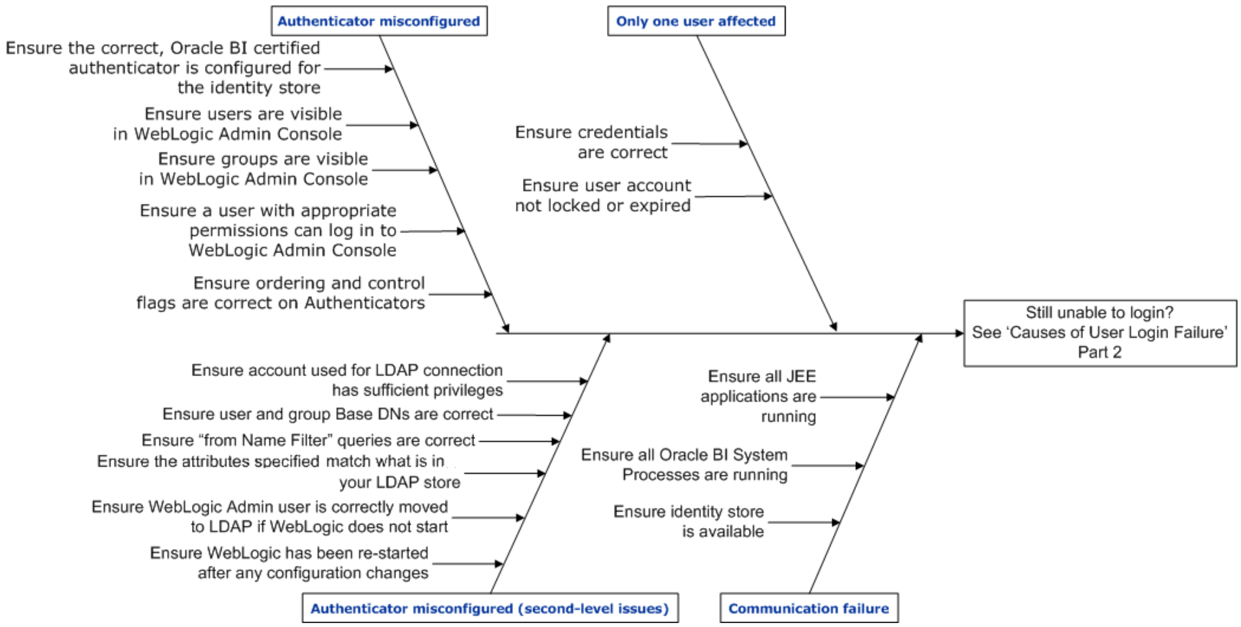
The login process flow begins with the user credentials entered in the login screen, being sent to Presentation Services, and then to the BI Server. The BI Server attempts to authenticate the user credentials by calling the BI Security web service, deployed in the WebLogic Managed Server, and protected 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.

Identifying Causes of User Login Authentication Failure

This section helps you to identify causes of authentication failure when logging in to Oracle Business Intelligence.

The diagrams below are cause and effect diagrams that you can use to identify possible causes of user login authentication failure. After identifying the likely cause of user login identification failure, see Resolving User Login Authentication Failures.

The following diagram shows: Causes of User Login Failure - Part 1

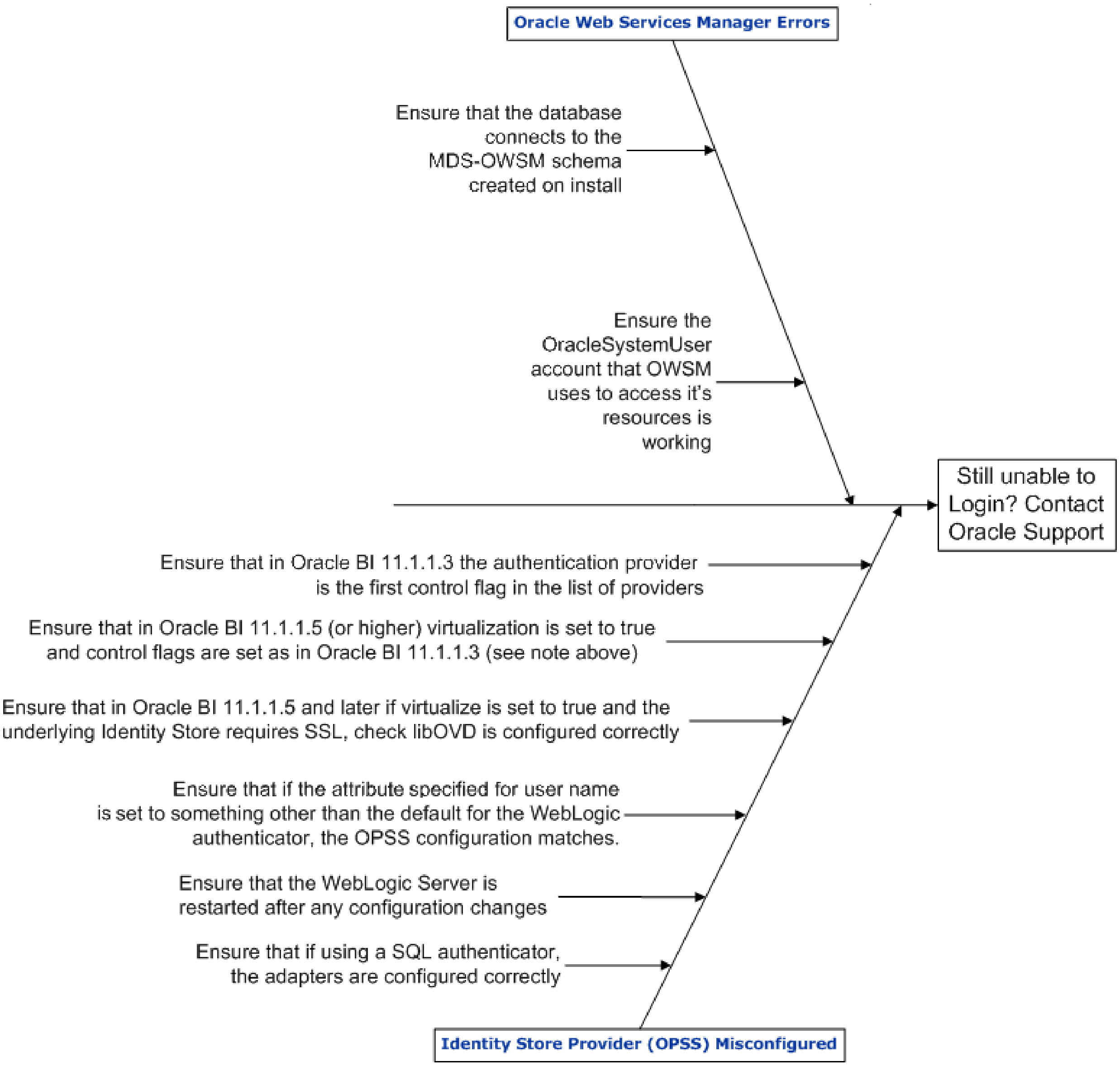

Authenticator misconfigured
Only one user affected
Ensure the correct, Oracle BI certified authenticator is configured for the identity store
Ensure users are visible in WebLogic Admin Console
Ensure groups are visible in WebLogic Admin Console
Ensure a user with appropriate permissions can log in to WebLogic Admin Console
Ensure ordering and control flags are correct on Authenticators
Ensure credentials are correct
Ensure user account not locked or expired
Still unable to login? See 'Causes of User Login Failure' Part 2
Ensure account used for LDAP connection has sufficient privileges
Ensure user and group Base DNs are correct
Ensure "from Name Filter" queries are correct
Ensure the attributes specified match what is in your LDAP store
Ensure WebLogic Admin user is correctly moved to LDAP if WebLogic does not start
Ensure WebLogic has been re-started after any configuration changes
Ensure all JEE applications are running
Ensure all Oracle BI System Processes are running
Ensure identity store is available
Authenticator misconfigured (second-level issues)
Communication failure

The description for the above diagram is as follows:

- Authenticator is incorrectly configured.
  - 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 is incorrectly configured (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.

The following diagram shows: Causes of User Login Failure — Part 2


Oracle Web Services Manager Errors
Ensure that the database connects to the MDS-OWSM schema created on install
Ensure the OracleSystemUser account that OWSM uses to access it's resources is working
Still unable to Login? Contact Oracle Support
Ensure that in Oracle BI 11.1.1.3 the authentication provider is the first control flag in the list of providers
Ensure that in Oracle BI 11.1.1.5 (or higher) virtualization is set to true and control flags are set as in Oracle BI 11.1.1.3 (see note above)
Ensure that in Oracle BI 11.1.1.5 and later if virtualize is set to true and the underlying Identity Store requires SSL, check libOVD is configured correctly
Ensure that if the attribute specified for user name is set to something other than the default for the WebLogic authenticator, the OPSS configuration matches.
Ensure that the WebLogic Server is restarted after any configuration changes
Ensure that if using a SQL authenticator, the adapters are configured correctly
Identity Store Provider (OPSS) Misconfigured

The above diagram helps you identify alternative causes of login failure if you cannot identify them using the first diagram. However, if you still cannot identify the causes of login failure after using the above diagram, contact Oracle Support at:

https://support.oracle.com

The description for the above diagram is as follows:

- Identity store provider (OPSS) is incorrectly configured.
  - Ensure that if using a SQL authenticator, the adapters are configured correctly.
  - Ensure that if the attribute specified for user name 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. See 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.

Resolving User Login Authentication Failures

This section explains user login authentication failures, describes how to resolve them, and contains the following topics:

- Single User Cannot Log in to Oracle Business Intelligence
- Users Cannot Log in to Oracle Business Intelligence Due to Misconfigured Authenticators
- Users Cannot Log in to Oracle Business Intelligence When Oracle Web Services Manager is not Working
- Users Cannot Log in to Oracle Business Intelligence - Is the External Identity Store Configured Correctly?
- Users Can Log in With Any or No Password
- Have Removed Default Authenticator and Cannot Start WebLogic Server

Single User Cannot Log in to Oracle Business Intelligence

This section contains the following topics:

- Is Login Failure the Result of User Error?
- Is User Account Locked?

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, see Is User Account Locked?.

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 WebLogic Server Administration Console Online Help*.

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 Using Alternative Authentication Providers.

- Have You Specified the Correct Authenticator for the Identity Store or LDAP Server?
- Is the Authenticator for the LDAP Server Configured Correctly?
- Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?

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.

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 Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?.

Are the Control Flags for Your Authenticators Set Correctly and Ordered Correctly?

Set the primary identity store as the first one in the list of authenticators. 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 Oracle Platform Security Services (OPSs) which only picks up the first identity store from the list of authenticators such as when looking up users, profile information, roles. Users can log in to Oracle WebLogic Server Administration Console when authentication succeeds, but the user cannot log 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, set the control flags to *SUFFICIENT* to enable trying each authenticator 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, set the `DefaultAuthenticator` to *SUFFICIENT* or *OPTIONAL*, if it is being retained. *SUFFICIENT* is the recommended setting.

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:

- Database Issues - OWSM Cannot Retrieve Policies

  Issues connecting to the MDS-OWSM schema created on install.

- OracleSystemUser Issues - OWSM Cannot Retrieve Policies

  Issues with the OracleSystemUser account that OWSM uses to access it's resources.

Database Issues - OWSM Cannot Retrieve Policies

Oracle Web Services Manager (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:9500,biserver:9704" due to invalid
configuration or inactive state.
```

You might 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?

Use these steps 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**.

Use these steps 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.

OracleSystemUser Issues - OWSM Cannot Retrieve Policies

By default, Oracle Web Services Manager (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:9500,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 is assigned the *OracleSystemRole* WebLogic Server global role. See Configuring Oracle Internet Directory LDAP Authentication as the Only Authenticator.

If 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, there is an entry similar to the following in the log:

```
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(LDAPAtnLog
inModuleImpl.java:261)
```

This error message occurs as a result of several different issues:

- You have removed the *DefaultAuthenticator* and did not create 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 was not found.
- The *OracleSystemUser* account was 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.

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 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 enabled, ensure that both it and the authentication provider refer 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 Configuring User and Group Name Attributes in the Identity Store. For example, the OID authentication provider defaults to expect that the value is the `UserName` attribute is *cn*, but many organizations actually use the attribute `uid` instead. In this instance, follow the instructions to set the `username.attr` and `user.login.attr` to `uid` in the identity store configuration in Fusion Middleware Control.

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, users can 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 attempts 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.

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 default domain home for your WebLogic BI Domain, unless you specified a different location during the installation, 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 is restored.

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:

- User Is Deleted from the Identity Store
- User Is Renamed in the Identity Store
- Group Associated with User Name Does Not Exist in the Identity Store

User Is Deleted from the Identity Store

Use this information to identify and resolve the issue.

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.

User Is Renamed in the Identity Store

Use this information to identify and resolve the issue.

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.

Group Associated with User Name Does Not Exist in the Identity Store

Use this information to identify and resolve the issue.

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 execution context ID (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(URServiceBean.java:
97)
      at

oracle.bi.security.service.SecurityServiceBean.getGrantedRolesForUser(SecurityService
Bean.java:270)
    at

oracle.bi.security.service.SecurityWebService$1GetGrantedRolesForUserAction.run(Secur
ityWebService.java:391)
    at

oracle.bi.security.service.SecurityWebService$1GetGrantedRolesForUserAction.run(Secur
ityWebService.java:381)
    at java.security.AccessController.doPrivileged(Native Method)
    at

oracle.bi.security.service.SecurityWebService.getGrantedRolesForUser(SecurityWebServi
ce.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 issue can occur if a group associated with a user name does not exist in the identity store.

Action

Verify that the LDAP groups assigned to the user exist, and are readable by the principal used by WebLogic to access the LDAP.

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:

- Application Role Was Deleted from the Policy Store
- Application Role Is Renamed in the Policy Store

Application Role Was Deleted from the Policy Store

Use this information to identify and resolve the issue.

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.

Application Role Is Renamed in the Policy Store

Use this information to identify and resolve the issue.

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.

Resolving SSL Communication Problems

Use this information to identify and resolve the issue.

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. See Disabling HTTP.

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.

See article IDs 1287479.1 and 1274953.1 on My Oracle Support at:

`https://support.oracle.com`

Resolving RSS Feed Authentication When Using SSO

When attempting to read an Oracle BI EE 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:

- Managing Security for Users of Oracle BI Presentation Services
- Using Oracle BI Presentation Services Administration Pages
- Determining a User's Privileges and Permissions in Oracle BI Presentation Services
- Providing Shared Dashboards for Users
- Controlling Access to Saved Customization Options in Dashboards
- Enabling Users to Act for Others

Managing Security for Users of Oracle BI Presentation Services

As a system administrator, you must configure a business intelligence system to ensure that all functionality including administrative functionality is secured by providing access only to authorized users that are allowed to perform appropriate operations. You must configure the system to secure all middle-tier communications.

This overview section contains the following topics:

- Security Settings in Oracle BI Presentation Services
- What Are the Security Goals in Oracle BI Presentation Services?
- How Are Permissions and Privileges Assigned to Users?

Security Settings in Oracle BI Presentation Services

Security settings that affect users of Presentation Services are made in the following Oracle Business Intelligence components:

- Use the Oracle BI Administration Tool 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.
- Oracle BI Presentation Services Administration enables setting privileges for users to access features and functions such as editing views and creating agents and prompts.
- Oracle BI Presentation Services enables assigning 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* for information on assigning permissions in Presentation Services.
- The Catalog Manager enables setting permissions for Oracle BI Presentation Catalog objects. See Configuring and Managing the Presentation Catalog in *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 Oracle BI Answers. The Security Administrator should enforce data security.

What Are the Security Goals in Oracle BI Presentation Services?

This topic provides guidelines for security with 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 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 *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 system wide 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 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. See Enabling SSO Authentication.

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 About 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.

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:

- Understanding the Administration Pages
- Managing Presentation Services Privileges
- Managing Sessions in Presentation Services

Understanding the Administration Pages

The main Oracle BI Presentation Services 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 User A and User B are both accessing and modifying the Manage Privileges page in Presentation Services Administration. If User A saves updates to privileges while User B is also editing them, then User B's changes are overwritten by those that User A saved.

Managing Presentation Services Privileges

This section contains the following topics about Presentation Services privileges:

- What Are Presentation Services Privileges?
- Default Presentation Services Privilege Assignments

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.

See Setting Presentation Services Privileges for Application Roles.

Default Presentation Services Privilege Assignments

You can manage privilege assignments for application roles that are granted by default.

These privileges apply to the Oracle Business Intelligence infrastructure. If your organization uses prebuilt applications, it is possible that some privileges are preconfigured. For more information, see the documentation for the specific application.

When building KPIs, KPI watchlists, KPI contribution wheels, or within Oracle Scorecard and Strategy Management, a combination of privileges are required to perform specific tasks. See 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 Oracle BI Presentation Services privileges:
>
> - 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.

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Are Dashboards? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Are Analyses? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and for Displaying and Processing Data in Views in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Is BI Composer? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Manually Changing Presentation Settings in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Access	Access to Delivers	Allows users to create and edit agents.	BI Content Author	Managing Objects in the Oracle BI Presentation Catalog in *User's Guide for Oracle Business Intelligence Enterprise Edition* About Controlling Access to Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to Briefing Books	Allows users to view and download briefing books.	BI Consumer	Managing Objects in the Oracle BI Presentation Catalog in *User's Guide for Oracle Business Intelligence Enterprise Edition* Adding Content to New or Existing Briefing Books in *User's Guide for Oracle Business Intelligence Enterprise Edition* Modifying the Table of Contents for PDF Versions of Briefing Books in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Getting Started with Oracle BI Mobile in *Oracle Business Intelligence Mobile Users Guide*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring Application Roles and Users in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* *Oracle Marketing Segmentation Guide* Configuring for Connections to the Marketing Content Server in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* *Oracle Marketing Segmentation Guide* Configuring for Connections to the Marketing Content Server in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* *Oracle Marketing Segmentation Guide* Configuring for Connections to the Marketing Content Server in *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 *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Installing and Deinstalling Oracle Business Client Tools in *Installing and Configuring Oracle Business Intelligence* What System Administration Tools Manage Oracle Business Intelligence? in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Integrating with Microsoft Office in *User's Guide for Oracle Business Intelligence Enterprise Edition* Manually Configuring for Export in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Access	Access to KPI Builder	Allows users to create KPIs.	BI Content Author	How Do I Create a KPI? in *User's Guide for Oracle Business Intelligence Enterprise Edition* See the table for KPIs in Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* See the table for Scorecards in Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Access to Oracle BI Enterprise Edition Actions
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 Processes in External Systems in *User's Guide for Oracle Business Intelligence Enterprise Edition* 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	You set the EnableSavingContentWithHTML element to *True* in instanceconfig.xml to enable this privilege. See EnableSavingContentWithHTML and Making Advanced Configuration Changes for Presentation Services.
Actions	Save Content With HTML Markup	Allows users to embed HTML code in content.	BI Service Administrator	You set the EnableSavingContentWithHTML element to *True* in instanceconfig.xml to enable this privilege. See EnableSavingContentWithHTML and Making Advanced Configuration Changes for Presentation Services. Managing Objects in the Oracle BI Presentation Catalog in *User's Guide for Oracle Business Intelligence Enterprise Edition* Who Can Create Actions? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Access to Oracle BI Enterprise Edition Actions
Admin: Catalog	Change Permissions	Allows users to modify permissions for catalog objects.	BI Content Author	Setting Permissions of Catalog Objects in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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	NA
Admin: General	Change Log Configuration	This privilege enables you to modify the log levels using the UI.	BI Service Administrator	NA
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	Understanding the Two Catalog Modes in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Create Dashboard	Allows users to create and edit dashboards, including editing their properties.	BI Service Administrator	Building and Using Dashboards in *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	Setting the Logging Levels for Oracle BI Presentation Services in *System Administrator'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	Testing the Oracle BI Server Using Issue SQL in *Logical SQL Reference 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	Diagnostics and Performance Monitoring in *System Administrator'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 *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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	Monitoring Active Agent Sessions and Configuring and Managing Agents in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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	Managing Device Types for Agents in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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	Administering Maps in *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	Diagnosing and Resolving Issues in Oracle BI in *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 Presentation Services in error messages.	BI Consumer	Diagnosing and Resolving Issues in Orals BI in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: General	Manage Global Variables	Allows users to add, update, and delete global variables. Global variables are created during the process of creating analyses.	BI Service Administrator	What Are Global Variables? in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* *Oracle Marketing Segmentation Guide* Configuring for Connections to the Marketing Content Server in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* *Oracle Marketing Segmentation Guide* Configuring for Connections to the Marketing Content Server in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Admin: Security	Manage Catalog Accounts	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	Setting Permissions of Catalog Objects in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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	Setting Permissions of Catalog Objects in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Oracle WebLogic Server Administration Console in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Oracle WebLogic Server Administration Console in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Oracle WebLogic Server Administration Console in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Oracle WebLogic Server Administration Console in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition*
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 *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Modifying the Table of Contents for PDF Versions of Briefing Books in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Managing Objects in the Oracle BI Presentation Catalog in *User's Guide for Oracle Business Intelligence Enterprise Edition* Securing Catalog Objects for Tenants in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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	Using Online and Offline Repository Modes in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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	Controlling Presentation Object Visibility in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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 *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Integrating with Microsoft Office Using Oracle Business Intelligence Add-in for Microsoft Office in *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions of Catalog Objects in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Searching with Oracle Secure Enterprise Search in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Searching with Oracle Secure Enterprise Search in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Searching with Oracle Secure Endeca Server in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Managing Objects in the Oracle BI Presentation Catalog in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Controlling Access to Saved Customization Options in Dashboards
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Enabling the Ability to Create Links to Dashboard Pages in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Enabling the Ability to Create Links to Dashboard Pages in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Enabling the Ability to Export Dashboard Pages to Oracle BI Publisher in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Enabling the Ability to Export Dashboard Pages to Oracle BI Publisher in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Formatting	Save SystemWide Column Formats	Allows users to save system wide defaults when specifying formats for columns.	BI Service Administrator	Saving Formatting Defaults in *User's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Is the Oracle BI EE Home Page? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Home page in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* How Can I Search for Objects? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* How Can I Search for Objects? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* How Can I Search for Objects? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Opening and Using Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Making Advanced Configuration Changes for Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Are Favorites? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Making Advanced Configuration Changes for Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Acting for Other Users in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Preferences in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Are Devices and Delivery Profiles? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Preferences in *User's Guide for Oracle Business Intelligence Enterprise Edition* Providing Custom Links in Presentation Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Displaying and Processing Data in Views in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Prompts in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Examining the Logical SQL Statements for Analyses in *User's Guide for Oracle Business Intelligence Enterprise Edition* Logical SQL Reference in *User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Edit Column Formulas	Allows users to edit column formulas.	BI Content Author	What Is the Analysis Editor? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Examining the Logical SQL Statements for Analyses in *User's Guide for Oracle Business Intelligence Enterprise Edition* Logical SQL Reference in *User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Save Content with HTML Markup	Allows HTML markup in analyses and dashboards, and allows users to save mission and vision statements in Oracle Scorecard and Strategy Management.	BI Service Administrator	The Save Content with HTML Markup privilege requires setting the EnableSavingContentWithHTML element to *True* in instanceconfig.xml. See EnableSavingContentWithHTML and Making Advanced Configuration Changes for Presentation Services. Working with HTML Markup in *User's Guide for Oracle Business Intelligence Enterprise Edition* Save Content with HTML Markup Privilege
Answers	Enter XML and Logical SQL	Allows users to use the Advanced SQL tab.	BI Content Author	What Is the Analysis Editor? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Examining the Logical SQL Statements for Analyses in *User's Guide for Oracle Business Intelligence Enterprise Edition* Logical SQL Reference in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Privileges for Direct Requests in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Logical SQL Reference in *User's Guide for Oracle Business Intelligence Enterprise Edition*

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 SQL** 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Using a Saved Analysis as a Filter in *User's Guide for Oracle Business Intelligence Enterprise Edition* Creating and Editing the SQL Statements for a Column Filter in an Analysis in *User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Save Filters	Allows users to save filters.		Saving Filters as Inline or Named in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Add EVALUATE_PREDICATE Function	Allows users to add the `EVALUATE_PREDICATE` function to an in-line filter.	BI Content Author	Working with the EVALUATE_PREDICATE Function in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition*
Answers	Upload Images	This privilege enables you to upload custom images using the UI wherever an image is selected.	BI Content Author	NA
Delivers	Create Agents	Allows users to create agents.	BI Content Author	Managing Objects in the Oracle BI Presentation Catalog in *User's Guide for Oracle Business Intelligence Enterprise Edition* Creating Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Controlling Access to Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Controlling Access to Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Controlling Access to Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Controlling Access to Agents in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Agents in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Enabling Users to Act for Others

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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 *User's Guide for Oracle Business Intelligence Enterprise Edition*
Scorecard	Create/Edit Scorecards	Allows users to create and edit scorecards.	BI Content Author	How Do I Create a Scorecard? in *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding
Scorecard	Create/Edit Objectives	Allows users to create and edit objectives.	BI Content Author	Creating Objectives in *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Scorecard	Create/Edit Initiatives	Allows users to create and edit initiatives.	BI Content Author	Creating Initiatives in *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* 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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* 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 *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* 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 *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding
Scorecard	Create/Edit KPIs	Allows users to create and edit KPIs and KPI watchlists.	BI Content Author	What Are Key Performance Indicators (KPIs)? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Understanding Watchlists in *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding

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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Identifying Privileges for KPIs, KPI Watchlists, and Scorecarding Configuring for Write Back in Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Scorecard Privileges and Permissions in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring the Repository for Oracle Scorecard and Strategy Management in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* 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 *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*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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*
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 *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 for Apple iOS
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* How Can I Search for Objects? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Performing Searches in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Mobile for Apple iOS* Configuring for Searching with Oracle Secure Enterprise Search in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* AccessControlToken Structure in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* impersonate() Method in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* MetadataService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ReportEditingService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ConditionService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* Common Steps for Configuring Full-Text Search in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* 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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* SecurityService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Access SchedulerService Service	Allows users to access the SchedulerService web service.	BI Consumer, BI System	Introduction to Oracle Business Intelligence Web Services in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* SchedulerService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access Tenant Information	Internal only.	BI System	Multitenancy Section Parameters in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access ScorecardMetadataService Service	Allows users to access the ScorecardMetadataService web service.	BI Consumer, BI System	Introduction to Oracle Business Intelligence Web Services in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ScorecardMetadataService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* ScorecardAssessmentService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* HtmlViewService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* iBotService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access XmlGenerationService Service	Allows users to access the XmlGenerationService web service.	BI Consumer, BI System	Introduction to Oracle Business Intelligence Web Services in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* XMLQueryExecutionOptions Structure in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
SOAP	Access JobManagementService Service	Allows users to access the JobManagementService web service.	BI Consumer, BI System	Introduction to Oracle Business Intelligence Web Services in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* JobManagementService Service in *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 *Integrator's Guide for Oracle Business Intelligence Enterprise Edition* KPIAssessmentService Service in *Integrator's Guide for Oracle Business Intelligence Enterprise Edition*
SOAP	Access UserPersonalizationService Service	The Oracle BI User Personalization web service is an application programming interface (API) that implements various APIs to manage user specific favorites and recent items.	BI Service Administrator	Introduction to Oracle Business Intelligence Web Services in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Setting Permissions for Presentation Layer Objects in *Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition* Providing Access to Metadata Dictionary Information in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit AnalyzerView	Allows users to access the Analyzer view.	BI Service Administrator	
Views	Add/Edit Canvas View	Allows users to create and edit canvas views.	BI Content Author	What Types of Views are Available in *User's Guide for Oracle Business Intelligence Enterprise Edition*.
Views	Add/Edit Column SelectorView	Allows users to create and edit column selector views.	BI Content Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Compound LayoutView	Allows users to create and edit compound layout views.	BI Content Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit FunnelView	Allows users to create and edit funnel graph views.	BI Content Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit FiltersView	Allows users to create and edit filter views.	BI Content Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit Performance TileView	Allows users to create and edit performance tile views.	BI Content Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Heat Matrix View	Allows users to create and edit heat matrix views.	BI Content Author	Editing Heat Matrix Views in *User's Guide for Oracle Business Intelligence Enterprise Edition*.
Views	Add/Edit Static TextView	Allows users to create and edit static text views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit NarrativeView	Allows users to create and edit narrative views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

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 *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 *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Generic Plugin View View	Allows users to create and edit generic plugin view views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Report Prompt View	Allows users to create and edit prompt views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Selection StepsView	Allows users to create and edit selection steps views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* What Types of Logical SQL Views Are Available? in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
Views	Add/Edit TableView	Allows users to create and edit table views.	BI Author	Adding Views for Display in Dashboards in *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 *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit Create Target ListView	Allows users to create and edit target list views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit TrellisView	Allows users to create and edit trellis views.	BI Author	Adding Views for Display in Dashboards in *User'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 *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*
Views	Add/Edit TreemapView	Allows users to create and edit treemap views.	BI Author	Adding Views for Display in Dashboards in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring and Managing Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Component	Privilege	Description	Default Role Granted	References or Reference Links for Additional Information
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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Handling Errors for Write Back in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Write Back in Analyses and Dashboards in *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 *User's Guide for Oracle Business Intelligence Enterprise Edition* About Handling Errors for Write Back in *User's Guide for Oracle Business Intelligence Enterprise Edition* Configuring for Write Back in Analyses and Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*

Access to Oracle BI Enterprise Edition Actions

You must set the Action privileges that 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

  The Create Navigate Actions privilege indicates whether the user can create a Navigate action type. Users who are denied this privilege do not have the user interface components that allow the creation of Navigate Actions. Users without the Create Navigate Actions privilege can add saved actions to analyses and dashboards, and execute an action from an analysis or dashboard that contains an action.

- Create Invoke Actions

  The Create Invoke Actions privilege indicates whether the user can create an Invoke action type. The Invoke Actions options include Invoke a Web Service, and Invoke an HTTP Request. 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

  The Save Actions Containing Embedded HTML privilege indicates whether users can embed HTML code in customized web service action results. You should use extreme care in assigning the Save Actions Containing Embedded HTML privilege, because users with this privilege can pose a security risk allowin users to run HTML code.

Access to Oracle BI for Microsoft Office Privilege

If your users have the Access to Oracle BI for Microsoft Office privilege, they can interact with Microsoft Office from Oracle BI EE.

When a user has the Access to Oracle BI for Microsoft Office privilege, the user can download desktop tools from 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. See Integration of Oracle BI EE with Microsoft Office and the **Copy** option in *User's Guide for Oracle Business Intelligence Enterprise Edition*.

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. 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. See EnableSavingContentWithHTML.

Users with this privilege can also save mission and vision statements in Oracle Scorecard and Strategy Management.

EnableSavingContentWithHTML

The EnableSavingContentWithHTML element along with the Save Content With HTML Markup and Save Actions Containing Embedded HTML privileges determine whether the **Contains HTML Markup** option is available in properties dialogs when editing analyses.

In Oracle Business Intelligence releases earlier than 12.2.1.3.0, various properties dialogs included an active **Contains HTML Markup** option. In Oracle Business Intelligence 12.2.1.3.0, the Contains HTML Markup functionality is disabled by default to reduce exposure to security vulnerabilities.

As the BI Service Administrator, you can use the EnableSavingContentWithHTML element to enable all HTML editing and you can grant the related privileges to users. You set the EnableSavingContentWithHTML element to *true* in the instanceconfig.xml file, and you grant users the Save Content With HTML Markup and Save Actions Containing Embedded HTML privileges in the Manage Privileges page to enable the **Contains HTML Markup** option. See Default Presentation Services Privileges Assignments and Making Advanced Configuration Changes for Presentation Services.

For the location of the instanceconfig.xml file, see Configuration Files.

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. The tables below 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:

See Scorecard Documents, Strategy pane, and Initiatives pane in *User's Guide for Oracle Business Intelligence Enterprise Edition*.

- 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:

  - See 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

The table below lists the combination of privileges that are 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 • See Edit_scorecard_set1 • See Edit_KPI_with_KPI_Builder_set4
Action link	**Create**, **edit**, or**delete** from within the KPI editor	• Actions - Create Navigate Actions • See 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 • See Edit_scorecard_set1
Business owner	**Modify** within the Scorecard editor using the KPI editor tab	• Admin: Security - User Population - Can List Users • See 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	• See Edit_scorecard_set1 • See 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.	• See 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.

Task Object	Task	Privileges Required to Perform the Task
KPI dimensioned target value (target setting)	**Edit** within the KPI watchlist on a dashboard	• Scorecard - Write Back to Database for KPI • See View_KPI_watchlist_on_dashboard_set3
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 • See View_or_edit_scorecard_set2
Related document	**Add**, **edit**, or**delete** a related document from within the KPI editor	• See Edit_KPI_with_KPI_Builder_set4
Related document	**Add**, **edit**, or**delete** a related document within the Scorecard editor using the KPI editor tab	• See Edit_scorecard_set1 • See Edit_KPI_with_KPI_Builder_set4

The table below lists the combination of privileges that are 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 • See 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 • See View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Action link	**Invoke** from a KPI watchlist on a dashboard	• See 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	• See 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 • See View_KPI_watchlist_on_dashboard_set3 Note that you must enable pop-ups in your browser.

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 • See 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 • See View_KPI_watchlist_on_dashboard_set3
Annotation	**Add** from within the standalone KPI watchlist editor	• Scorecard - Add Annotations • See View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
Annotation	**View** from a KPI watchlist on a dashboard	• See View_KPI_watchlist_on_dashboard_set3
Annotation	**View** from within the standalone KPI watchlist editor	• See 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 • See 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 • See 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 • See View_KPI_watchlist_on_dashboard_set3
KPI chart	**View** a KPI chart from within the standalone KPI watchlist editor	• Access - Access to Answers • See 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 • See 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 • See View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
KPI watchlist	**Add** to a dashboard	• Access - Access to Dashboards • Scorecard - Add Scorecard Views to Dashboards • See View_or_edit_scorecard_set2
KPI watchlist	**Create** or **edit** within the Scorecard editor	• Scorecard - Create Views • See View_or_edit_scorecard_set2

Task Object	Task	Privileges Required to Perform the Task
KPI watchlist	**Create** or **edit** from within the standalone KPI watchlist editor	• See View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6 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	• See View_KPI_watchlist_in_standalone_KPI_watchlist_editor_set6
KPI watchlist	**View** on a dashboard	• See View_KPI_watchlist_on_dashboard_set3
Related document	**Follow** a related document link from within the standalone KPI watchlist editor	• See 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	• See Edit_KPI_watchlist_with_standalone_KPI_watchlist_editor_set5 • Actions - Create Navigate Actions

The table below lists the combination of privileges that are 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 • See View_or_edit_scorecard_set2
<Device>	**Contact owner** within the Scorecard editor	• Access - Access to Delivers • Admin: Security - User Population - Can List Users • Delivers - Create Agents • See View_or_edit_scorecard_set2
Action link	**Invoke** in a scorecard view on a dashboard	• Access - Access to Dashboards • See View_or_edit_scorecard_set2 Note that you must enable pop-ups in your browser.
Action link	**Invoke** within the Scorecard editor	• See 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 • See View_or_edit_scorecard_set2

Task Object	Task	Privileges Required to Perform the Task
All scorecard nodes[4], views, and documents (excludes KPI editor)	**View in read-only** within the Scorecard editor	• See 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 • See 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 • See 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 • See View_or_edit_scorecard_set2
Annotation	**Add** in a scorecard view within the Scorecard editor	• Scorecard - Add Annotations • See View_or_edit_scorecard_set2
Annotation	**View** in a scorecard view on a dashboard	• Access - Access to Dashboards • See View_or_edit_scorecard_set2
Annotation	**View** within the Scorecard editor	• See View_or_edit_scorecard_set2
Business owner	**Modify** within the Scorecard editor	• Admin: Security - User Population - Can List Users • See Edit_scorecard_set1
Business owner	**View** within the Scorecard editor	• Admin: Security - User Population - Can List Users • See View_or_edit_scorecard_set2
Causal linkage	**Create**, **edit**, or**delete** within the Scorecard editor	• Scorecard - Create/Edit Cause and Effects Linkages • See 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 • See 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 • See 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 • See 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	• See View_or_edit_scorecard_set2

Task Object	Task	Privileges Required to Perform the Task
Filter	**Add a user** to the filter in a scorecard smart watchlist within the Scorecard editor	• Admin: Security - User Population - Can List Users • See 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 • See 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 • See 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 • See Edit_scorecard_set1
KPI chart	**View** in a scorecard view on a dashboard	• Access - Access to Answers • Access - Access to Dashboards • See View_or_edit_scorecard_set2
KPI chart	**View** within the Scorecard editor	• Access - Access to Answers • See View_or_edit_scorecard_set2
Mission or vision statement	**Create** or **Edit** within the Scorecard editor	• Access - Access to Answers • Answers - Save Content with HTML Markup • Scorecard - Create Views • See Edit_scorecard_set1
Permissions dialog	**Modify** within the Scorecard editor	• Admin: Catalog - Change Permissions • See Edit_scorecard_set1 • Security: Access to Permissions Dialog
Perspective	**Create**, **Edit**, or **Delete** within the Scorecard editor	• Scorecard - Create/Edit Perspectives • See Edit_scorecard_set1
Related document	**Add**, **Edit**, or **Delete** for a scorecard node or scorecard view within the Scorecard editor	• See 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	• See View_or_edit_scorecard_set2
Scorecard	**Create**	• See 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	• See Edit_scorecard_set1 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 • See View_or_edit_scorecard_set2

Task Object	Task	Privileges Required to Perform the Task
Scorecard view, excludes mission and vision statements and KPI watchlists	**Create**, **Edit**, or **Delete** within the Scorecard editor	• Scorecard - Create Views • See Edit_scorecard_set1
Scorecard view	**View** on a dashboard	• Access - Access to Dashboards • See View_or_edit_scorecard_set2
Settings dialog	**Modify** or **View** settings	• See Edit_scorecard_set1
Strategy node[6]	**Create**, **Edit**, or **Delete** within the Scorecard editor using the Objective tab or KPI Details tab	• Scorecard - Create/Edit Objectives • See 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.
   - 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.
6. Strategy node is an objective or KPI within the **Strategy** pane.

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.

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**.

Cancel one running analysis as shown below.

- 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.

Use these steps to clear the web cache.

1. In the Cursor Cache table, identify the analysis and click **Close All Cursors**.
2. Click **Finished**.

Clear the cache entry associated with an analysis as described below.

- In the Cursor Cache table, identify the analysis and click the **Close** link in the **Action** column.

View the query file for information about an analysis as described below.

- 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.

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.

- 11*g* 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:

- Rules for Determining a User's Privileges or Permissions
- Example of Determining a User's Privileges with Application Roles
- Example of Determining a User's Permissions with Application Roles
- Example of Determining a User's Privileges with Removed Catalog Groups
- Example of Determining a User's Permissions with Removed Catalog Groups

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 access control (ACL) record that is *Denied* always takes precedence over any other grants. Within an individual step, a permission ACL record that has *No Access* always takes precedence over any access grant.
>
> The privilege *Denied* is the same as the permission *No Access*. The term *deny* is used interchangeably for both privileges and permissions.

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 .

Task 2 - Check for records for this user's Catalog groups

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, 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 Step 2.
   - 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.

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.

Task 4 - Fall back default behavior

The following sequence represents the checks completed for a specific application role called Authenticated User.

> **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.

1. If there is a record for the authenticated user application role, return that record's access. Done.
2. Else there is no record for the special application role. Go to Task 5 - No matching records at all.

Task 5 - No matching records at all

Return access denied. Done.

Example of Determining a User's Privileges with Application Roles

The diagram 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.

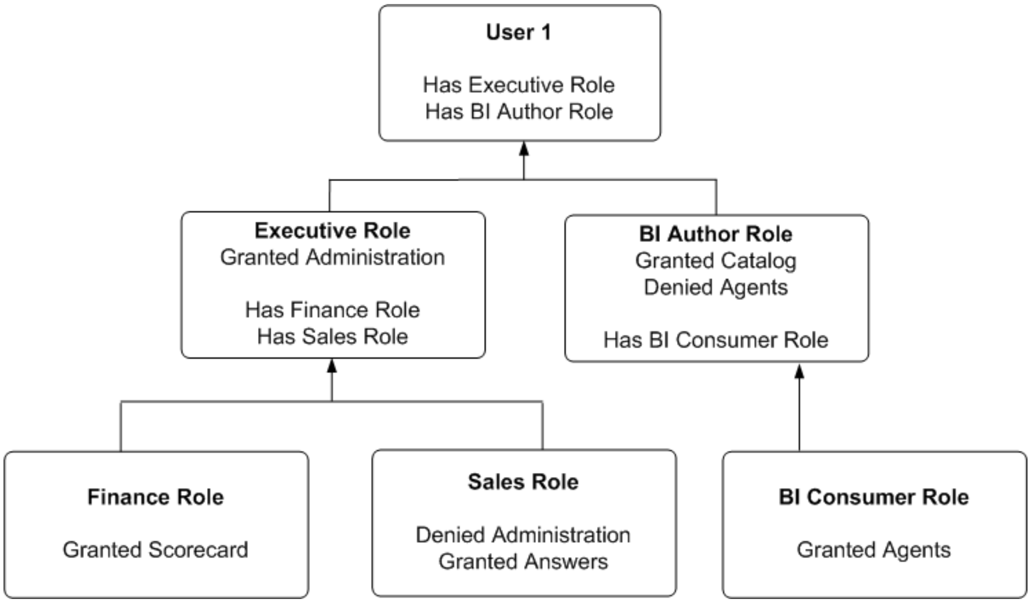
- The Executive role rectangle specifies that Executive is granted the Access to Administration privilege, and that the application roles Finance and Sales have in turn been given to Executive.
- The BI Author role rectangle specifies that BI Author is granted the Catalog privilege, is Denied the Agents 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.



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.

Example of Determining a User's Permissions with Application Roles

The diagram below 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.

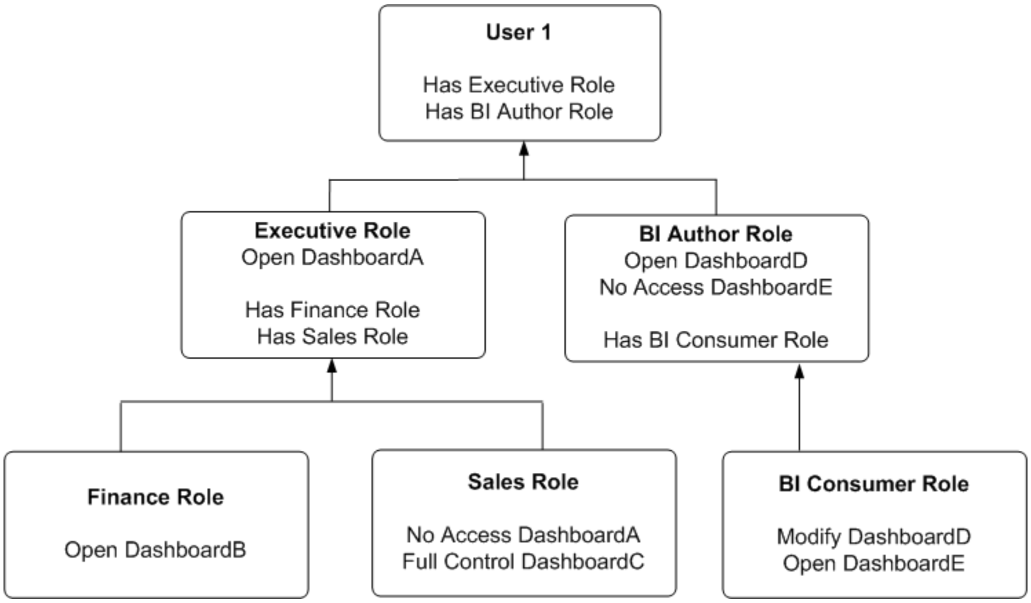
- The Executive Role rectangle specifies that Executive has no access to DashboardA, and that the application roles Finance and Sales have in turn been given to Executive.
- The BI Author Role rectangle specifies that BI Author role has open access to DashboardD, has no access to DashboardE, and that 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.



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. The 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. The 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.

Example of Determining a User's Privileges with Removed Catalog Groups

The diagram 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.

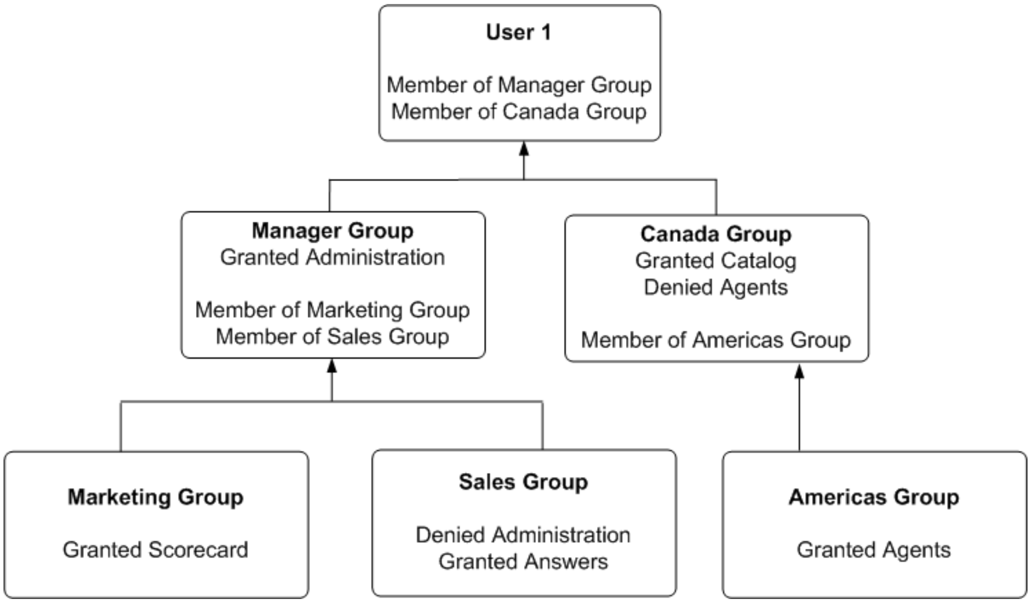
- The Manager Group rectangle specifies that Manager Group is granted the Access to Administration privilege, and that the Manager Group is in turn itself a member of both Marketing Group and Sales Group.
- The Canada Group rectangle specifies that Canada Group is granted the Catalog privilege, is denied 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.



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. The 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. The 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.

Example of Determining a User's Permissions with Removed Catalog Groups

The diagram below shows an example of how permissions are determined with removed 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.

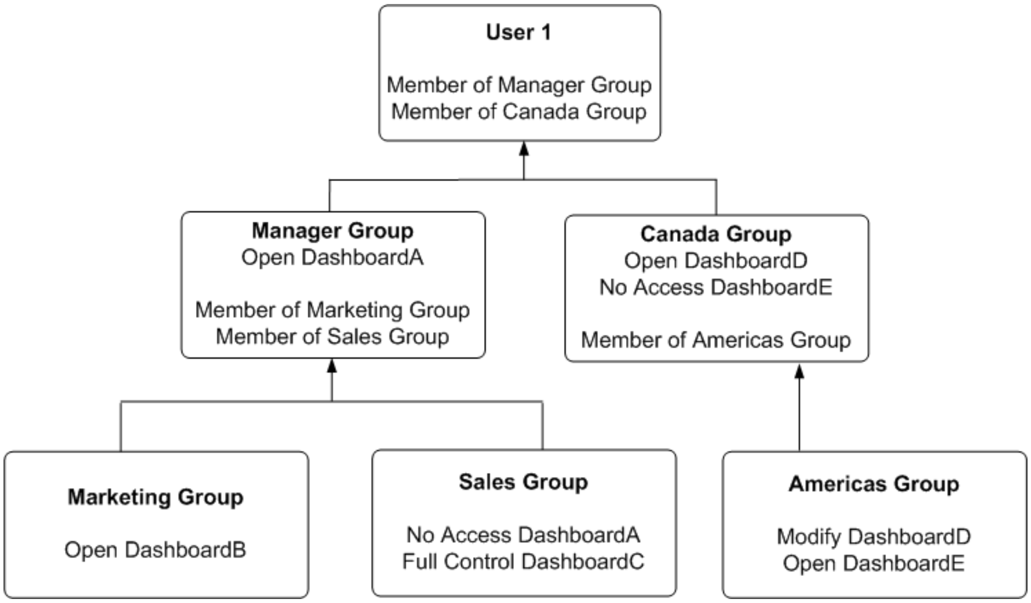
- The Manager Group rectangle specifies that Manager Group has open access to DashboardA, and that the Manager Group is in turn itself a member of both Marketing Group and Sales Group.
- The Canada Group rectangle specifies that Canada Group has open access to DashboardD, has no access to DashboardE, 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.



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.

Providing Shared Dashboards for Users

This section contains the following topics on providing shared dashboards for users:

- Understanding the Catalog Structure for Shared Dashboards
- Creating Shared Dashboards
- Testing the Dashboards
- Releasing Dashboards to the User Community

Understanding the Catalog Structure for Shared Dashboards

Learn about the catalog structure of My Folders and Shared Folders for shared dashboards.

The Oracle BI Presentation Catalog has two main folders:

- My Folders contain the personal storage for individual users. Includes a Subject Area Contents folder where you save objects such as calculated items and groups.
- Shared Folders contain 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.

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 *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.

See Managing Dashboards in *System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Testing the Dashboards

Before releasing dashboards and content to the user community, perform some tests.

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.

Releasing Dashboards to the User Community

What to do after testing is complete.

Notify the user community that the dashboard is available, ensuring that you provide the relevant network address.

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:

- Overview of Saved Customizations in Dashboards
- Administering Saved Customizations
- Permission and Privilege Settings for Creating Saved Customizations
- Example Usage Scenario for Saved Customization Administration

Overview of Saved Customizations in Dashboards

Saved customizations allow users to save and view 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.

Administering Saved Customizations

This topic describes the privileges and permissions that are required to administer 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 either 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.

Permissions are required so users can administer Oracle BI Presentation Catalog on shared and personal saved customizations.

Permission and Privilege Settings for Creating Saved Customizations

The topic describes user roles and specific permission settings that you can grant to users for creating saved customizations.

User Role	Permission and Privilege Settings
Power users such as IT users 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` You do not need to assign additional privileges.
Technical users such as managers 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` You do not need to assign additional privileges.
Everyday users that 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, you do not need to assign additional privileges.

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, you do not need to assign additional privileges.

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**.

Enabling Users to Act for Others

This section contains the following topics on enabling users to act for others:

- Why Enable Users to Act for Others?
- What Are the Proxy Levels?
- Process of Enabling Users to Act for Others

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 target user, the proxy user can access the objects in the catalog for which the target (another) user has permission.

Enabling a user to act for another is useful such as 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.

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*

  Users have read-only permissions to the objects that the target user can 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*

  Users inherit permissions and privileges 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.

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 another user can impersonate you as 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).

Process of Enabling Users to Act for Others

To enable users to act for others, perform the following tasks:

- Defining the Association Between Proxy Users and Target Users
- Creating Session Variables for Proxy Functionality
- Modifying the Configuration File Settings for Proxy Functionality
- Creating a Custom Message Template for Proxy Functionality

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.

Creating Session Variables for Proxy Functionality

To authenticate proxy users, you must create the two session variables along with their associated initialization blocks. For both variables, modify the sample SQL statement using the database schema.

- `PROXY`

  Use the `PROXY` variable to store the name of the proxy user.

  Use the initialization block, `ProxyBlock`, and include code such as the following:

  ```
   select targetId from Proxies where UPPER(targetid) =
  UPPER('VALUEOF(NQ_SESSION.RUNAS)') and UPPER(proxyid) = UPPER(':USER')
  ```

- `PROXYLEVEL`

  Use `PROXYLEVEL` variable to store the proxy level as *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(':USER')
  ```

Modifying the Configuration File Settings for Proxy Functionality

Use various elements in the instanceconfig.xml file to configure the proxy functionality.

See Creating a Custom Message Template for Proxy Functionality

1. Open the `instanceconfig.xml` file for editing.
2. In the configuration file, locate the sections to add the following elements:
   - `LogonParam` as the parent element for the `TemplateMessageName` and `MaxValues` elements.
   - `TemplateMessageName` as 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.

- `MaxValues` specifies the maximum number of target users that are listed in the **User** field in the Act As dialog.

  If the number of target users for a proxy user exceeds`MaxValues`, then an edit box is shown for the proxy user to enter the ID of a target user. The default value is *200*.

3. Include the elements and their child elements, 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.

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** field 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
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

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. See Modifying the Configuration File Settings for Proxy Functionality.

1. To create the custom message template in the original custom message file:
    1. Make a backup of the original custom message file in a separate directory.
    2. 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 configure a folder (custommessages) as an application in WebLogic Server, to make Oracle BI Presentation Services aware of it.
3. Start the custom message template by adding the WebMessage element's begin and end tags. For example:

    ```
    <WebMessage name="LogonParamSQLTemplate">
    </WebMessage>
    ```
4. After the `</WebMessage>` tag:
    1. Add the <XML> and </XML> tags
    2. Between the <XML> and </XML> tags, add the <logonParam name="RUNAS"> and </logonParam> tags.
    3. Between the `<logonParam name="RUNAS">` and `</logonParam>` elements, add each of the following elements 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>
    ```

    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 custom messages 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 BI Server Administration screen.