ORACLE

Installing and Configuring Oracle Analytics Server 24 (7.6) for use with Oracle Enterprise Manager 24ai Release 1 (24.1)

A technical brief for using OAS 24 (7.6) with EM 24ai (24.1)

November 18, 2024 | Version 1.0 – First Proof

PURPOSE STATEMENT

This document provides an overview of the installation and configuration of Oracle Analytics Publisher 24 (7.6) for use with Enterprise Manager 24ai.

Oracle Analytics Publisher is readily adaptable to utilize the rich data set that is available via Enterprise Manager 24ai.

This guide has been written and validated against Oracle Analytics Server 24 (7.6).

THE NUMEROUS SCREEN SHOTS DISPLAYED IN THIS DOCUMENT ARE FROM ORACLE ANALYTICS SERVER 24 (7.6)

DISCLAIMER

This document in any form, software, or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement, nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

DISCLAIMERS FOR PRE-RELEASE, PRE-GA PRODUCTS

The **revenue recognition disclaimer** on this page is required for any technical brief that addresses future functionality or for products that are not yet generally available (GA). If you are unsure whether your statement of direction needs the disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.

The **testing disclaimer** in the copyright section on the last page (highlighted in yellow) is provided by the FCC for hardware products. It must appear in the copyright section for all pre-release, pre-GA hardware products. Be sure to remove the yellow highlighting before publishing. When the product becomes GA, update your collateral by removing the disclaimer from the copyright section. If your product is already GA or if you are writing about a software product, delete the disclaimer from the copyright section.

Important: If your product is not GA, then you cannot include any regulatory compliance information in the statement of direction. Regulatory compliance information may be included for GA products only if you have completed all required safety and emissions testing, and you have received the certificates issued by the testing organization

TABLE OF CONTENTS

APPENDICES

Preface

- Oracle Analytics Server cannot be installed in the same WebLogic domain, nor on the same host system, as Enterprise manager 24ai.
- This guide is meant to be utilized as a supplement to, and not a replacement for, the existing Oracle Analytics Server document set.
- An outline of the required steps for the fresh installation of OAS 24 (7.6) is provided, but no support for OAS will generally be provided by the Oracle Analytics team.
- The document provides specific details and instructions for an installation of Oracle Analytics Server 24 (7.6), on separate host system, to run Pixel Perfect Reports against the Enterprise Manager 24ai repository database.

BEFORE BEGINNING THE PROCEDURES DOCUMENTED IN THIS HANDBOOK, DOWNLOAD ANY CUSTOMIZED PIXEL PERFECT REPORTS FROM THE STANDALONE OAS 6.4, USING THE OAS USER INTERFACE.

Licensing Model and Support for Pixel Perfect Reporting with Oracle Analytics Server 24 (7.6)

For those customers can continue to use Oracle Analytics Publisher for use with Enterprise Manager 24ai.

The Enterprise Manager licensing and support model continues to carry forward from prior Enterprise Manager 13c releases.

Installation and configuration of Oracle Analytics Publisher will be the responsibility of the customer.

Requirements

This guide provides a best practice for installation and configuration of OAS 24 (7.6).

Enterprise Manager will continue to supply and support a set of feature-rich Oracle provided Out of Box reports designed and tested with Oracle Analytics Publisher 24 (7.6).

This guide is not meant to replace or otherwise supersede the large set of documentation books that are currently developed and available for Oracle Analytics Server, and Fusion Middleware as a whole, via the Oracle Help Center.

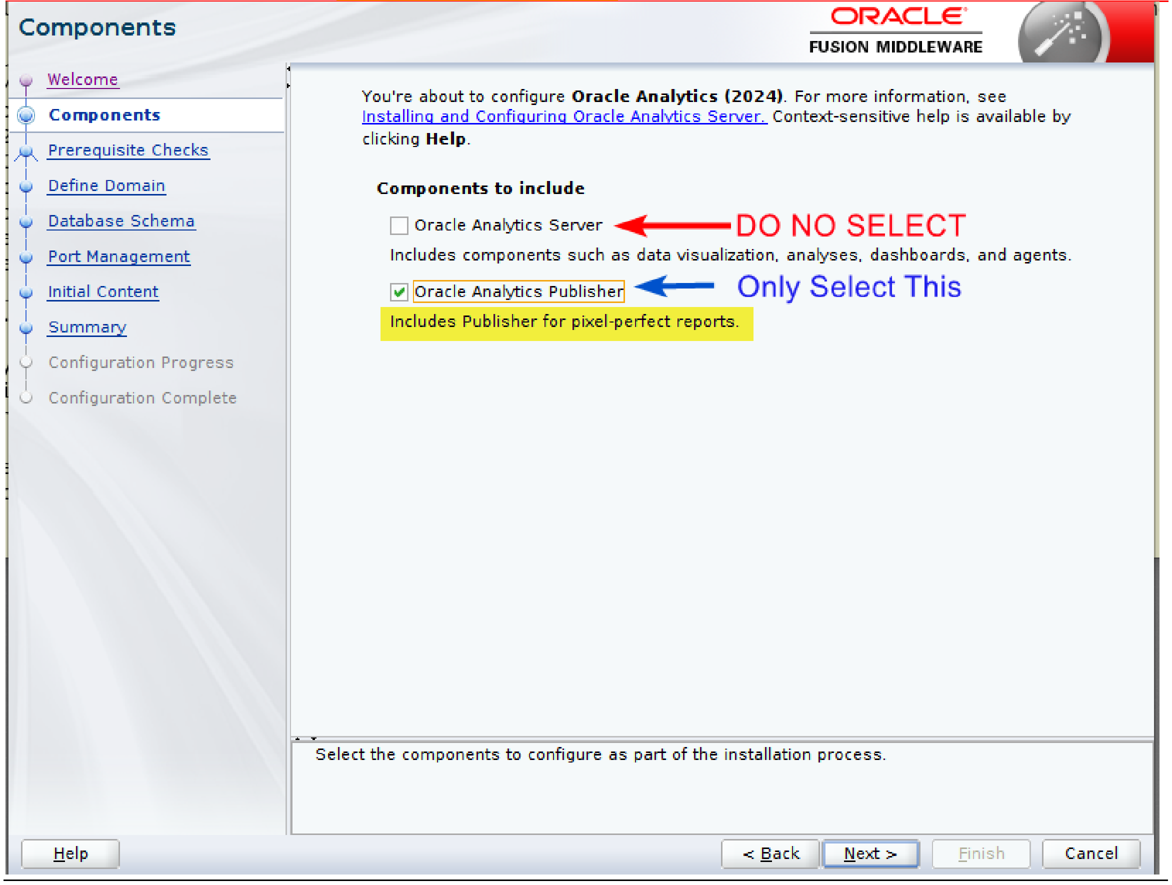
External References

Throughout this guide many footnotes are available that reference more detailed documentation books available for Oracle Analytics Server, Fusion Middleware Control, and other Oracle technologies.

These footnotes are cross referenced in ‘Chapter 10 - References’.

Limited Scope

1. Configuration of the full Oracle Analytics Server is not supported with Enterprise Manager 24ai.
   - This guide only addresses configurations including the Oracle Analytics Publisher component, and **not the full Oracle Analytics Server component.**
     - Be sure to only select Oracle Analytics Publisher.



You're about to configure **Oracle Analytics (2024)**. For more information, see Installing and Configuring Oracle Analytics Server. Context-sensitive help is available by clicking **Help**.

Components to include

□ Oracle Analytics Server

Includes components such as data visualization, analyses, dashboards, and agents.

☑ Oracle Analytics Publisher

Includes Publisher for pixel-perfect reports.

Select the components to configure as part of the installation process.

   - As an alternative to this guide, utilize the standard Oracle OAS configuration documentation.[1]

2. High Availability configurations and/or Disaster Recovery solutions for OAS are beyond the scope of this guide.
   - Oracle Analytics Server fully supports Oracle's Maximum Availability Architecture (MAA).
     - The Oracle MAA architecture supports multiple Oracle Analytics Server systems as part of a single WebLogic cluster.
     - As an alternative to this guide, reference these documents:
       - Oracle® Analytics Enterprise Deployment Guide for Oracle Analytics Server.[2]
       - Oracle's Maximum Availability Architecture.[3]

3. A dedicated host system is required for the standalone Oracle Analytics Server.
   - It is theoretically possible to install and utilize OAS on the same host system as Enterprise Manager 24c.
   - However, there are many disadvantages to this approach.
     - Out of the box, configuration of a standalone OAS on the same host system as Enterprise Manager will fail.
     - This is due to a limitation in the underlying WebLogic framework related to "Coherence Clusters".
   - If a customer managed to install and configure OAS on the same host system as EM 24ai, there could be unintended side effects that impact the operation of both EM 24ai and OAS 24 (7.6).

[1] (Configuring Oracle Analytics Server, 2021)
[2] (Oracle® Analytics Enterprise Deployment Guide for Oracle Analytics Server, 2020)
[3] (Oracle Maximum Availability Architecture, MAA, 2021)

Planning for a Fresh Installation of Oracle Analytics Server 24 (7.6)

Step A: Install and configure Enterprise Manager 24ai

1. Follow all documented procedures according to the official Enterprise Manager documentation set.
2. Do not proceed to step C until all relevant corporate internal requirements are met.

Step B: Follow the detailed steps in this technical brief

1. Utilize this technical brief to install and configure a standalone OAS 24 (7.6) installation on a separate, dedicated, host system.
2. Ensure that all relevant procedures up to and including chapter 15 are complete.

Step C: Update the standalone OAS installation for use with Enterprise Manager 24ai

1. Follow the procedures detailed in 'Chapter 8- Uploading Enterprise Manager Provided Reports':
2. Upload the updated set of Oracle Provided out of Box reports that are included with EM 24ai.
   - Utilize the standalone OAS User Interface to upload this new set of Oracle Provided Out-of-Box reports to OAS.

Recommendation for the version of Oracle Analytics Server

Please note that there are currently two versions of this guide.

- This guide is specific to Oracle Analytics Server (OAS) version 24 (7.6).
- The prior versions of this guide was specific to Oracle Analytics (OAS) version 6.4.
- OAS version 23 (7.0) has not been certified for use with Enterprise Manager, and no plans exist for this.

Both versions of this guide have been written, developed, and tested by the Enterprise Manager Development organizations.

Cross References to Relevant Oracle Documents

OAS supports all the same architectural and security options as was provided via the embedded BI Publisher.

However, lifecycle management for the standalone OAS product is via a rich, and complex, set of documentation books.

Beyond OAS, numerous other Oracle technologies and products are referenced and outlined within these pages.

References to relevant Oracle documentation are available throughout this guide, utilizing document footnotes.

Organization of this Guide

STEP	DESCRIPTION	CROSS-REFERENCE
1	base install and configuration of OAS	Chapter 1
2	Major concepts and components	**Error! Reference source not found.**
3	OAS Security Configuration	Chapter 3
	If Repository Based:	
4a	OAS For EM Repository-based Security	Chapter 4 ⇨ Skip to Chapter 6
	else LDAP Based:	
4b	OAS LDAP Configuration – Enterprise Manager parity	Chapter 5 ⇨ Continue to Chapter 6
5	Configuration of required OAS Datasource(s)	Chapter 6
6	Prepare for Oracle Provided Out of Box Reports	Chapter 7
7	Uploading Enterprise Manager Provided Reports	Chapter 8
8	Migrating BIP Schedules from standalone OAS 6.4	Chapter 9

Table 1. Outline of Guide

There is also a flow chart of the above table in Figure 1 - Overview of installation and configuration steps

CHAPTER 1. BASE INSTALL AND CONFIGURATION OF OAS

A general overview of the installation and configuration of Oracle Analytics Server is shown in the below table, with hyperlink references to the appropriate Oracle Analytics Server documentation:

- Installing and Configuring Oracle Analytics Server
- Describes how to install, configure, and uninstall Oracle Analytics Server

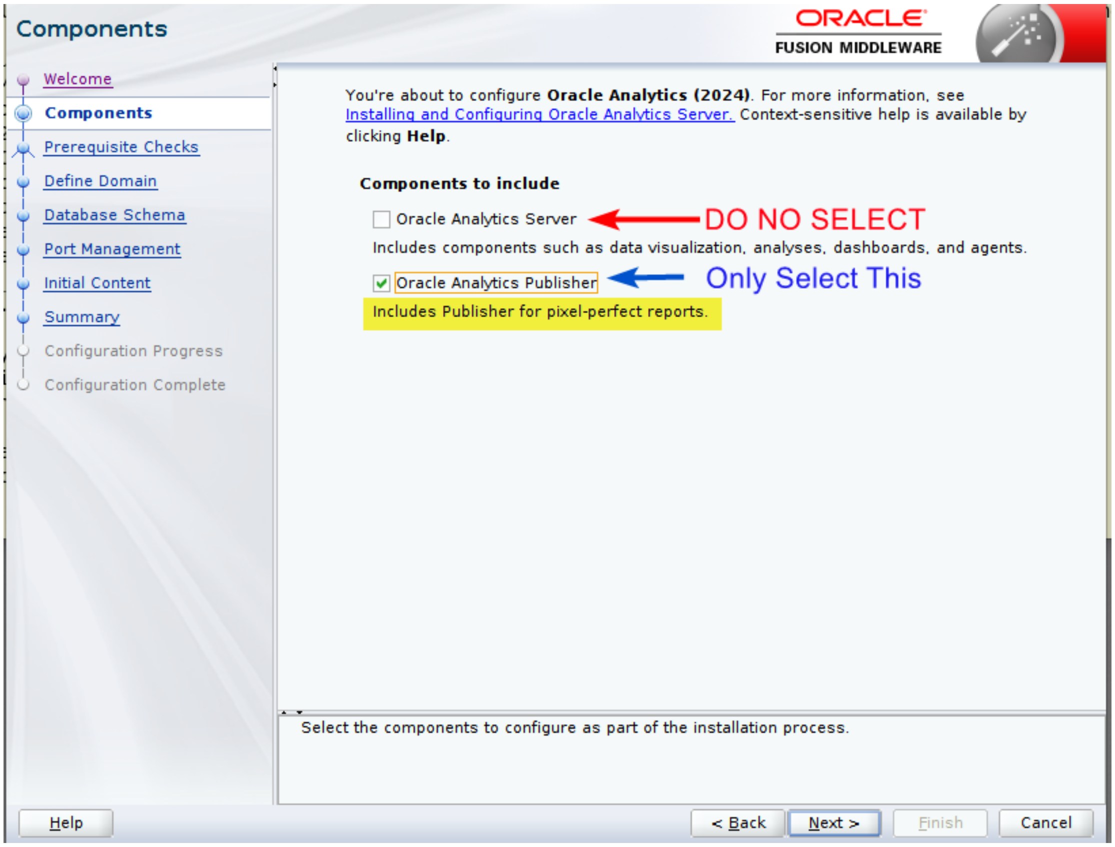
Step	Link
1	Roadmap for Installing and Configuring a Standard Installation Topology
2	Roadmap for Verifying Your System Environment
3	Obtaining the Product Distribution
4	About Product Distributions

Table 2. High-level steps required for installing a standard installation topology.

General order of installation procedure

1. Install pre-requisite software.
2. Check for any mandatory patches.
3. Obtain Product distributions.
   a) Supported Java JDK software.
   b) Fusion Middleware Infrastructure software.
   c) Oracle Analytics Server software.
4. Install Java JDK.
5. Install Fusion Middleware infrastructure.
6. Install Oracle Analytics Server.
7. Configure Oracle Analytics Server with only pixel perfect reporting.

NOTE: ONLY CONFIGURE PIXEL PERFECT REPORTING:



You're about to configure **Oracle Analytics (2024)**. For more information, see Installing and Configuring Oracle Analytics Server. Context-sensitive help is available by clicking **Help**.

Components to include

☐ Oracle Analytics Server ← DO NO SELECT

Includes components such as data visualization, analyses, dashboards, and agents.

☑ Oracle Analytics Publisher ← Only Select This

Includes Publisher for pixel-perfect reports.

Select the components to configure as part of the installation process.

Overview of post install steps for OAS specific to Enterprise Manager

THE STEPS IN THIS DOCUMENT WERE SPECIFICALLY DEVELOPED AND TESTED AGAINST ENTERPRISE MANAGER 24C ONLY

Below is an outline of the steps needed to be followed the successful base install and configuration of OAS 24 (7.6).

It is important to follow these detailed steps against Enterprise Manager 24ai only

1. If appropriate, download any customized reports from the prior standalone OAS 6.4.
2. Configure the appropriate OAS security model and required roles.[4]
3. Configure the OAS Datasource(s), for use with the Enterprise Manager Repository database(s). [5]
4. Configure the EM repository database such that EM administrators have access to EM data, when logged into the standalone OAS.
5. Install and utilize the Oracle Enterprise Manager 24c provided out-of-the-box Reports.
6. If appropriate, upload any customized reports from the prior standalone OAS 6.4.
7. Migrate the BIP Report Schedules from the standalone OAS 6.4 to the standalone OAS 24 (7.6).[6]

Overview of OAS Security Configurations

Enterprise Manager is generally configured with one of the security configurations shown below. [7]

The standalone OAS can then to be configured to match, or map, to this same security configuration.

ENTERPRISE MANAGER SECURITY CONFIGURATION	CORRESPONDING OAS SECURITY MODEL	UNDERLYING SECURITY STORE
Repository-based security: Default, out-of-box.	Database Security Model[8]	Enterprise Manager Repository database system. (RDBMS): All users and roles defined in the RDBMS.
LDAP: `emctl` commands.	Fusion Middleware[9] Default, out-of-box.	LDAP server (i.e., OID or AD): All users and groups defined in the LDAP server.

Table 3. Mapping of Enterprise Manager Security Configurations to OAS Configuration

[4] (Integrate with Other Oracle Security Models, 2024)

[5] (Set Up Data Sources, 2024)

[6] (Migrating Scheduler Jobs and Job History, 2024)

[7] (Security Features : Supported Authentication Schemes, 2024)

[8] (Integrate with Oracle Database Security, 2024)

[9] (Configure Oracle Fusion Middleware Security Model, 2024)

CHAPTER 2. MAJOR CONCEPTS AND COMPONENTS

Concept: EM Repository based authentication

- Requirements:
  - OAS 'Database Security Model'[10]
  - Fallback 'SuperUser'
  - Create required DBMS roles.
  - Grant/Revoke these roles to appropriate Enterprise Manager administrator(s).
    - Note: Out of box, EM administrators have a corresponding DBMS user.
  - Create and configure the JDBC Datasource EMREPOS for use with Enterprise Manager.

Concept: LDAP-based authentication

Requirements:

- OAS 'Fusion Middleware Security Model'[11]
- corresponding Fusion Middleware Configuration,
- Configuration steps are required, utilizing the Fusion Middleware Control that is bundled with OAS
- Additional manual steps involving editing of specific Fusion Middleware configuration files.
- Create and configure the JDBC Datasource(s [`EMREPOS`].

Concept: OAS 24 (7.6) database references

Oracle Analytics Server is configured with either 2 or 3 database references.

DATABASE REFERENCE	OAS SECURITY MODEL	REFERENCED DATA
1. Oracle Analytics Server Schema	Common to Both	• Standard WebLogic schema. • OAS scheduler schema.
2. Enterprise Manager Repository	Common to Both	The actual Enterprise Manager Repository data that is rendered by Oracle Analytics Publisher Reports.
3. Enterprise Manager Repository	Database Security Model[12]	The credentials for all Enterprise Manager Administrators.

Note that the databases referenced can utilize any of the standard Oracle Databases (for example, pluggable databases).

Two Common Database References

1. Oracle Analytics Server Schema:
   - The Oracle Database that contains all the database objects required by Oracle Analytics Server:
   - This consists of the complete Oracle Analytics database schema, including the OAS scheduler schema.
     - This database is configured as part of the Oracle Analytics configuration process. [13]
   - For further details on the OAS scheduler, see 'section Chapter 9-Migrating BIP Schedules from standalone OAS 6.4.
2. Enterprise Manager Repository:
   - This is the complete Enterprise Manager Repository Database Schema.
   - This database is configured for use with OAS in 'Chapter 6 - Configuration of required OAS Datasource(s)'.
   - This database contains all the Repository data that is utilized to run Oracle Analytics Publisher reports.

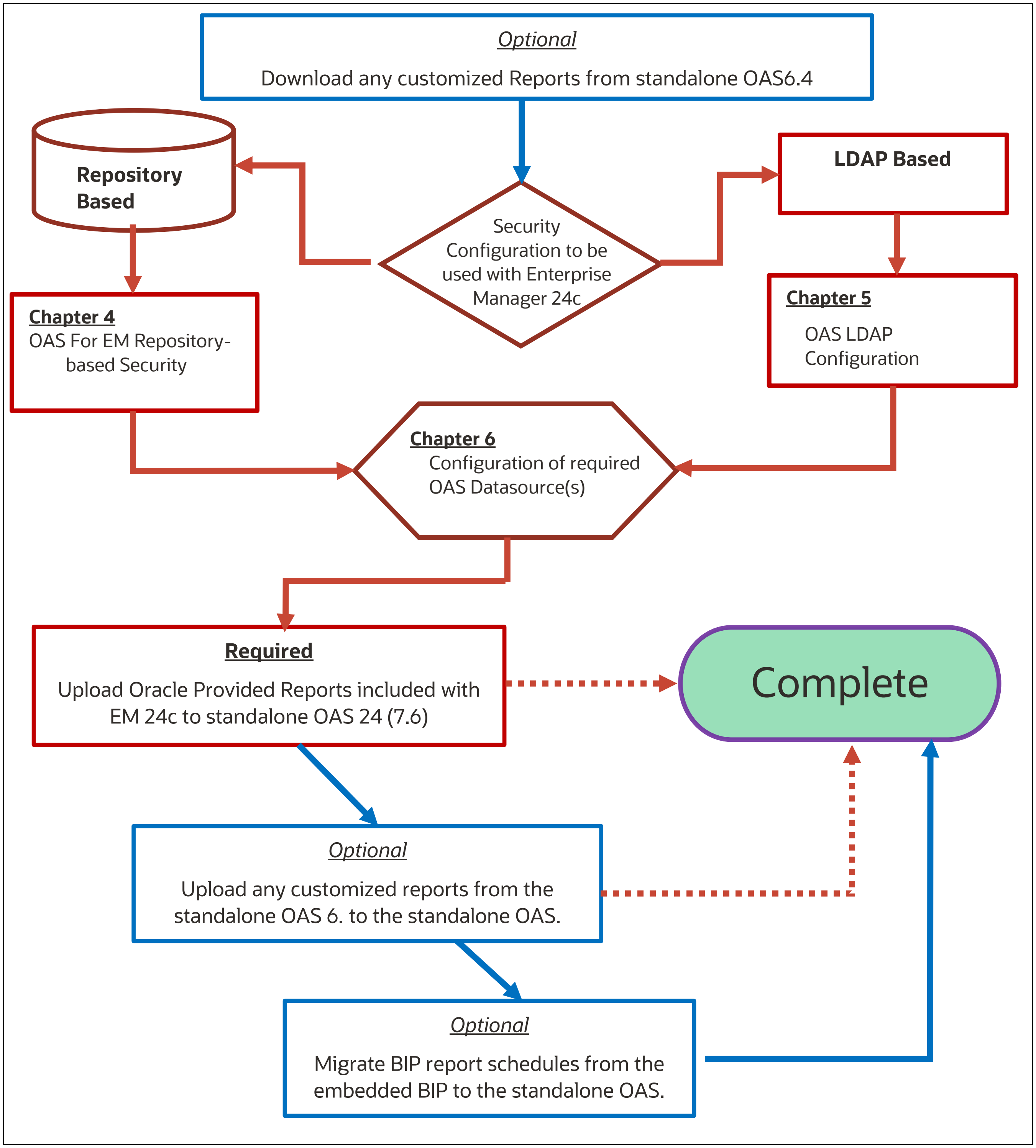
Concept: Repository Based Authentication – 3rd Database Reference

3. Enterprise Manager Repository:

[10] (Integrate with Oracle Database Security, 2024)
[11] (Configure Oracle Fusion Middleware Security Model, 2024)
[12] (Integrate with Oracle Database Security, 2024)
[13] (Configuring Oracle Analytics Server, 2024)

- The Oracle Database that contains all required credentials of all Enterprise Manager Administrators.
- This provides support for logging into OAS as Enterprise Manager Administrators, for use with OAS..

Figure 1. Overview of installation and configuration steps


Optional
Download any customized Reports from standalone OAS6.4
Repository Based
Security Configuration to be used with Enterprise Manager 24c
LDAP Based
Chapter 4
OAS For EM Repository-based Security
Chapter 5
OAS LDAP Configuration
Chapter 6
Configuration of required OAS Datasource(s)
Required
Upload Oracle Provided Reports included with EM 24c to standalone OAS 24 (7.6)
Complete
Optional
Upload any customized reports from the standalone OAS 6. to the standalone OAS.
Optional
Migrate BIP report schedules from the embedded BIP to the standalone OAS.

CHAPTER 3. OAS SECURITY CONFIGURATION

This chapter provides an overview of the remaining configuration steps, which are somewhat complex.

BEFORE BEGINNING THE PROCEDURES DOCUMENTED IN THIS HANDBOOK, DOWNLOAD ANY CUSTOMIZED BIP REPORTS FROM THE EMBEDDED BIP IN EM 13.4, USING THE BIP USER INTERFACE.

There are two distinct OAS security models that are fully documented below.

Each of these two OAS security models map directly to a corresponding Enterprise Manager Security Configuration.

- A single installation of OAS can only support one of the two security models below at any given time.

EM SECURITY CONFIGURATION	OAS SECURITY MODEL AND ADDITIONAL REQUIRED STEPS
1. Enterprise Manager Repository-based security ▪ Out of box configuration	OAS Database Security Model ▪ Additional steps: 1. Configure OAS for Database Security Model. 2. On EM Repository DBMS, perform DBMS role assignments.
2. LDAP	OAS Fusion Middleware Security Model ▪ Additional steps: 1. Ensure OAS is configured for Fusion Middleware Security Model. 2. On OAS WebLogic Domain: a. WebLogic Authentication Provider configuration. b. Fusion Middleware Control Application Role assignments. c. Edits to Java Platform Services (JPS) configuration file.

Table 4. OAS Security Configuration Steps

In order to change the OAS Security Model, access to the OAS **Administration** link, and the subsequent **Administration screens**, as shown in 'Figure 4 - Administration Screens and Security Center. Needed for Security Configuration', it is necessary to login to OAS as a user with the required permissions to access these pages.

When OAS is initially installed, the **OAS Fusion Middleware security model** is configured by default.

In this configuration, the **weblogic** user will always be available, with the password that was chosen during OAS configuration. See 'section **Error! Reference source not found.** - **Error! Reference source not found.**'.

Additionally, the **weblogic** user will by default have the required permissions to access the **Administration screens**.

If mistakes are made, and login to OAS using standard procedures is unavailable, or no user has the required permissions to access to the **Administration** link (and subsequent **Administration screens)**, then there is no way to resolve issues using the OAS user interface and manual edits to XML configuration files would be required.

Given this, it is strongly recommended to enable the internal **Superuser** during these initial configuration steps.

This special **Superuser** does not rely on any underlying OAS security model, but instead utilizes the simpler file-based security model that is built-in to OAS.

For simplicity and proper management of OAS, ensure that the username chosen for this internal OAS Super User does not overlap with a *real* Enterprise Manager (or LDAP) user.

For example, do not use the name **sysman.**

Oracle Analytics Publisher Authentication and Report Execution Flow

There are four main interactions that all Enterprise Manager Administrators will utilize when Oracle Analytics Publisher is accessed.

1. Oracle Analytics Server Authentication
2. Oracle Analytics Server User Interface Capabilities.
3. Oracle Analytics Server Catalog Access.
4. Oracle Analytics Server Report Execution.

OAS Authentication

As specified above, for Enterprise Manager 13.5, two main mechanisms for user authentication are provided:

1. Enterprise Manager Repository-based Security
2. LDAP, with or without SSO, based upon Fusion Middleware Security Providers.

OAS User Interface Privileges

OAS supports three hierarchical levels of User Interface Privileges.

As the levels below are followed, they are additive.

All capabilities from level 1 are available in level 2, and all capabilities from level 1 and level 2 are available in level 3, and all capabilities from levels 1,2, and 3, are available in level 4.

#	DESCRIPTION	DBMS ROLE EM REPOSITORY BASED	LDAP ROLE WITH OR WITHOUT SSO
1	View and execute OAS Reports.	MGMT_USER	BI Consumer
2	Schedule OAS Reports	XMLP_SCHEDULER	BI Consumer: *Includes*
3	Author OAS Reports (and manipulate catalog objects, see next table).	XMLP_DEVELOPER	BI Author
4	Administer OAS ○ Manage and maintain the OAS Security Model. ○ Manage and maintain the OAS Data Source Configuration (i.e., EMREPOS, EMREPOS2, etc.) ○ Manage and maintain the OAS Scheduler. ○ General OAS System Administration.	XMLP_ADMIN	BI Administrator

Table 5. OAS Privileges

OAS Server Catalog Access

The same Role Names specified above are also utilized to provide varying levels of access to each OAS Catalog Object (reports, Datamodels, folders).

Typically, these Role Names are applied in a similar hierarchical manner as User Interface Level Access.

This works out as below:

#	DESCRIPTION	DBMS ROLE EM REPOSITORY BASED	LDAP ROLE LDAP, WITH OR WITHOUT SSO
1	• View Reports, and corresponding Datamodels. • Expand Folder Nodes. • Execute Reports (not applicable to Datamodels).	MGMT_USER	BI Consumer
2	• Schedule OAS Reports.	XMLP_SCHEDULER	*BI Consumer* *(There is no separate FMW Scheduler Role by default)*
3	• Edit, Cut/Copy/Paste/Delete OAS Catalog Objects (i.e., Reports, Datamodels, and folders).	XMLP_DEVELOPER	BI Author
4	• Full Capabilities on all Catalog Objects	XMLP_ADMIN	BI Administrator

Table 6. OAS Catalog Permissions

OAS Report Execution

Once an Enterprise Manager Administrator is logged into OAS, and has access to an OAS Report, the report itself can be executed (or scheduled).

When an OAS Report Executes, the execution model from Enterprise Manager 13.4 is maintained.

That is, for a given user logged into OAS, OAS Reports will only have target-level access to those Enterprise Manager Targets that that EM Administrator normally would have access to.

In this way, EM Data can be viewed inside of OAS with the same visibility as when utilizing the Enterprise Manager Console directly.

The following two sections provide a flow chart of the two main components of OAS Report Execution.

1. OAS Login Flow – Valid or invalid credentials provided.
2. OAS *privilege* assignment – If a user is valid, associate roles.

OAS Login Processing and Privilege Assignment

Flow charts for OAS Login Processing and Privilege Assignment can be found in Appendix F and Appendix G.

CHAPTER 4. OAS FOR EM REPOSITORY-BASED SECURITY

As discussed earlier, the standalone OAS is to be configured either using OAS Database Security Model or the OAS Fusion Middleware Security Model.

This chapter details the steps for the OAS Database Security Model.

Enterprise Manager Repository-based security ▪ Out of box configuration	OAS Database Security Model ▪ Additional steps: Configure OAS for Database Security Model. On EM Repository DBMS, perform DBMS role assignments.

If utilizing the Fusion Middleware Security Model, skip to 'Chapter 5 - OAS LDAP Configuration – Enterprise Manager parity'.

From this point forward, the required steps are complex, and somewhat error prone.

This chapter details configuration of the standalone OAS against an Enterprise Manager Installation using the default security configuration of 'Repository based Authentication'.

For this configuration of EM, the OAS '**Database Security Model**' is utilized.

The referenced database for iem 3 above will not necessarily be the same as items 1 and 2.

Create required DBMS roles and grant to required EM administrators.

Create the required roles, and minimal role grants, on the Enterprise Manager repository database:

```
$ sqlplus sys/●●●●●● as sysdba
sql> REM Create base roles
sql> create role XMLP_ADMIN;
sql> create role XMLP_DEVELOPER;
sql> create role XMLP_SCHEDULER;
sql>
sql> REM Create Role Hiearchy
sql> grant XMLP_DEVELOPER to XMLP_ADMIN;
sql> grant XMLP_SCHEDULER to XMLP_ADMIN;
sql> grant MGMT_USER to XMLP_ADMIN;
sql>
sql> grant XMLP_SCHEDULER to XMLP_DEVELOPER;
sql> grant MGMT_USER to XMLP_DEVELOPER;
sql>
sql> REM Sysman gets super admin
sql> grant XMLP_ADMIN to sysman;
sql> exit;
```

When additional Enterprise Manager users need OAS permissions beyond basic report viewing, one or more of the above roles will need to be granted to them. For example:

```
$ sqlplus sys/●●●●●● as sysdba
sql> REM Grant any required roles to individual EM Administrators
sql> grant XMLP_DEVELOPER to USER1;
sql> grant XMLP_SCHEDULER to USER2;
sql> exit;
```

For full details on this process, consult (OAS - Integrate with Oracle Database Security, 2021) Database Security.

Preparation for upload of Oracle Provided Reports

In preparation for the upload of the Oracle Provided Reports, detailed in Chapter 7 - Prepare for Oracle Provided Out of Box Reports, the following set of role grants should be created.

```
$ sqlplus sys/●●●●●● as sysdba
REM Create base EMBIP roles
create role EMBIPADMINISTRATOR;
create role EMBIPAUTHOR;
create role EMBIPSCHEDULER;
create role EMBIPVIEWER;

REM Create Role Mapping
grant XMLP_ADMIN to EMBIPADMINISTRATOR;
grant XMLP_DEVELOPER to EMBIPAUTHOR;
grant XMLP_SCHEDULER to EMBIPSCHEDULER;
grant MGMT_USER to EMBIPVIEWER;

Rem Ensure SYSMAN is an OAS Super Administrator
grant EMBIPADMINISTRATOR to SYSMAN;
```

Allowing access to Oracle Provided Reports for Individual EM users

The Oracle provided reports are installed with the four `EMBIP`* roles shown above.

For complete and proper access to these Oracle Provided Reports, ensure that the respective EMBIP* role(s) are assigned to the individual Enterprise Manager users.

- *If there are many EM users to process, a small SQL script can be written for this purpose.*

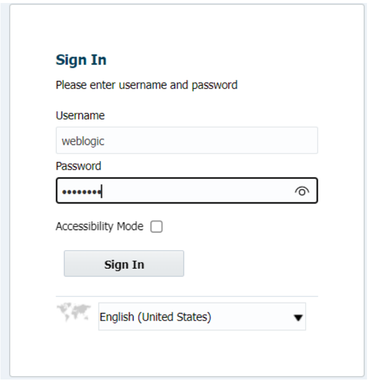
```
REM Setup an EMCC Report Author 'USER1'
grant EMBIPAUTHOR to USER1

REM Setup an EMCC Report Viewer 'USER2'
grant EMBIPVIEWER to USER2
```

4.1 Configure OAS for 'Database Security Model'

The complete set of steps are outlined below, followed by example screenshots.

Step 1 - Login to OAS

- For first time configuration, login to OAS as the **weblogic** user.
  - If OAS is already configured for the 'Database Security Model', login as an Enterprise Manager Super Administrator, for example 'SYSMAN'.
  - If neither of these logins are possible, and the instructions to setup a local SuperUser were followed, login as this local 'SuperUser'.



Sign In

Please enter username and password

Username: weblogic

Password: ••••••••

Accessibility Mode □

Figure 2. Login to OAS as the **weblogic** user (or the local SuperUser)

Step 2 - Click on the Administration link

In the far right-hand side of the OAS user interface, just to the right-hand side of the **Open** link, single click on the user icon. In the drop-down menu that is shown, choose Administration.

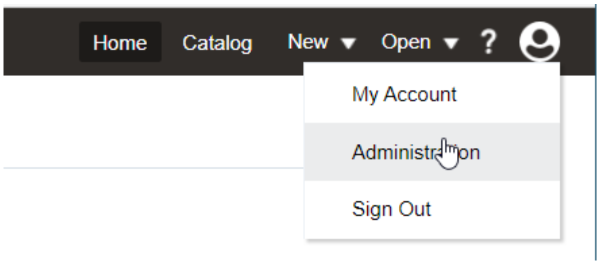
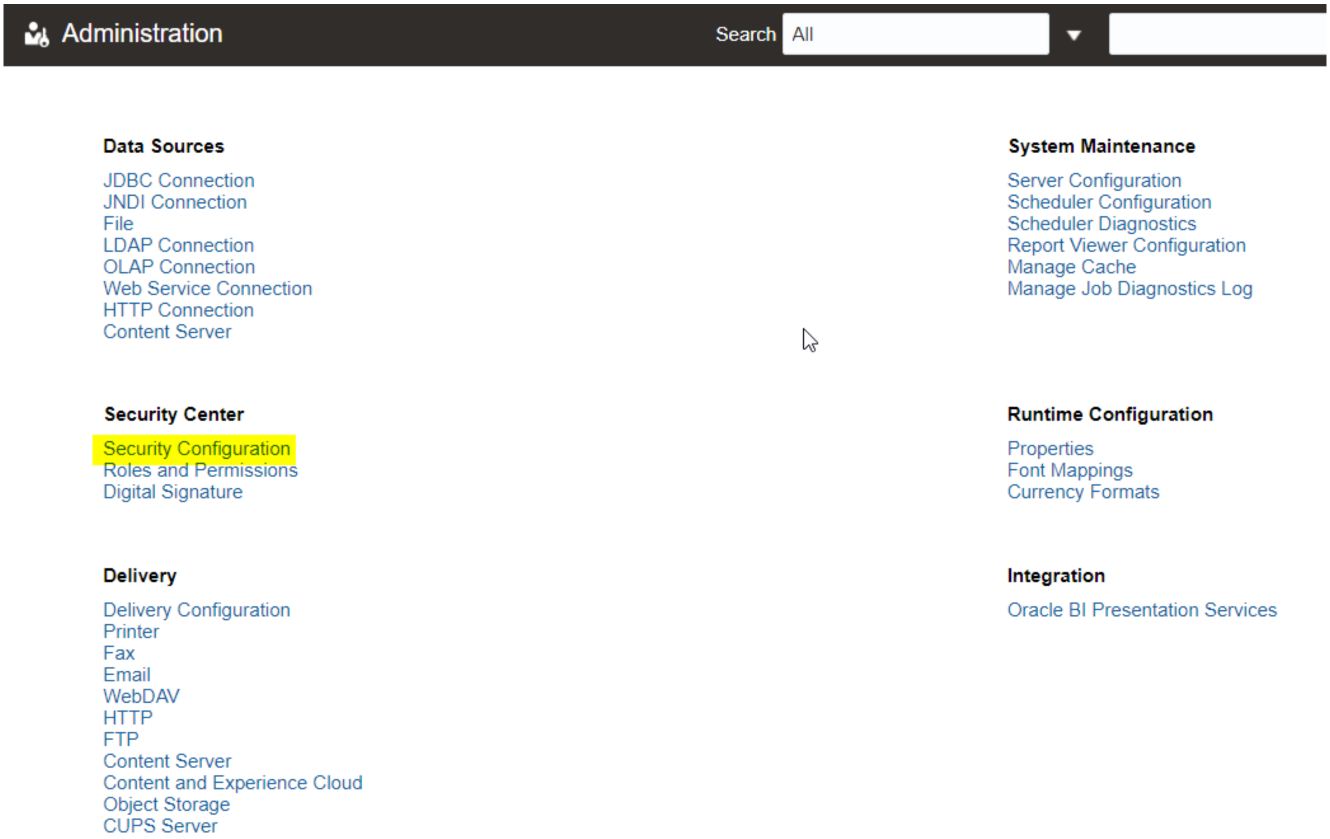


Figure 3. Click on the **Administration** link underneath **My Account**

Step 3 - Security Configuration (located under Security Center)

After the Administration link is pressed, the Administration screen below should be shown.

- Underneath the Security Center label, choose Security Configuration.



Data Sources

JDBC Connection
JNDI Connection
File
LDAP Connection
OLAP Connection
Web Service Connection
HTTP Connection
Content Server

System Maintenance

Server Configuration
Scheduler Configuration
Scheduler Diagnostics
Report Viewer Configuration
Manage Cache
Manage Job Diagnostics Log

Security Center

Security Configuration
Roles and Permissions
Digital Signature

Runtime Configuration

Properties
Font Mappings
Currency Formats

Delivery

Delivery Configuration
Printer
Fax
Email
WebDAV
HTTP
FTP
Content Server
Content and Experience Cloud
Object Storage
CUPS Server

Integration

Oracle BI Presentation Services

Figure 4. Administration Screens and Security Center. Needed for Security Configuration

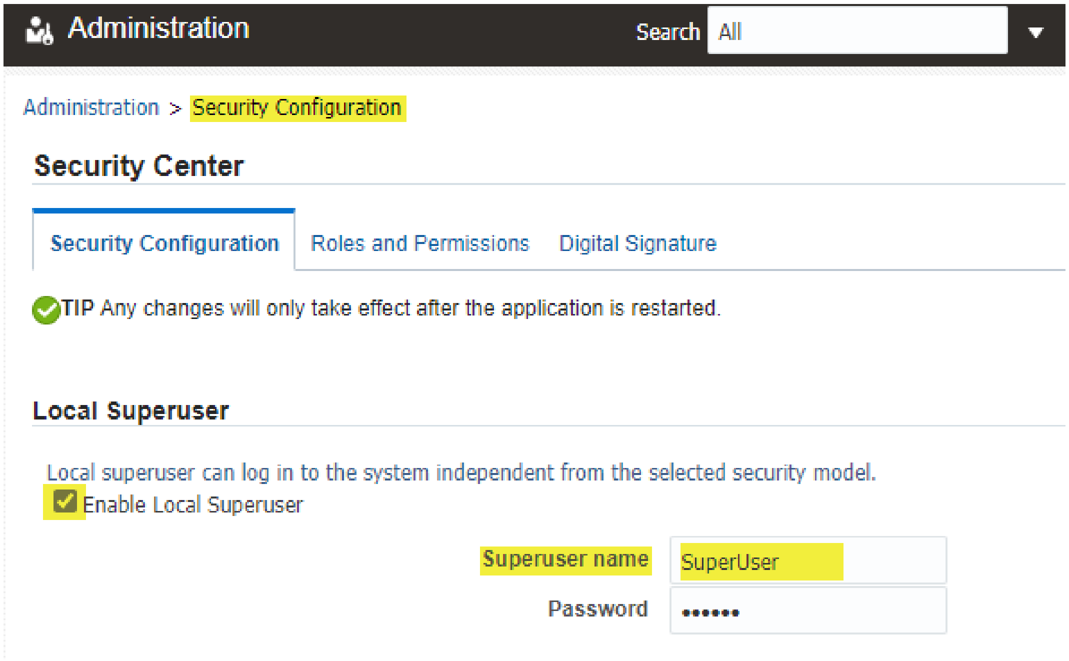
Step 4 - Enable the local Superuser

Due to the complexities associated with these steps, and the possibility of accidentally locking yourself out of OAS, it is highly recommended to temporarily enable the local SuperUser:

This *special* account is not designed to be utilized for running or scheduling reports, but only to administer OAS.

Proceed with these steps to enable this *special* account:

- Click the check-box next to **Enable Local Superuser**.
- Enter a username and password, for example:
  - User: SuperUser
  - Password: ●●●●●●●●●



Administration Search All

Administration > Security Configuration

Security Center

Security Configuration | Roles and Permissions | Digital Signature

✓TIP Any changes will only take effect after the application is restarted.

Local Superuser

Local superuser can log in to the system independent from the selected security model.

☑ Enable Local Superuser

Superuser name: SuperUser

Password: ••••••

Figure 5. Enable local **Superuser**

Step 5 – Configuring the OAS Database Security Model

Configuration settings for the OAS Database Security Model are somewhat error prone.

- Detailed instructions follow and can be found in the standard OAS documentation set.[14]

Step 5, Part 1 - Determining the proper value for the JDBC Simple Connect Descriptor

It can be challenging to enter the correct syntax for the Simple connect string. [15]

The definitive reference for the JDBC Connection String can be found here:

Oracle® Database JDBC Developer's Guide 23ai

F47013-14

October 2024

The salient details are contained in this chapter:

- 8.2 Database URLs and Database Specifiers

'Appendix E - Details on the JDBC Simple Connect ' provides additional insights and pointers.

A trivial example is shown below:

```
jdbc:oracle:thin:@emrepos.example.com:1521/orclpdb.example.com
```

Step 5, Part 2 - Determining the Administrator Username and Password

The Administrator username and password are straightforward. They are simply '**sysman'** and the sysman password.

Step 5, Part 3 - Example values

Security Model:	**`Oracle Database`**
Connection String:	`jdbc:oracle:thin:@//emrepos.example.com:1521:orclpdb.example.com`
Administrator Username:	**`sysman`**
Administrator Password:	●●●●●●
Database Driver Class:	`oracle.jdbc.driver.OracleDriver`

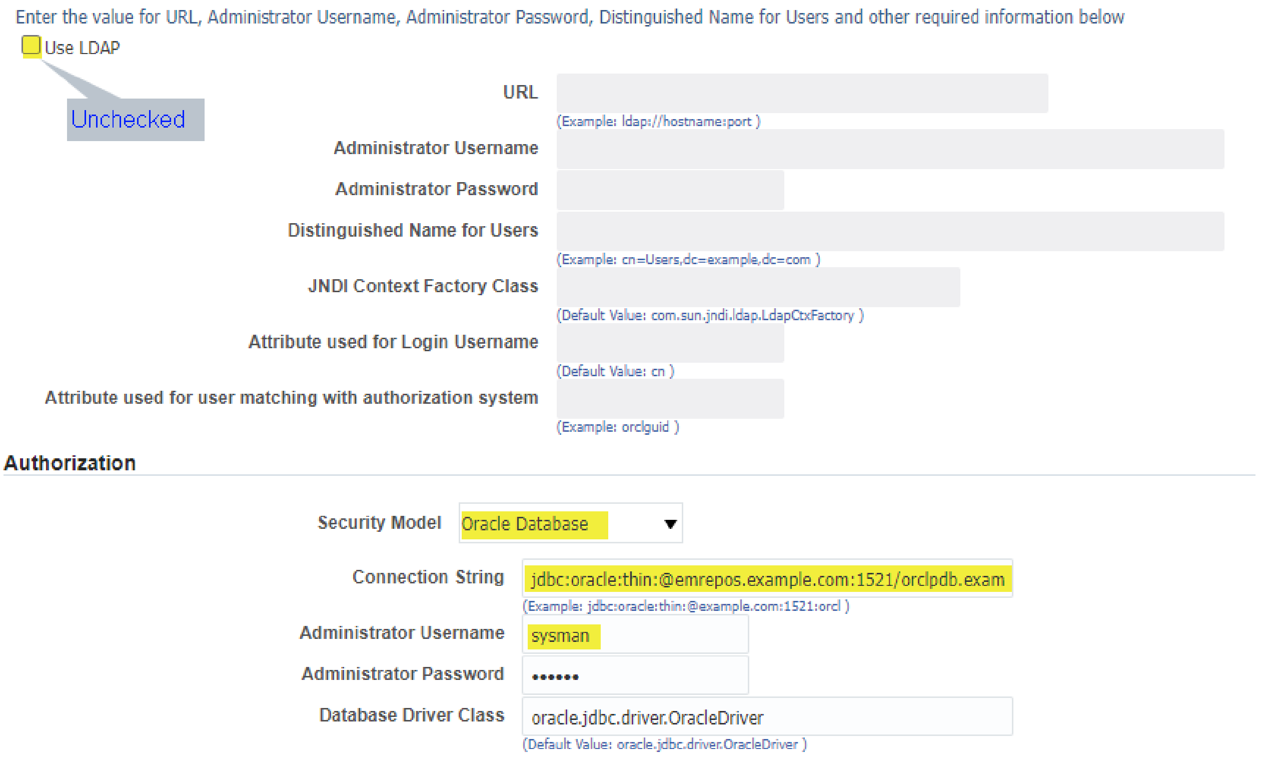
[14] Integrate with Oracle Database Security

[15] Configuring the Oracle Analytics Server Domain with the Configuration Assistant

Step 6 - Setting the OAS Security Model to “Oracle Database”

Scroll down to the Authorization section and fill in the appropriate fields.

- Make sure that ‘Use LDAP’ is not checked.
- Make sure that the Security Model is set to Oracle Database
- Fill in the appropriate connect descriptor for the Enterprise Manager Repository DBMS.
- Ensure to provide the sysman credentials.



Enter the value for URL, Administrator Username, Administrator Password, Distinguished Name for Users and other required information below

□ Use LDAP

URL: (Example: ldap://hostname:port)

Administrator Username

Administrator Password

Distinguished Name for Users: (Example: cn=Users,dc=example,dc=com)

JNDI Context Factory Class: (Default Value: com.sun.jndi.ldap.LdapCtxFactory)

Attribute used for Login Username: (Default Value: cn)

Attribute used for user matching with authorization system: (Example: orclguid)

Authorization

Security Model: Oracle Database

Connection String: jdbc:oracle:thin:@emrepos.example.com:1521/orclpdb.exam

(Example: jdbc:oracle:thin:@example.com:1521:orcl)

Administrator Username: sysman

Administrator Password: ••••••

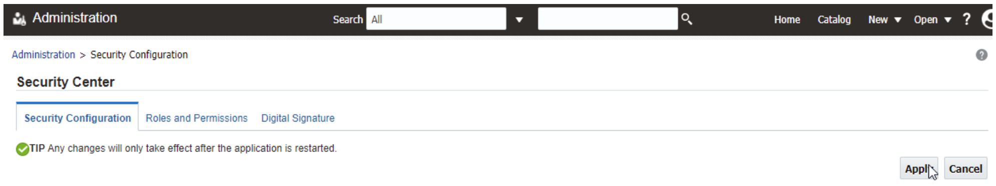
Database Driver Class: oracle.jdbc.driver.OracleDriver

(Default Value: oracle.jdbc.driver.OracleDriver)

Figure 6. Configure OAS for **Oracle Database** Security Model

*NOTE: The database connection string and credentials are for the **EM Repository** database, and **not** for the OAS database.*

Step 7 - Hit apply



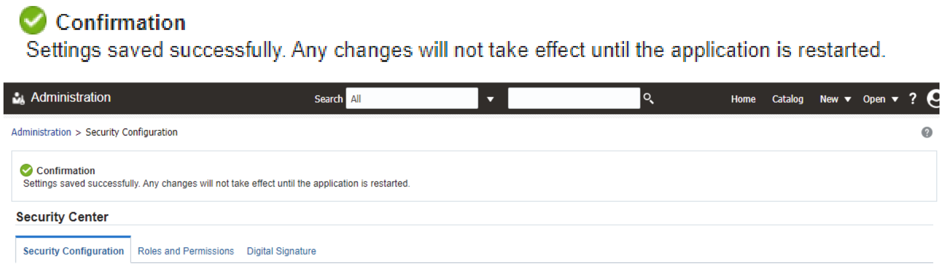
Administration > Security Configuration

Security Center

TIP Any changes will only take effect after the application is restarted.

Figure 7. Apply Security Model Changes

Step 8 - Notice that a restart of the application is required



Confirmation

Settings saved successfully. Any changes will not take effect until the application is restarted.

Administration > Security Configuration

Confirmation

Settings saved successfully. Any changes will not take effect until the application is restarted.

Security Center

Figure 8. Required Restart of OAS

Step 9 - Shutdown OAS

Use the instructions in Appendix C - Stopping the full OAS stack.

Step 10 - Startup OAS

Use the instructions Appendix B - Starting the full OAS stack.

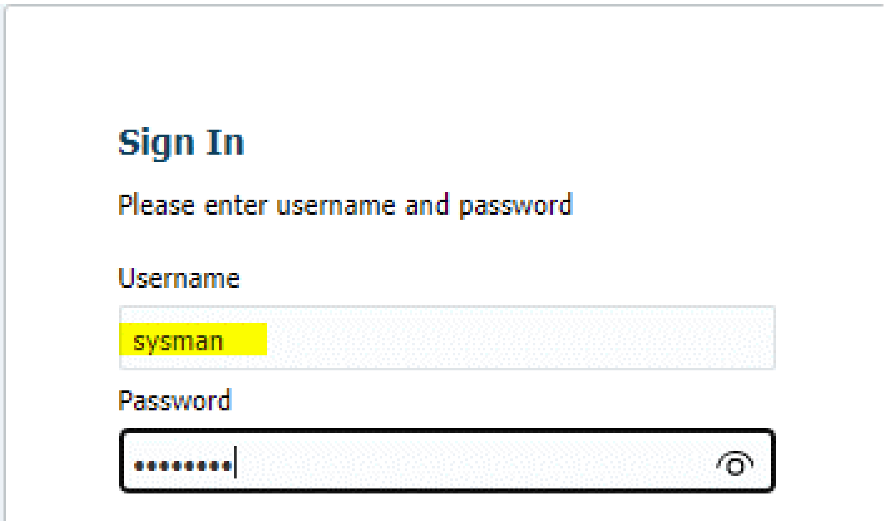
Step 11 - Monitor the bipublisher.log file for errors

In case the connect descriptor was entered incorrectly, monitor the bipublisher.log during the startup process.

```
$ cd $MW_HOME/user_projects/domains/bi/servers/bi_server1/logs
$ tail -f bi_server1.outXXXX
...
...
java.sql.SQLRecoverableException: Listener refused the connection with the following error:
ORA-12514, TNS:listener does not currently know of service requested in connect descriptor

        at oracle.jdbc.driver.T4CConnection.logon(T4CConnection.java:855) ...
        at oracle.xdo.security.OraValidator.validate(OraValidator.java:117) ...
        at oracle.xdo.servlet.security.ORCLDBSecurityHandler...
        at oracle.xdo.servlet.security.ORCLDBSecurityHandler.getPrincipal ...
...
...
```

Step 12 – Confirm success

If no errors are encountered, you can proceed to login to OAS using the SYSMAN account and credentials.



Sign In

Please enter username and password

Username

sysman

Password

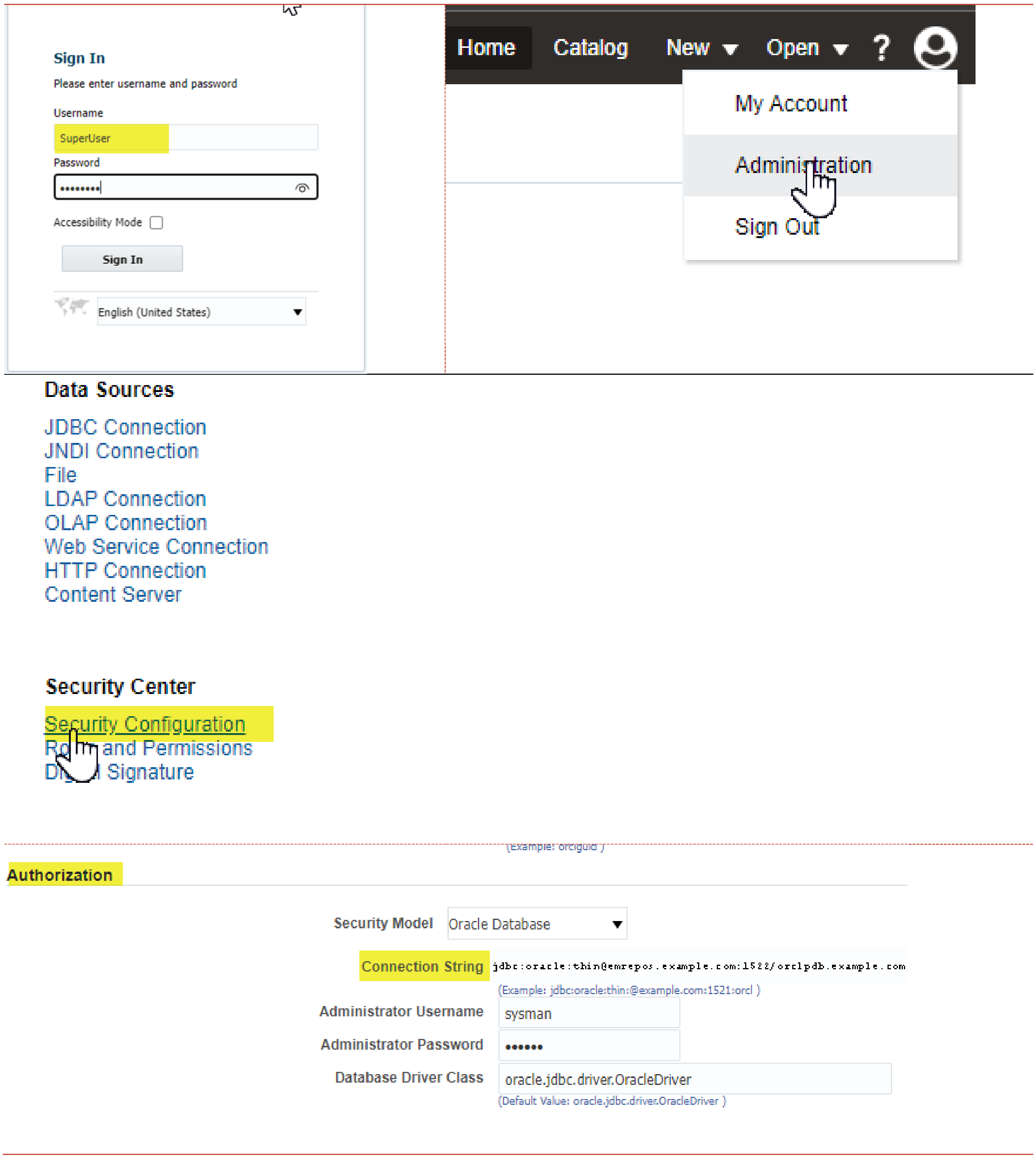
••••••••

Figure 9. Login to OAS as the SYSMAN User

Resolving issues logging into OAS after making the above changes

If you are unable to login to OAS as the SYSMAN user above, you can utilize the temporary SuperUser account we created to login and resolve the issue.

Here are few screen shots outlining this procedure.



Username: SuperUser

Password: ••••••••

Security Model: Oracle Database

Connection String: jdbc:oracle:thin@emrepos.example.com:1522/orclpdb.example.com

(Example: jdbc:oracle:thin:@example.com:1521:orcl)

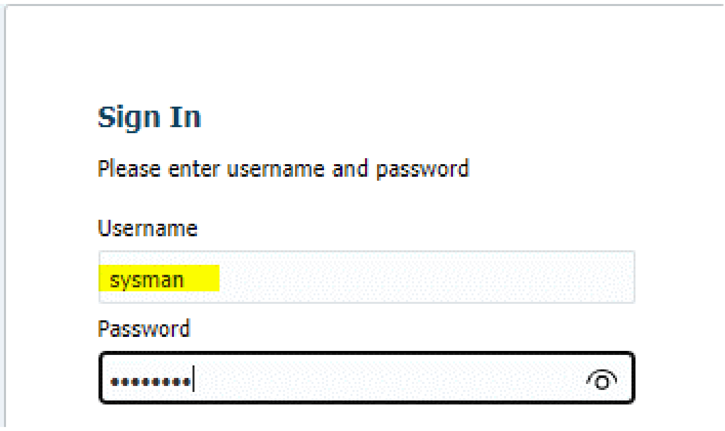
Administrator Username: sysman

Administrator Password: ••••••

Database Driver Class: oracle.jdbc.driver.OracleDriver

(Default Value: oracle.jdbc.driver.OracleDriver)

Confirm the correct OAS Group Assignments



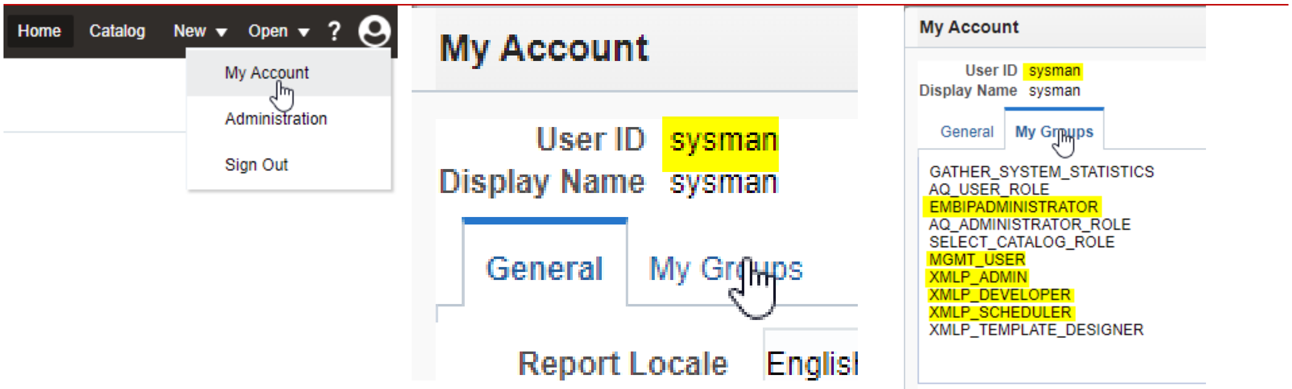
Sign In

Please enter username and password

Username: sysman

Password: ••••••••

Figure 10. Login to OAS as the SYSMAN User



My Account

User ID sysman

Display Name sysman

GATHER_SYSTEM_STATISTICS
AQ_USER_ROLE
EMBIPADMINISTRATOR
AQ_ADMINISTRATOR_ROLE
SELECT_CATALOG_ROLE
MGMT_USER
XMLP_ADMIN
XMLP_DEVELOPER
XMLP_SCHEDULER
XMLP_TEMPLATE_DESIGNER

Figure 11. Confirm Database Security Model

Proceed to next steps in the guide

Once all the steps in this chapter are completed, proceed to Chapter 6 - Configuration of required OAS Datasource(s).

CHAPTER 5. OAS LDAP CONFIGURATION – ENTERPRISE MANAGER PARITY

As discussed earlier, the standalone OAS is to be configured either using OAS Database Security Model or the OAS Fusion Middleware Security Model.

This chapter details the steps for the Fusion Middleware Security Model.

If utilizing the OAS Database Security Model, and chapter 10 has been completed successfully, skip to 'chapter Chapter 6 - Configuration of required OAS Datasource(s)'. Otherwise, continue with this chapter.

If Enterprise Manager is configured with LDAP alone, or LDAP along with Single Sign-on, the steps in this chapter are a required step to for the OAS configuration to match the Enterprise Manager configuration.

For this configuration of EM, the default OAS '**Fusion Middleware Security Model**' is utilized.

There are five steps to achieve this required configuration for OAS. These three steps are required whether OAS is to be configured with Single Sign-on (SSO) or not.

1. Configure the OAS Security Model:
   - Utilizing the OAS Administration screens.
   - requires either the **SYSMAN**, **weblogic**, or **SuperUser** credentials, as appropriate for the existing OAS Security Model).

2. Configure the OAS WebLogic Domain:
   - Utilizing the WebLogic console UI.
   - Requires the **weblogic** credentials.

3. Configure the OAS WebLogic Domain's Java Platform Services (JPS):
   - Utilizing the command-line.
   - Requires Operating System privileges to the OAS WebLogic domain's filesystem.

4. Stop and then start the complete OAS WebLogic domain.

5. Grant OAS Fusion Middleware Application roles to EM LDAP Users and/or LDAP Groups:
   - Utilizing Fusion Middleware Control.
   - Requires the **weblogic** user's credentials.

5.1 OAS Security Model Configuration – OAS Administration Steps

- Due to possible user errors locking out access to OAS, a fallback '**Super User**' is highly recommended.

Step 1 - Login to OAS

- For first time configuration, login to OAS as the **weblogic** user.
- If OAS is already configured for the 'Database Security Model', login as an Enterprise Manager Super Administrator, for example 'SYSMAN'.
- If neither of these logins are possible, and the instructions to setup a local SuperUser were followed, login as this local 'SuperUser'

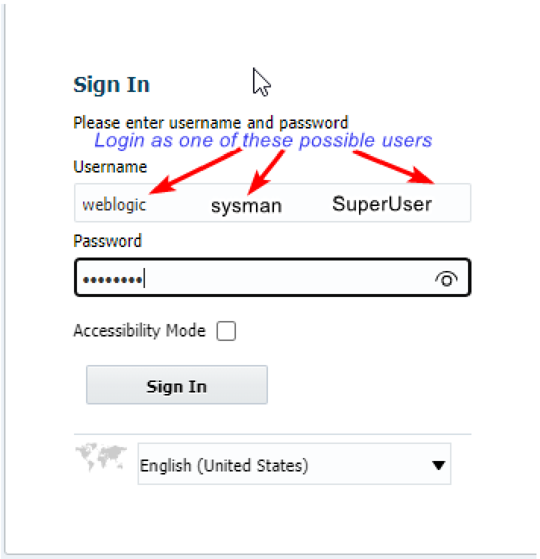
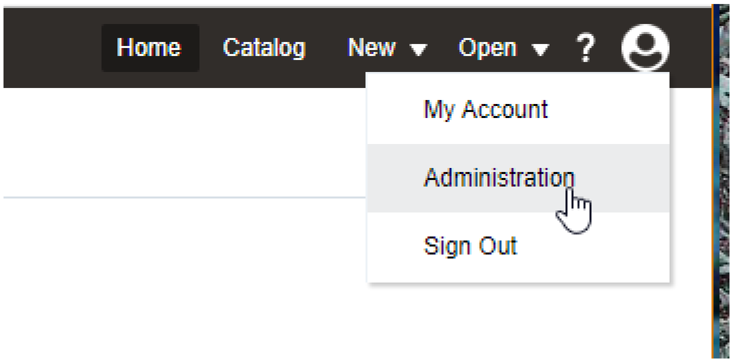


Figure 12. Login to OAS as the **weblogic** user (or local **superuser)**

Step 2 - Click on the Administration link underneath My Account

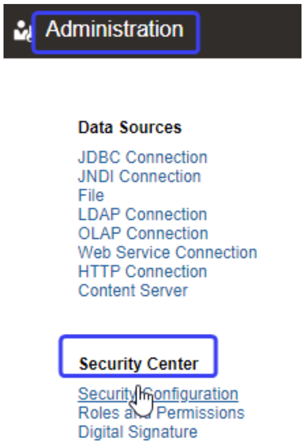
Towards the top right-hand section of the OAS user interface, above the **Open** link, and to the left of the **Help** link, click on the **Administration** link.



Step 3 - Security Configuration (located under Security Center)

After the **Administration** link is pressed, the **Administration** screen below should be shown.

- Underneath the Security Center label, choose Security Configuration.



Administration

Data Sources

JDBC Connection
JNDI Connection
File
LDAP Connection
OLAP Connection
Web Service Connection
HTTP Connection
Content Server

Security Center

Security Configuration
Roles and Permissions
Digital Signature

Figure 13. Administration Screens and Security Center. Needed for Security Configuration

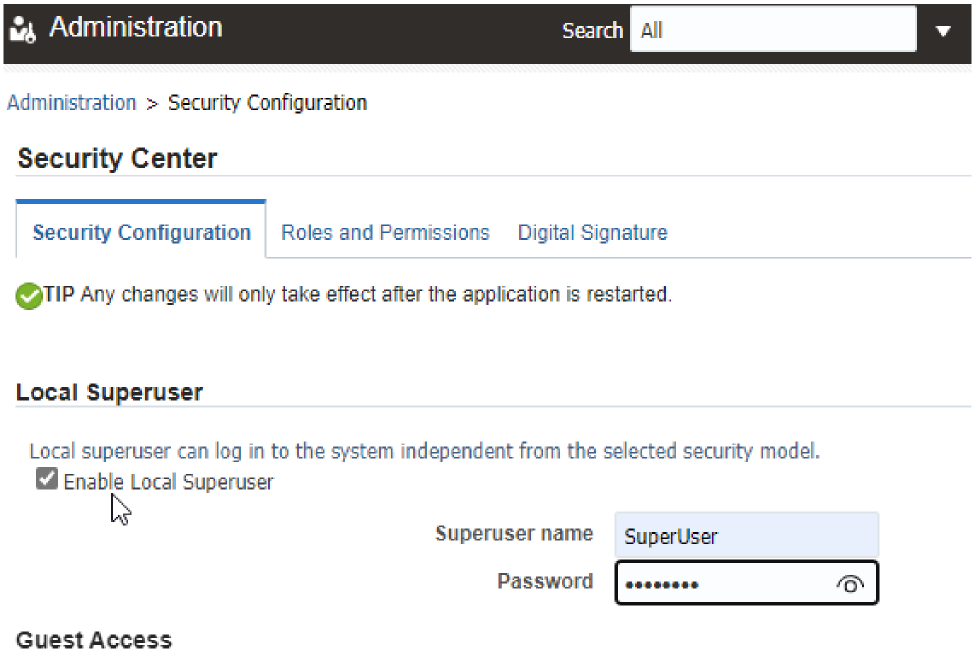
Step 4 - Enable the local SuperUser

Due to the complexities associated with these steps, and the possibility of accidentally locking yourself out of OAS, it is highly recommended to temporarily enable the local SuperUser:

- This *special* account is not designed to be utilized for running or scheduling reports, but only to administer OAS.

Proceed with these steps to enable this *special* account:

- Click the check-box next to **Enable Local Superuser**.
- Enter a username and password, for example:
  - User: SuperUser
  - Password: ●●●●●●



Administration Search All

Administration > Security Configuration

Security Center

Security Configuration | Roles and Permissions | Digital Signature

TIP Any changes will only take effect after the application is restarted.

Local Superuser

Local superuser can log in to the system independent from the selected security model.

☑ Enable Local Superuser

Superuser name: SuperUser

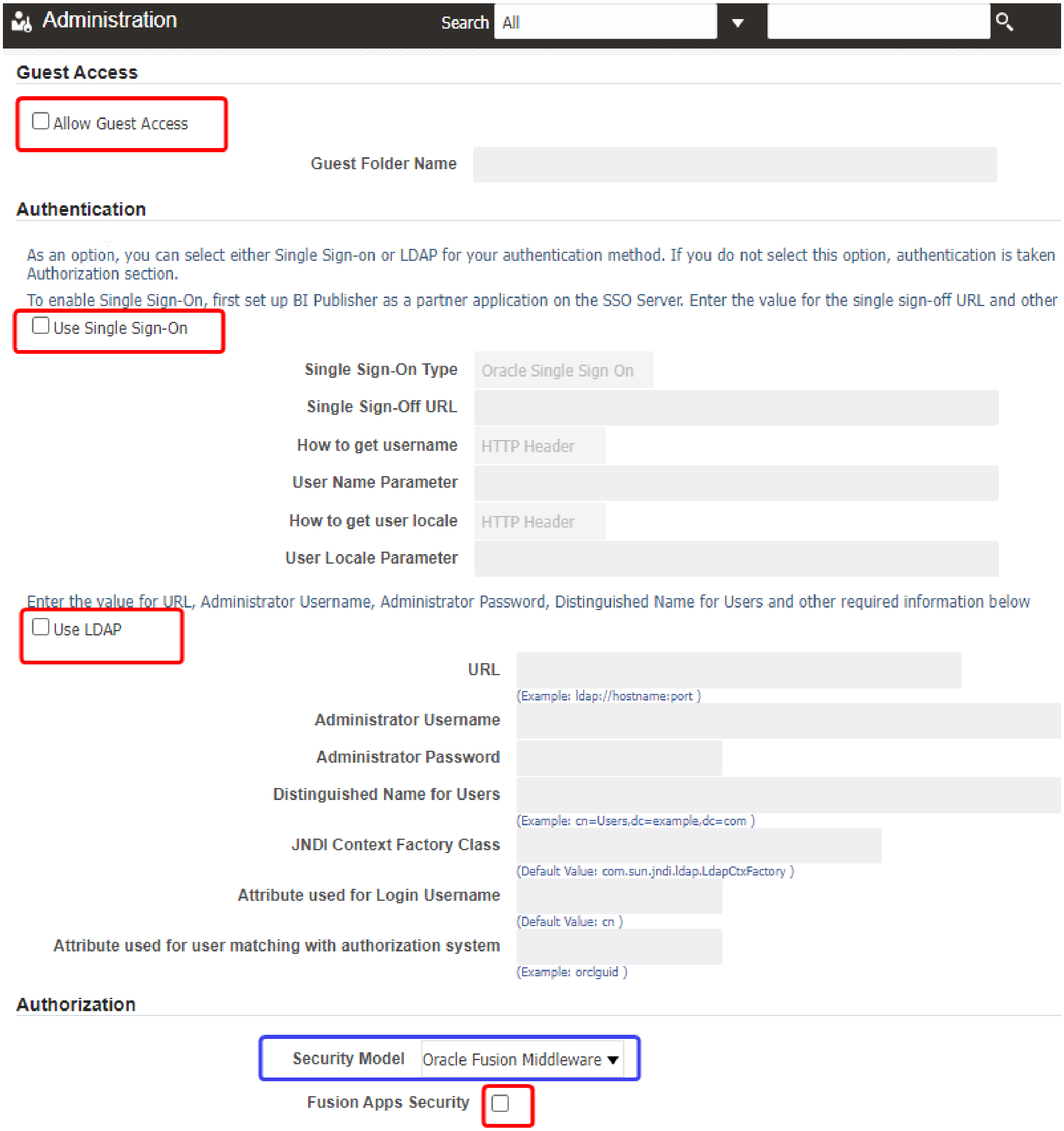
Password: ••••••••

Guest Access

Figure 14. Enable local **Superuser**

Step 5- Confirm correct configuration of ‘Fusion Middleware Security Model’

- For the first LDAP configuration, without Single Sign-On, make sure that **Use Single Sign-On** is <u>not</u> checked.
  - For subsequent configuration of Single Sign-on, the steps are outlined in ‘**Error! Reference source not f ound. - Error! Reference source not found.**’.
  - LDAP configuration is a pre-requisite for Single Sign-On, but do not set that option at this stage.
- Make sure that 'Allow Guest Access' is <u>not</u> checked.
- Make sure that 'Use Single Sign-On' is <u>not</u> checked.
- Make sure that 'Use LDAP' is <u>not</u> checked.
- Make sure that the 'Security Model' <u>is set to</u> Oracle Fusion Middleware.
- Make that 'Fusion Apps Security' is <u>not</u> checked.



Guest Access

☐ Allow Guest Access

Guest Folder Name

Authentication

As an option, you can select either Single Sign-on or LDAP for your authentication method. If you do not select this option, authentication is taken Authorization section.

To enable Single Sign-On, first set up BI Publisher as a partner application on the SSO Server. Enter the value for the single sign-off URL and other

☐ Use Single Sign-On

Single Sign-On Type: Oracle Single Sign On
Single Sign-Off URL
How to get username: HTTP Header
User Name Parameter
How to get user locale: HTTP Header
User Locale Parameter

Enter the value for URL, Administrator Username, Administrator Password, Distinguished Name for Users and other required information below

☐ Use LDAP

URL
(Example: ldap://hostname:port)
Administrator Username
Administrator Password
Distinguished Name for Users
(Example: cn=Users,dc=example,dc=com)
JNDI Context Factory Class
(Default Value: com.sun.jndi.ldap.LdapCtxFactory)
Attribute used for Login Username
(Default Value: cn)
Attribute used for user matching with authorization system
(Example: orclguid)

Authorization

Security Model: Oracle Fusion Middleware ▾
Fusion Apps Security ☐

Figure 15. Ensure that **Oracle Fusion Middleware** Security Model is configured correctly.

5.2 OAS WebLogic Domain Configuration – Using the WebLogic Console UI

The overall goal of these sections is to configure the OAS WebLogic domain's Security Configuration in such a way that it is functionally identical to Enterprise Manager's WebLogic domain Security Configuration.

Approved Fusion MiddleWare Tools

Throughout the rest of these sections, all examples will utilize the below WebLogic tools.

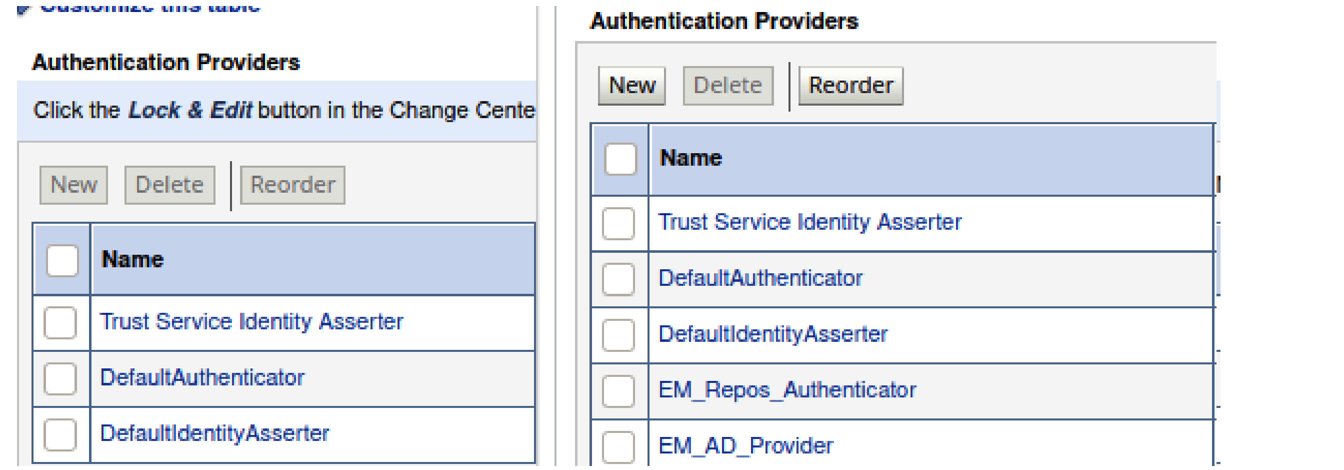
- WebLogic Console
- Fusion Middleware Control

The easiest approach for implementing the screenshots on the following pages is to bring up the WebLogic console for the EM domain side-by-side with the OAS WebLogic domain.

Due to certain limitations in the WebLogic console's user interface, it is necessary to utilize two separate browser sessions.

Once **Steps 1** through **step 7** are complete, you will see screens similar to what is shown in one of the below:

- Figure 16-Comparison of WebLogic Security Configurations – Oracle Internet Directory
- Figure 17-Comparison of WebLogic Security Configuration – Microsoft Active Directory



Authentication Providers

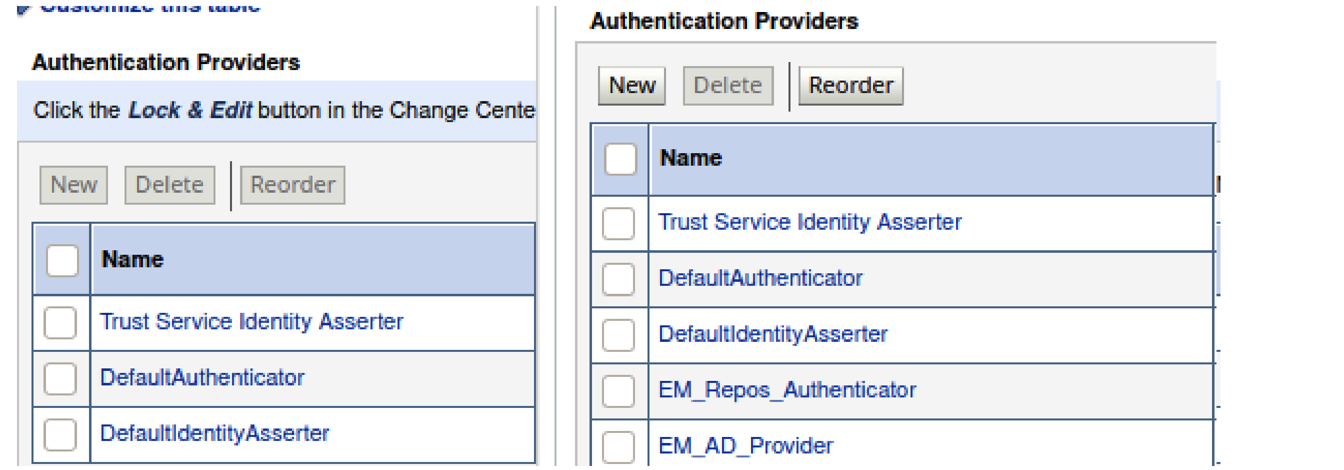
Click the *Lock & Edit* button in the Change Cente

□	Name
□	Trust Service Identity Asserter
□	DefaultAuthenticator
□	DefaultIdentityAsserter

Authentication Providers

□	Name
□	Trust Service Identity Asserter
□	DefaultAuthenticator
□	DefaultIdentityAsserter
□	EM_Repos_Authenticator
□	EM_AD_Provider

Figure 16. Comparison of WebLogic Security Configurations – Oracle Internet Directory



Authentication Providers

Click the *Lock & Edit* button in the Change Cente

□	Name
□	Trust Service Identity Asserter
□	DefaultAuthenticator
□	DefaultIdentityAsserter

Authentication Providers

□	Name
□	Trust Service Identity Asserter
□	DefaultAuthenticator
□	DefaultIdentityAsserter
□	EM_Repos_Authenticator
□	EM_AD_Provider

Figure 17. Comparison of WebLogic Security Configuration – Microsoft Active Directory

There are a total of 7 steps to accomplish parity between OAS and EM

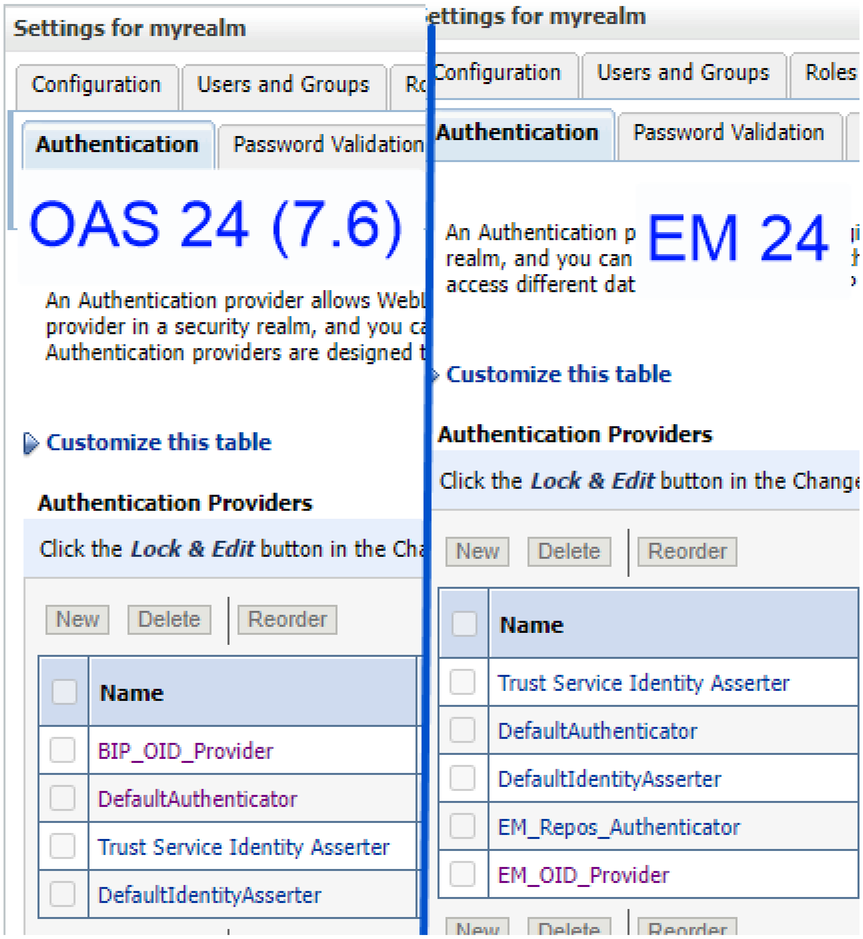
Step 1 - For each WebLogic console, Navigate to the Authentication Providers Screen

1. Login to the WebLogic console as the weblogic user (remember, for both OAS and EM).
2. On the left-hand side of the browser window, underneath the Domain Structure, click on the link for **Security Realms**.
3. There should just be one realm, named **myrealm**.
4. Click on **myrealm**.
5. Click on the tab for **Providers**.
6. For the OAS WebLogic Domain only:
   – In the top left-hand corner of the UI, click on **Lock & Edit**.

Step 2 – Configure a new WebLogic Provider (for OAS only)

1. Click on the **New** button.
2. In the text box for the Name: field, choose a name as appropriate:
3. **BIP_OID_Provider** or **BIP_AD_Provider**
4. In the drop-down for the Type: field, scroll down, and choose as appropriate:
5. **OracleInternetDirectoryAuthenticator** or **ActiveDirectoryAuthenticator**
6. Click on the **OK** button.

Step 3 – Confirm correct ordering of providers



An Authentication provider allows Webl
provider in a security realm, and you ca
Authentication providers are designed t

Click the *Lock & Edit* button in the Cha

□	Name
□	BIP_OID_Provider
□	DefaultAuthenticator
□	Trust Service Identity Asserter
□	DefaultIdentityAsserter

An Authentication p
realm, and you can
access different dat

Click the *Lock & Edit* button in the Change

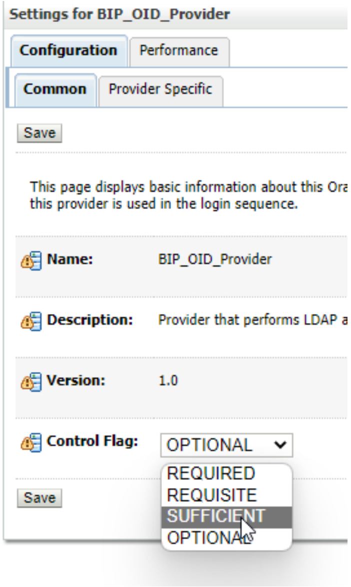
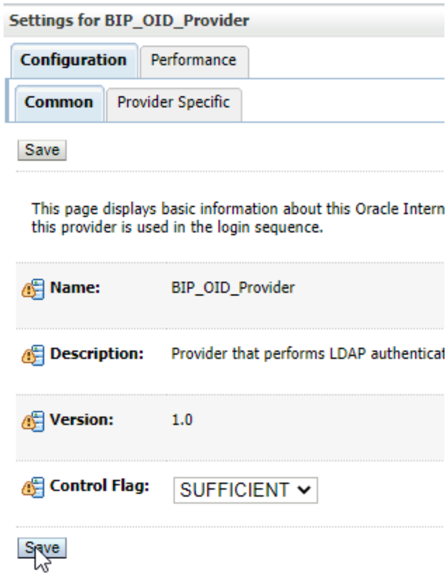
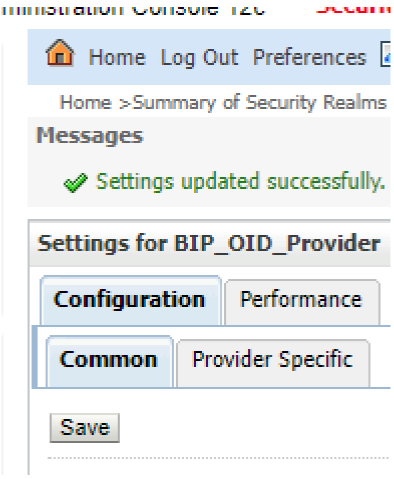
□	Name
□	Trust Service Identity Asserter
□	DefaultAuthenticator
□	DefaultIdentityAsserter
□	EM_Repos_Authenticator
□	EM_OID_Provider

Figure 18. Correct order of WebLogic Authentication Providers – Oracle Access Manager (SSO) with OID

Step 4 – Change the OID Provider to SUFFICIENT

By default, both the BIP_OID_Provider and the BIP_AD_Provider are configured as OPTIONAL, with the WebLogic defaults.

Click on the appropriate provider (BIP_OID_Provider or BIP_AD_Provider) and then change the provider to be SUFFICIENT.

Step 4a – Change to Sufficient	Step 4b – Click Save	Step 4c - Confirmation
 Settings for BIP_OID_Provider Configuration / Performance Common / Provider Specific Save This page displays basic information about this Ora this provider is used in the login sequence. Name: BIP_OID_Provider Description: Provider that performs LDAP a Version: 1.0 Control Flag: OPTIONAL REQUIRED REQUISITE SUFFICIENT OPTIONAL Save	 Settings for BIP_OID_Provider Configuration / Performance Common / Provider Specific Save This page displays basic information about this Oracle Intern this provider is used in the login sequence. Name: BIP_OID_Provider Description: Provider that performs LDAP authenticat Version: 1.0 Control Flag: SUFFICIENT Save	 inistration Console 12c Home Log Out Preferences Home >Summary of Security Realms Messages ✓ Settings updated successfully. Settings for BIP_OID_Provider Configuration / Performance Common / Provider Specific Save

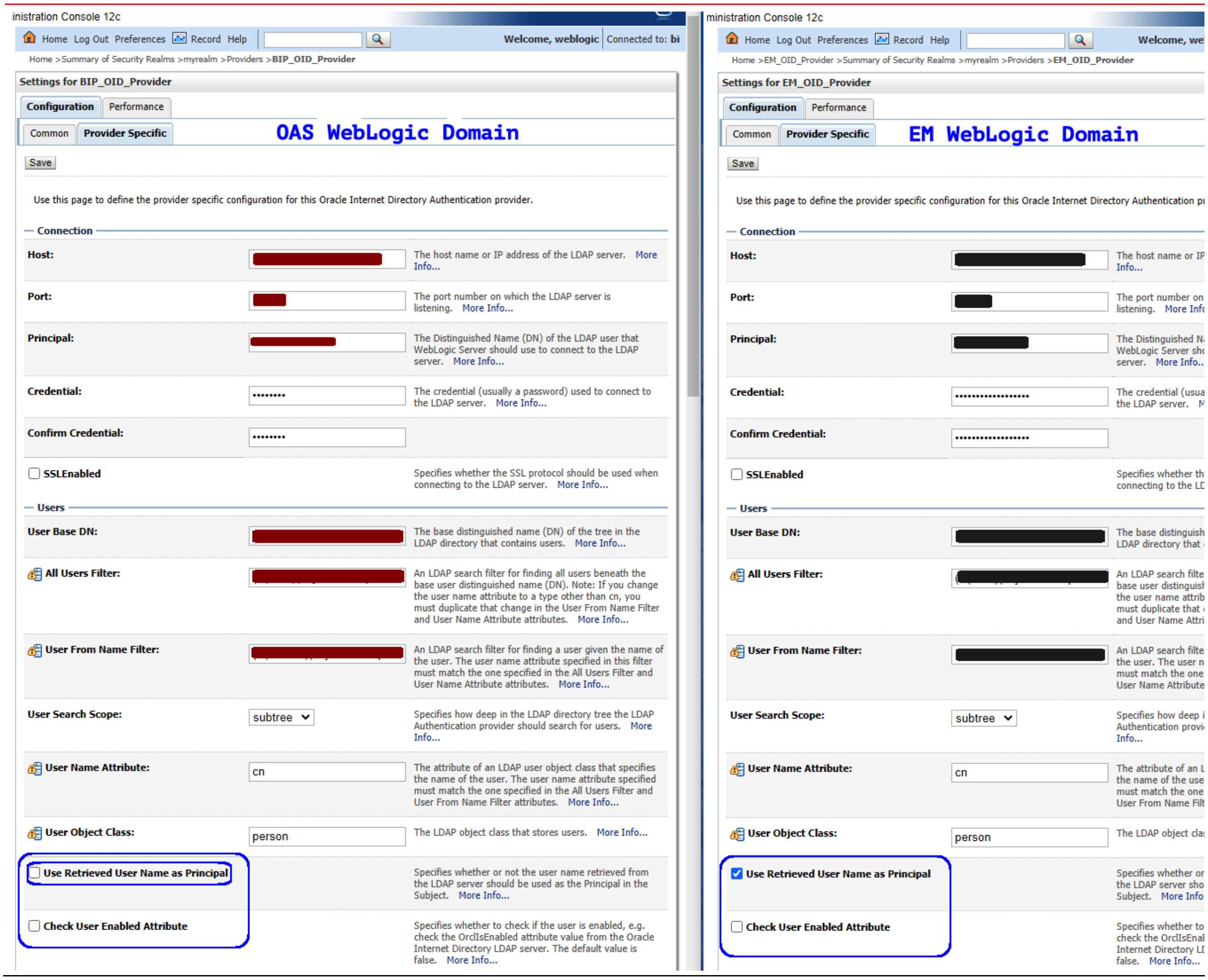
Step 5 – Configure OID Provider for OAS WebLogic Domain

The next step is to configure the OID Provider for OAS WebLogic Domain to match EM's WebLogic Domain.

The procedure will be to copy entries from the values used for the the EM WebLogic Domain) to the OAS WebLogic Domain.

Step 5 – Screen Section 1

- Provide the **Hostname** of the common LDAP server to be shared between EM and OAS.
- Provide the same **port** for OAS as EM is using.
- Provide same **principal** for OAS as EM is using.
- Provide same **credential** for OAS as EM is using.
- Copy/Paste the following items from EM to OAS:
  - **User Base DN**
  - **All Users Filter**
  - **Users** from Name Filter
  - Ensure to select Use **Retrieved Username as Principal**



inistration Console 12c

Home Log Out Preferences Record Help Welcome, weblogic Connected to: bi

Home >Summary of Security Realms >myrealm >Providers >BIP_OID_Provider

Settings for BIP_OID_Provider

Configuration | Performance

Common | Provider Specific

OAS WebLogic Domain

Save

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.

Connection

Host:	[redacted]	The host name or IP address of the LDAP server. More Info...
Port:	[redacted]	The port number on which the LDAP server is listening. More Info...
Principal:	[redacted]	The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. More Info...
Credential:	••••••••	The credential (usually a password) used to connect to the LDAP server. More Info...
Confirm Credential:	••••••••	
☐ SSLEnabled		Specifies whether the SSL protocol should be used when connecting to the LDAP server. More Info...

Users

User Base DN:	[redacted]	The base distinguished name (DN) of the tree in the LDAP directory that contains users. More Info...
All Users Filter:	[redacted]	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:	[redacted]	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:	cn	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...
User Object Class:	person	The LDAP object class that stores users. More Info...
☐ 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. More Info...
☐ Check User Enabled Attribute		Specifies whether to check if the user is enabled, e.g. check the OrclIsEnabled attribute value from the Oracle Internet Directory LDAP server. The default value is false. More Info...

ministration Console 12c

Home Log Out Preferences Record Help Welcome, we

Home >EM_OID_Provider >Summary of Security Realms >myrealm >Providers >EM_OID_Provider

Settings for EM_OID_Provider

Configuration | Performance

Common | Provider Specific

EM WebLogic Domain

Save

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication pi

Connection

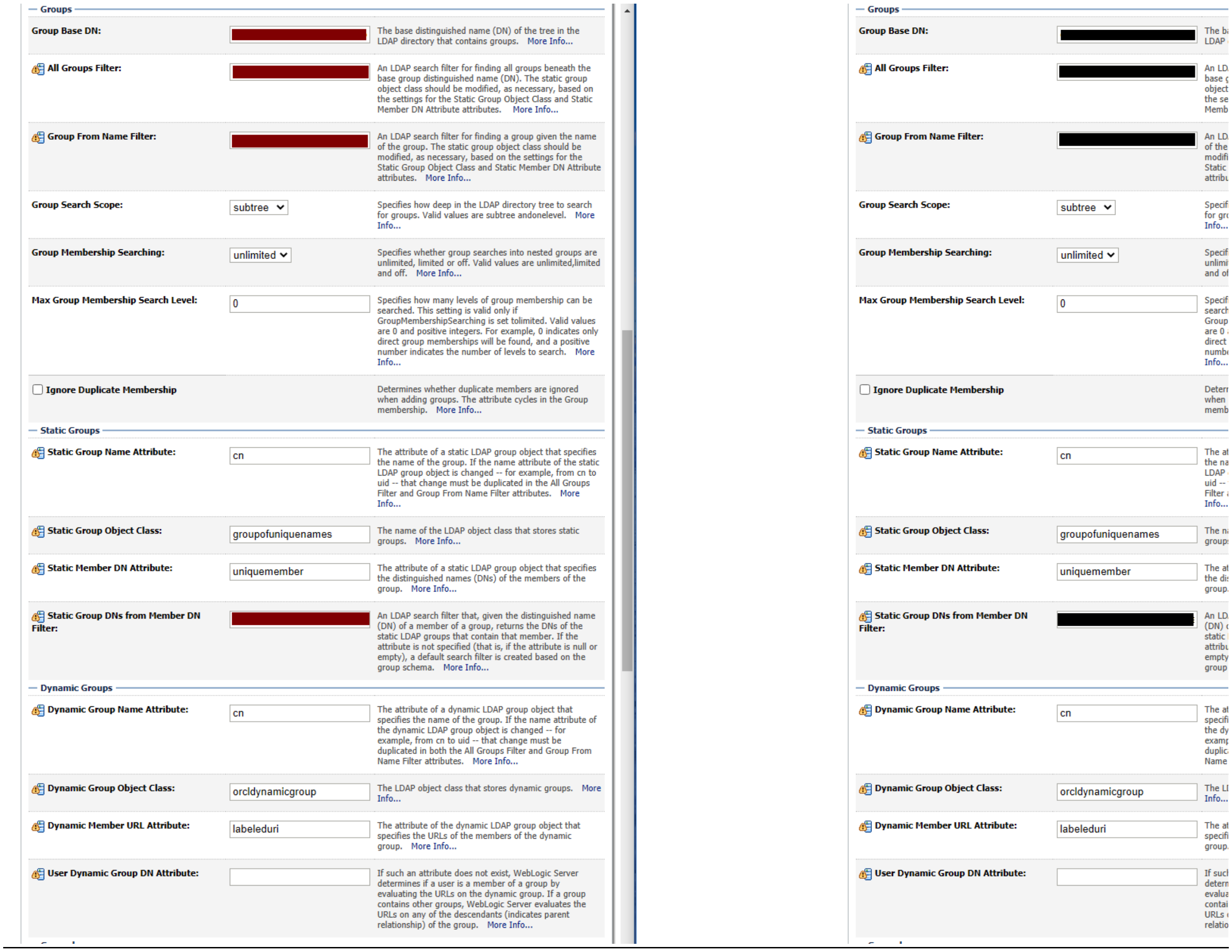
Host:	[redacted]	The host name or IP Info...
Port:	[redacted]	The port number on listening. More Info
Principal:	[redacted]	The Distinguished N WebLogic Server sho server. More Info..
Credential:	••••••••••••••••••	The credential (usua the LDAP server. M
Confirm Credential:	••••••••••••••••••	
☐ SSLEnabled		Specifies whether th connecting to the LD

Users

User Base DN:	[redacted]	The base distinguish LDAP directory that
All Users Filter:	[redacted]	An LDAP search filte base user distinguish the user name attrib must duplicate that and User Name Attri
User From Name Filter:	[redacted]	An LDAP search filte the user. The user n must match the one User Name Attribute
User Search Scope:	subtree	Specifies how deep i Authentication provi Info...
User Name Attribute:	cn	The attribute of an L the name of the use must match the one User From Name Filt
User Object Class:	person	The LDAP object clas
☑ Use Retrieved User Name as Principal		Specifies whether or the LDAP server sho Subject. More Info
☐ Check User Enabled Attribute		Specifies whether to check the OrclIsEnal Internet Directory LI false. More Info...

Step 5 – Screen Section 2

- Copy/Paste the following items from EM to OAS:
  - **Group Base DN**
  - **All Groups Filter**
  - **Group from Name Filter**
  - Copy/**Paste Static Group DNs from Member DN…**



Groups

Group Base DN:	[redacted]	The base distinguished name (DN) of the tree in the LDAP directory that contains groups. More Info...
All Groups Filter:	[redacted]	An LDAP search filter for finding all groups beneath the base group distinguished name (DN). The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group From Name Filter:	[redacted]	An LDAP search filter for finding a group given the name of the group. The static group object class should be modified, as necessary, based on the settings for the Static Group Object Class and Static Member DN Attribute attributes. More Info...
Group Search Scope:	subtree	Specifies how deep in the LDAP directory tree to search for groups. Valid values are subtree andonelevel. More Info...
Group Membership Searching:	unlimited	Specifies whether group searches into nested groups are unlimited, limited or off. Valid values are unlimited,limited and off. More Info...
Max Group Membership Search Level:	0	Specifies how many levels of group membership can be searched. This setting is valid only if GroupMembershipSearching is set tolimited. Valid values are 0 and positive integers. For example, 0 indicates only direct group memberships will be found, and a positive number indicates the number of levels to search. More Info...
☐ **Ignore Duplicate Membership**		Determines whether duplicate members are ignored when adding groups. The attribute cycles in the Group membership. More Info...

Static Groups

Static Group Name Attribute:	cn	The attribute of a static LDAP group object that specifies the name of the group. If the name attribute of the static LDAP group object is changed -- for example, from cn to uid -- that change must be duplicated in the All Groups Filter and Group From Name Filter attributes. More Info...
Static Group Object Class:	groupofuniquenames	The name of the LDAP object class that stores static groups. More Info...
Static Member DN Attribute:	uniquemember	The attribute of a static LDAP group object that specifies the distinguished names (DNs) of the members of the group. More Info...
Static Group DNs from Member DN Filter:	[redacted]	An LDAP search filter that, given the distinguished name (DN) of a member of a group, returns the DNs of the static LDAP groups that contain that member. If the attribute is not specified (that is, if the attribute is null or empty), a default search filter is created based on the group schema. More Info...

Dynamic Groups

Dynamic Group Name Attribute:	cn	The attribute of a dynamic LDAP group object that specifies the name of the group. If the name attribute of the dynamic LDAP group object is changed -- for example, from cn to uid -- that change must be duplicated in both the All Groups Filter and Group From Name Filter attributes. More Info...
Dynamic Group Object Class:	orcldynamicgroup	The LDAP object class that stores dynamic groups. More Info...
Dynamic Member URL Attribute:	labeleduri	The attribute of the dynamic LDAP group object that specifies the URLs of the members of the dynamic group. More Info...
User Dynamic Group DN Attribute:		If such an attribute does not exist, WebLogic Server determines if a user is a member of a group by evaluating the URLs on the dynamic group. If a group contains other groups, WebLogic Server evaluates the URLs on any of the descendants (indicates parent relationship) of the group. More Info...

Groups

Group Base DN:	[redacted]
All Groups Filter:	[redacted]
Group From Name Filter:	[redacted]
Group Search Scope:	subtree
Group Membership Searching:	unlimited
Max Group Membership Search Level:	0
☐ **Ignore Duplicate Membership**	

Static Groups

Static Group Name Attribute:	cn
Static Group Object Class:	groupofuniquenames
Static Member DN Attribute:	uniquemember
Static Group DNs from Member DN Filter:	[redacted]

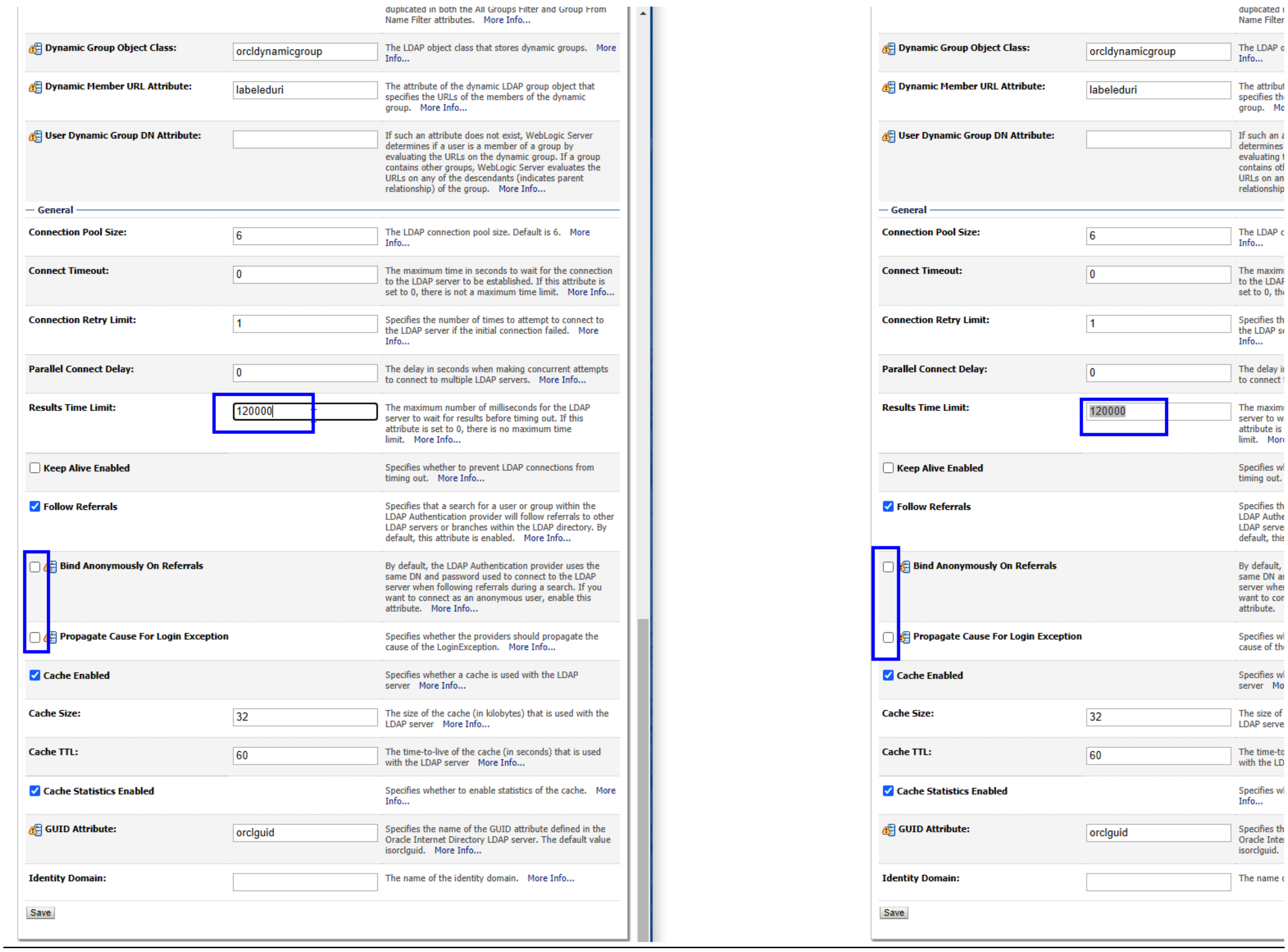
Dynamic Groups

Dynamic Group Name Attribute:	cn
Dynamic Group Object Class:	orcldynamicgroup
Dynamic Member URL Attribute:	labeleduri
User Dynamic Group DN Attribute:	

Step 5 – Screen Section 3

Copy/Paste Results time limit from EM to OAS.

Make sure the radio buttons are not selected.



duplicated in both the All Groups Filter and Group From Name Filter attributes. More Info...

Dynamic Group Object Class:	orcldynamicgroup	The LDAP object class that stores dynamic groups. More Info...
Dynamic Member URL Attribute:	labeleduri	The attribute of the dynamic LDAP group object that specifies the URLs of the members of the dynamic group. More Info...
User Dynamic Group DN Attribute:		If such an attribute does not exist, WebLogic Server determines if a user is a member of a group by evaluating the URLs on the dynamic group. If a group contains other groups, WebLogic Server evaluates the URLs on any of the descendants (indicates parent relationship) of the group. More Info...

— General

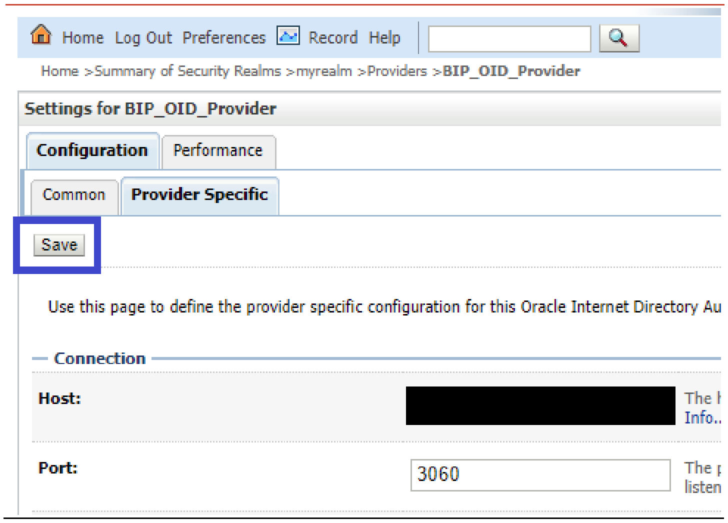
Connection Pool Size:	6	The LDAP connection pool size. Default is 6. More Info...
Connect Timeout:	0	The maximum time in seconds to wait for the connection to the LDAP server to be established. If this attribute is set to 0, there is not a maximum time limit. More Info...
Connection Retry Limit:	1	Specifies the number of times to attempt to connect to the LDAP server if the initial connection failed. More Info...
Parallel Connect Delay:	0	The delay in seconds when making concurrent attempts to connect to multiple LDAP servers. More Info...
Results Time Limit:	120000	The maximum number of milliseconds for the LDAP server to wait for results before timing out. If this attribute is set to 0, there is no maximum time limit. More Info...
□ Keep Alive Enabled		Specifies whether to prevent LDAP connections from timing out. More Info...
☑ Follow Referrals		Specifies that a search for a user or group within the LDAP Authentication provider will follow referrals to other LDAP servers or branches within the LDAP directory. By default, this attribute is enabled. More Info...
□ Bind Anonymously On Referrals		By default, the LDAP Authentication provider uses the same DN and password used to connect to the LDAP server when following referrals during a search. If you want to connect as an anonymous user, enable this attribute. More Info...
□ Propagate Cause For Login Exception		Specifies whether the providers should propagate the cause of the LoginException. More Info...
☑ Cache Enabled		Specifies whether a cache is used with the LDAP server More Info...
Cache Size:	32	The size of the cache (in kilobytes) that is used with the LDAP server More Info...
Cache TTL:	60	The time-to-live of the cache (in seconds) that is used with the LDAP server More Info...
☑ Cache Statistics Enabled		Specifies whether to enable statistics of the cache. More Info...
GUID Attribute:	orclguid	Specifies the name of the GUID attribute defined in the Oracle Internet Directory LDAP server. The default value isorclguid. More Info...
Identity Domain:		The name of the identity domain. More Info...

Save

Dynamic Group Object Class:	orcldynamicgroup
Dynamic Member URL Attribute:	labeleduri
User Dynamic Group DN Attribute:	
Connection Pool Size:	6
Connect Timeout:	0
Connection Retry Limit:	1
Parallel Connect Delay:	0
Results Time Limit:	120000
□ Keep Alive Enabled	
☑ Follow Referrals	
□ Bind Anonymously On Referrals	
□ Propagate Cause For Login Exception	
☑ Cache Enabled	
Cache Size:	32
Cache TTL:	60
☑ Cache Statistics Enabled	
GUID Attribute:	orclguid
Identity Domain:	

Save

Step 8 - Press the Save button



Home >Summary of Security Realms >myrealm >Providers >**BIP_OID_Provider**

Settings for BIP_OID_Provider

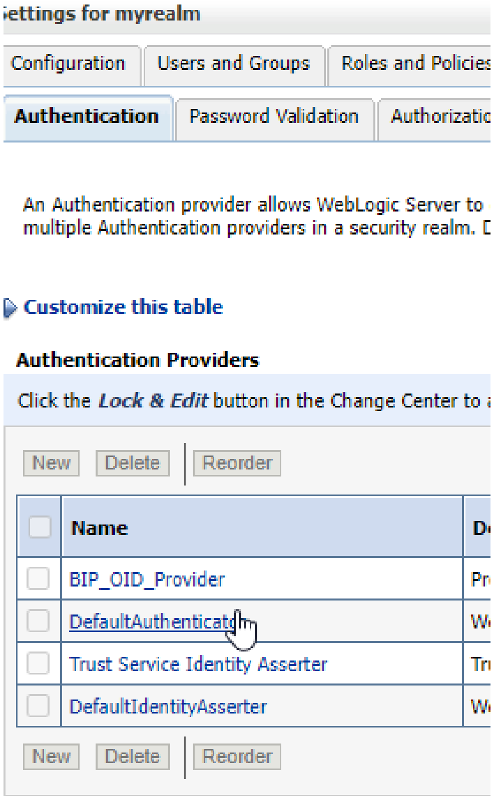
Use this page to define the provider specific configuration for this Oracle Internet Directory Au

— Connection

Host:	[redacted]	The I Info..
Port:	3060	The p listen

Step 6 – Change the DefaultAuthenticator from REQUIRED to SUFFICIENT

The DefaultAuthenticator must be changes from REQUIRED to SUFFICIENT, otherwise logins will fail.



ettings for myrealm

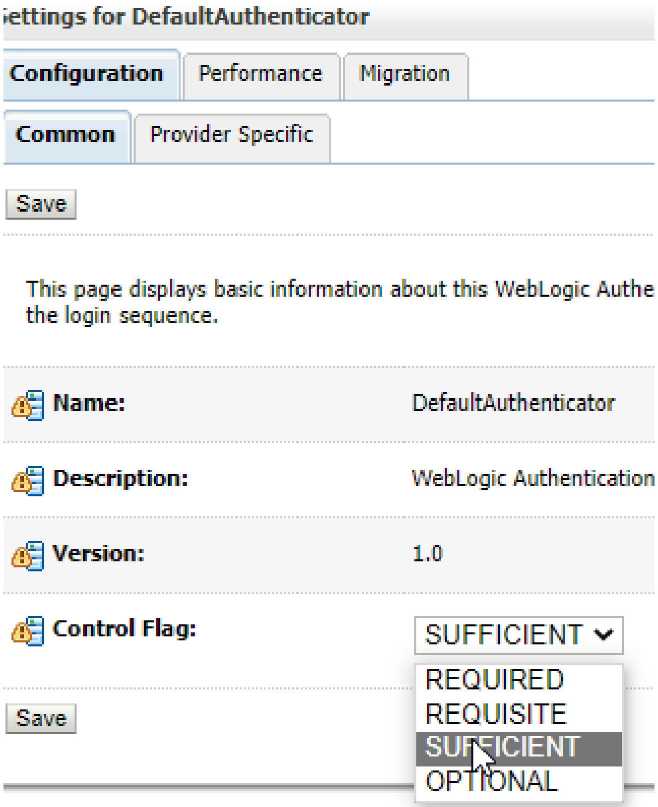
An Authentication provider allows WebLogic Server to
multiple Authentication providers in a security realm. D

Customize this table

Authentication Providers

Click the *Lock & Edit* button in the Change Center to a

□	Name	De
□	BIP_OID_Provider	Pr
□	DefaultAuthenticato	We
□	Trust Service Identity Asserter	Tr
□	DefaultIdentityAsserter	We



ettings for DefaultAuthenticator

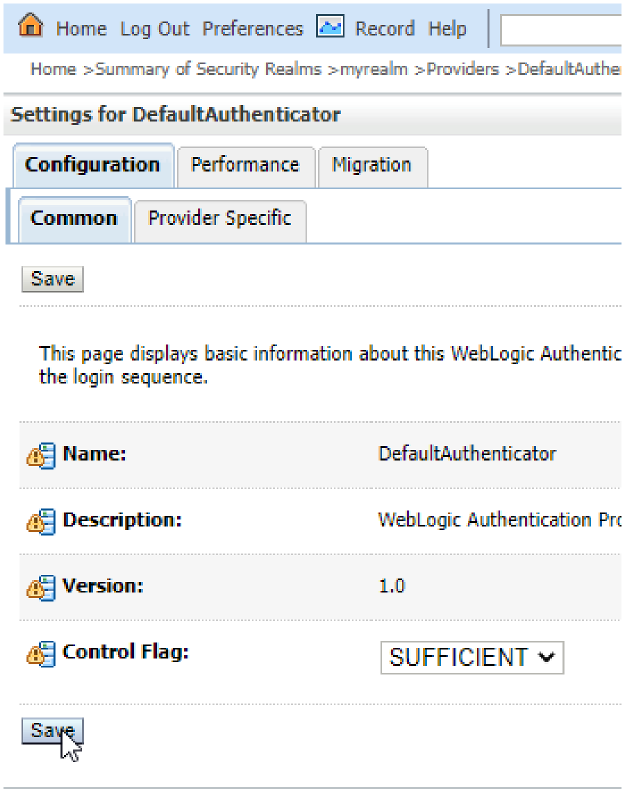
This page displays basic information about this WebLogic Authe
the login sequence.

Name: DefaultAuthenticator

Description: WebLogic Authentication

Version: 1.0

Control Flag: SUFFICIENT



Home >Summary of Security Realms >myrealm >Providers >DefaultAuthe

Settings for DefaultAuthenticator

This page displays basic information about this WebLogic Authentic
the login sequence.

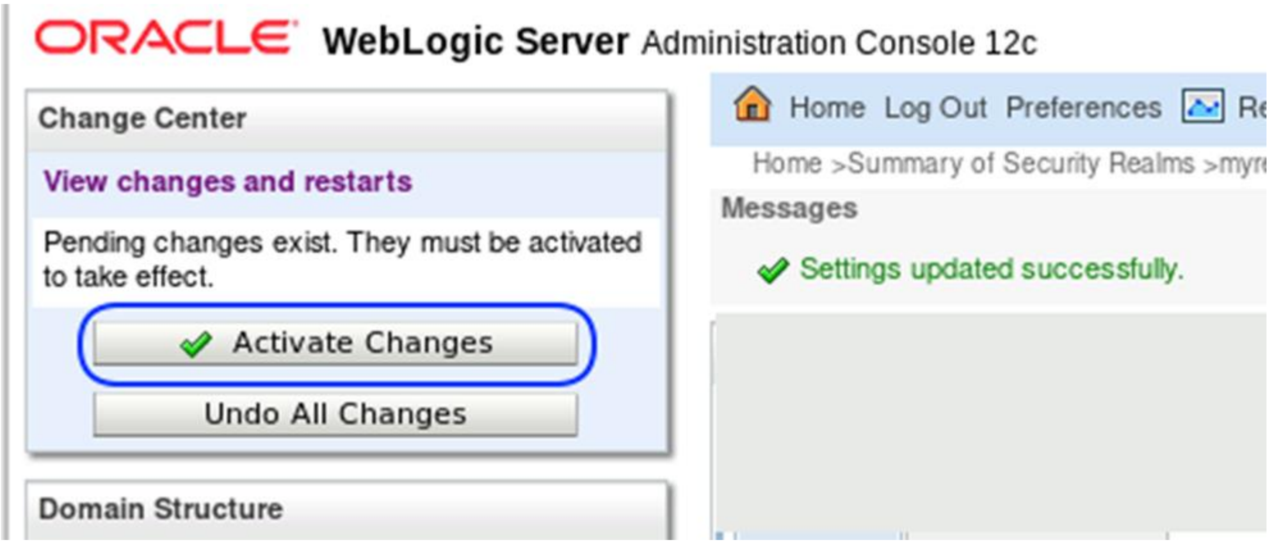
Name: DefaultAuthenticator

Description: WebLogic Authentication Pro

Version: 1.0

Control Flag: SUFFICIENT

Step 7 – Activate all the changes


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
Home
Log Out
Preferences
Re
Home >Summary of Security Realms >myre
Messages

Pending changes exist. They must be activated to take effect.

✓ Settings updated successfully.

5.3 Configuration of Java Platform Services (JPS)

To fully utilize an LDAP Server, such as Oracle Internet Directory (OID) or Microsoft Active Directory (AD), it is necessary to configure the Oracle Virtual Directory (OVD) subsystem.

This requires logging into the Operating System for the OAS product's Oracle Home and issuing the command-lines below.

Prior to editing these files, it is necessary to bring down the entire stack. See ' Appendix C - Stopping the full OAS stack'.

There are two required steps.

Step 1 - Configure Java Platform Services

The file **jps-config.xml** needs to be edited by adding the following text as shown below:

```
<property name="virtualize" value="true"/>
```

```
$ cd $MW_HOME
$ cd user_projects/domains/bi/config/fmwconfig
$ cp jps-config.xml jps-config.xml.ORIG
$ vi jps-config.xml
$ diff -b jps-config.xml jps-config.xml.ORIG
84d83
<  <property name="virtualize" value="true"/>
```

After the edits, the file **jps-config.xml** should look something like this:

```
Line#   Text
80      <serviceInstance name="idstore.ldap" provider="idstore.ldap.provider">
81         <description>LDAP Identity Store Service Instance</description>
82         <property name="idstore.config.provider"  value="......
83         <property name="CONNECTION_POOL_CLASS" value="......
84            <property name="virtualize" value="true"/>
85      </serviceInstance>
```

Step 2 - Configuring Oracle Virtual Directory (OVD)

The file **provider.os_xml** needs to be edited by changing the text as shown below:

```
      <property name="enabled" value="true"/>
```

```
$ cd $MW_HOME/user_projects/domains/bi/config/fmwconfig/ovd/default/
$ cp provider.os_xml provider.os_xml.ORIG
$ diff -b provider.os_xml provider.os_xml.ORIG
58c58
<              <property name="enabled" value="true"/>
---
>              <property name="enabled" value="false"/>
```

After the edits, the file should look something like this:

```
Line#   Text
55      <provider name="BlindTrustManager">
56         <configClass>oracle.ods.virtualization.config.BlindTrustManagerProviderConfig</.....
57         <properties>
58            <property name="enabled" value="true"/>
59         </properties>
60       </provider>
```

5.4 Stop the complete OAS stack

In order for the above sets of changes to be made permanent, it is necessary to completely bounce the OAS WebLogic domain.

Stop the OAS WebLogic Domain using ‘Appendix C- Stopping the full OAS stack’.

5.5 Start the complete OAS stack

Start the OAS WebLogic domain using ‘Appendix B - Starting the full OAS stack’

5.6 Mapping Fusion Middleware Application roles to EM LDAP Users

As a pre-requisite, all the steps earlier in this chapter must have already been completed.

If the prior sections are followed, the full OAS stack should be down.

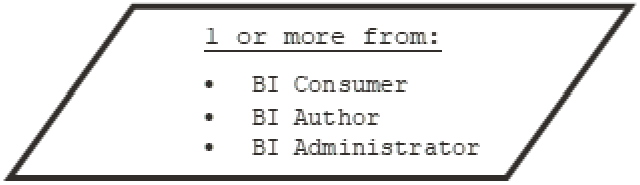
Start the full OAS stack, using the instructions in 'Appendix B - Starting the full OAS stack'.

This section will detail the steps for granting OAS Fusion Middleware Application roles to LDAP Users, and/or LDAP Groups, utilizing Fusion Middleware Control.

These same LDAP users and LDAP groups will be shared between the two products (Enterprise Manager and Oracle Analytics Server).

The specifics role names and mapping form the basis of the termination, as shown in the flow charts from Appendix F and Appendix G.

- Appendix F- Oracle Analytics Publisher Login Flow
- Appendix G - OAS Privilege Assignment



1 or more from:

- BI Consumer
- BI Author
- BI Administrator

NOTES:

- The three roles above would have already been created as part of the initial OAS Configuration.
- These roles are managed by the Oracle Platform Services (**OPSS**) as part of the '**obi-stripe**'.
- The '**obi-stripe**' is created as part of OAS configuration, and populated with these three roles, in a hierarchical manner.

OBI-Stripe Role	Description
BI Consumer	Can login to OAS and view reports
BI Consumer	Can also schedule OAS reports
BI Author	Can manipulate the OAS catalog (cut/copy/paste/delete)
BI Author	Can also edit OAS reports
BI Administrator	Full access to OAS, including access to the special **Administration** screens.

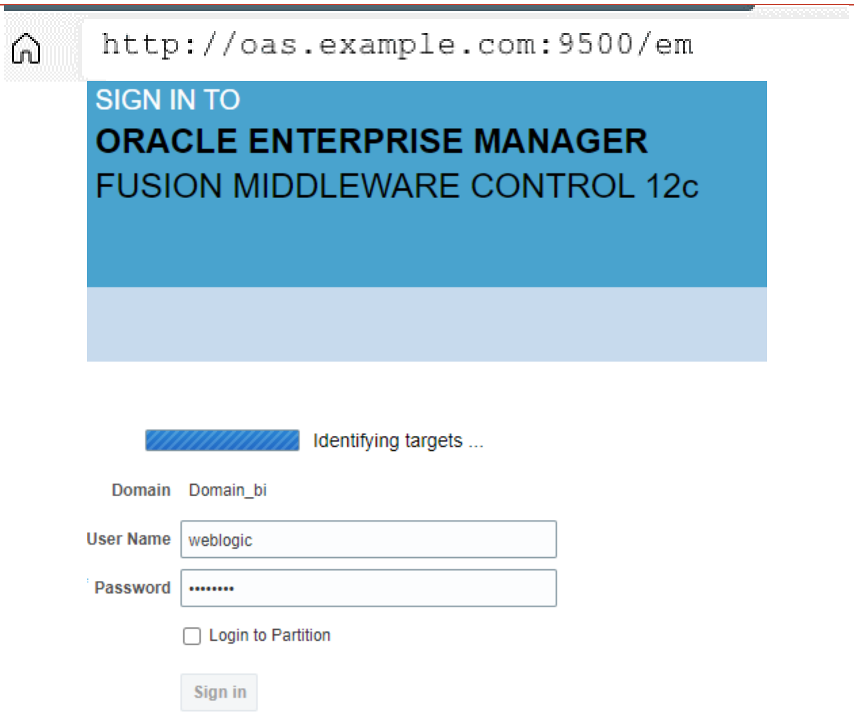
Note: Step 4 has a total of 11 parts

Step 4 Part 1 – Login to Fusion Middleware Control

Login to Fusion Middleware control, in a browser, as the 'weblogic' user.

For example:

http://oas.example.com:9500/em



http://oas.example.com:9500/em

SIGN IN TO
ORACLE ENTERPRISE MANAGER
FUSION MIDDLEWARE CONTROL 12c

Identifying targets ...

Domain Domain_bi

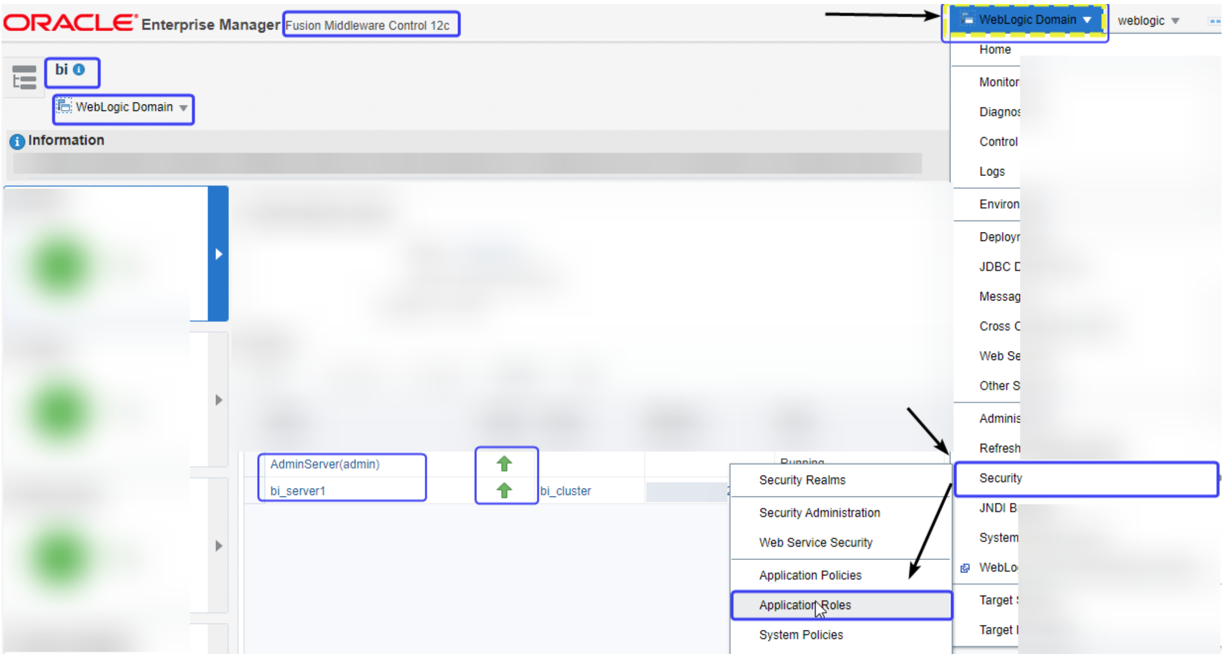
User Name weblogic

Password ••••••••

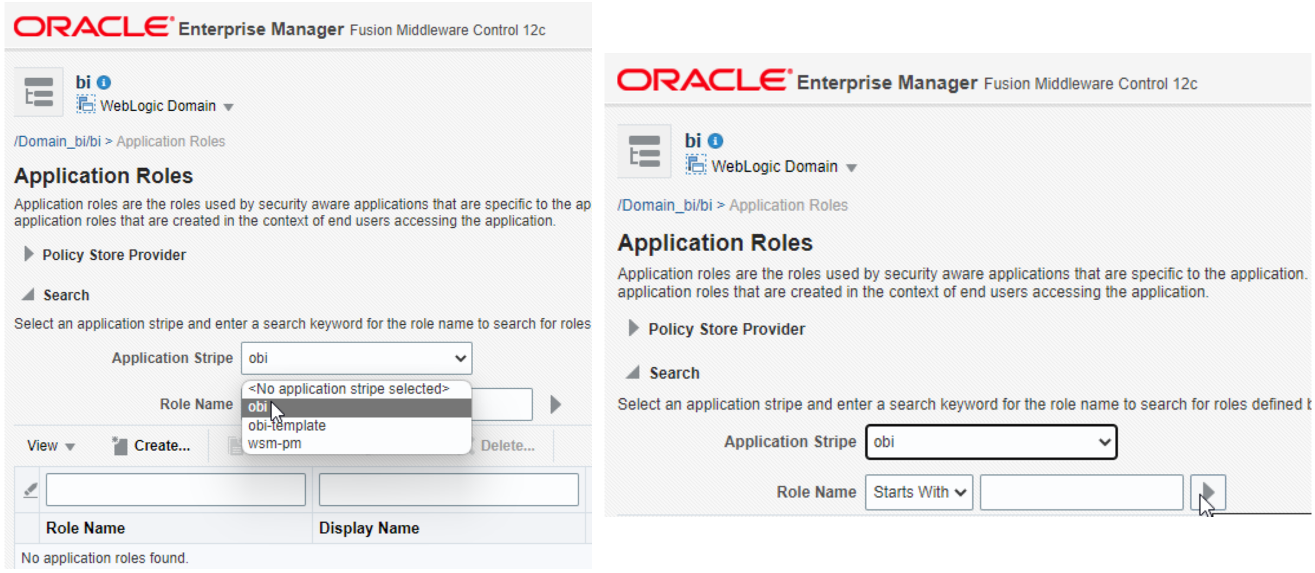
□ Login to Partition

Sign in

Step 4 - Part 2 - Configure Fusion Middleware Application Roles for OAS



Step 4 - Part 3 - Select the ‘obi’ Application Stripe and click the search button


ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Application Roles
Policy Store Provider
Search
View
Create...
Delete...
<No application stripe selected>
obi
obi-template
wsm-pm
Starts With

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. application roles that are created in the context of end users accessing the application.

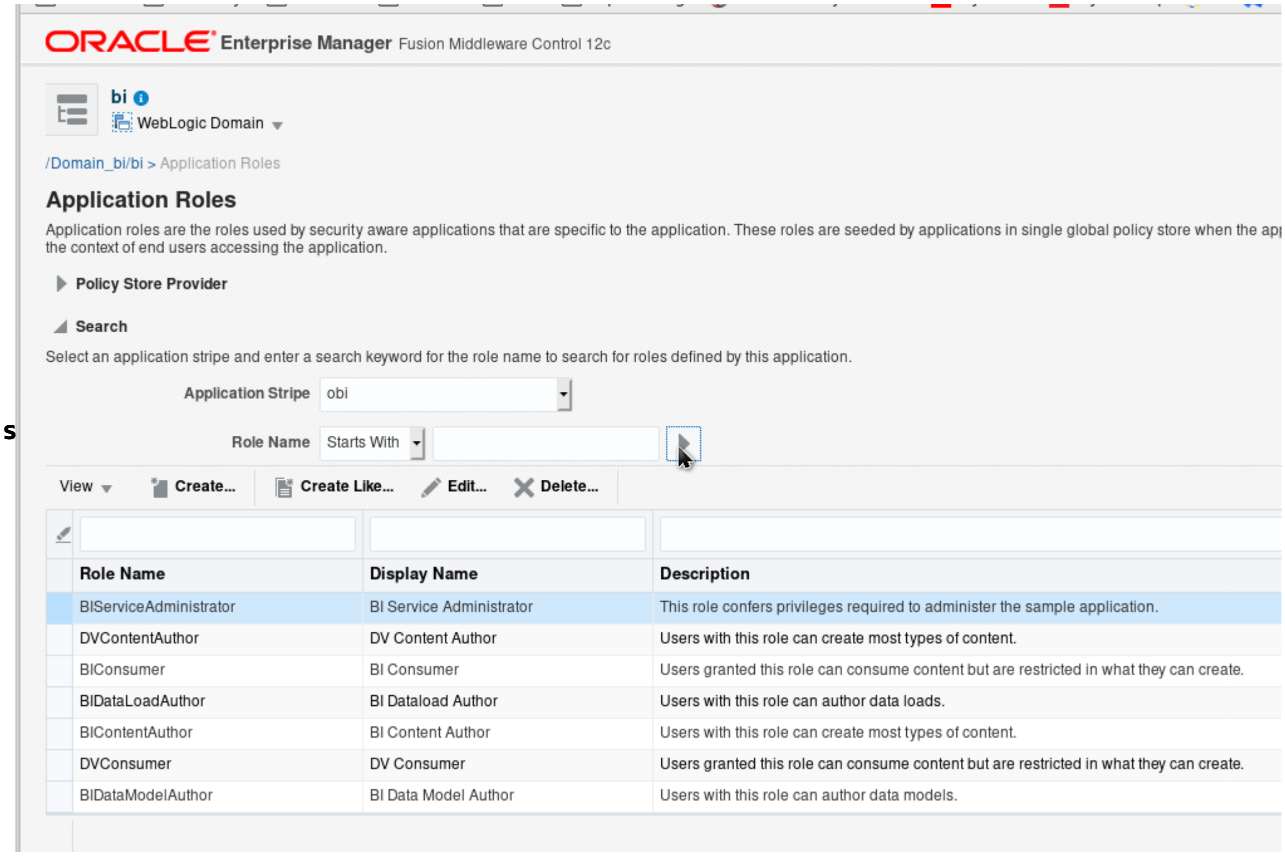
Select an application stripe and enter a search keyword for the role name to search for roles defined b

Application Stripe: obi

Role Name

Role Name	Display Name
No application roles found.	

Step 4 - Part 4 - Select the Role BIServiceAdministrator


S
ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Application Roles
Policy Store Provider
Search
View
Create...
Create Like...
Edit...
Delete...

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the ap the context of end users accessing the application.

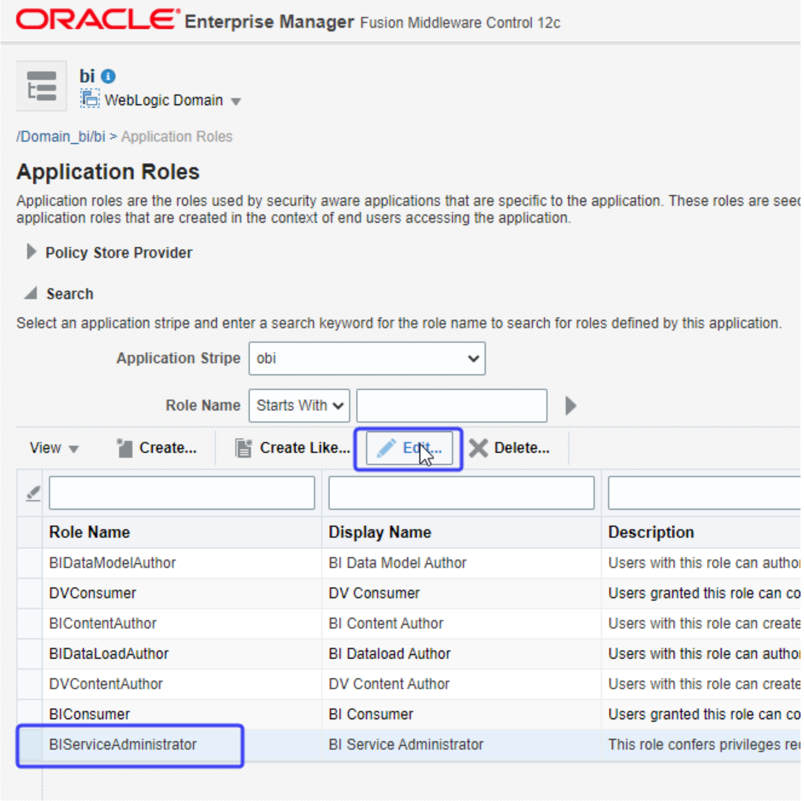
Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe: obi

Role Name: Starts With

Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer the sample application.
DVContentAuthor	DV Content Author	Users with this role can create most types of content.
BIConsumer	BI Consumer	Users granted this role can consume content but are restricted in what they can create.
BIDataLoadAuthor	BI Dataload Author	Users with this role can author data loads.
BIContentAuthor	BI Content Author	Users with this role can create most types of content.
DVConsumer	DV Consumer	Users granted this role can consume content but are restricted in what they can create.
BIDataModelAuthor	BI Data Model Author	Users with this role can author data models.

Step 4 - Part 5 - Press Edit



/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seed
application roles that are created in the context of end users accessing the application.

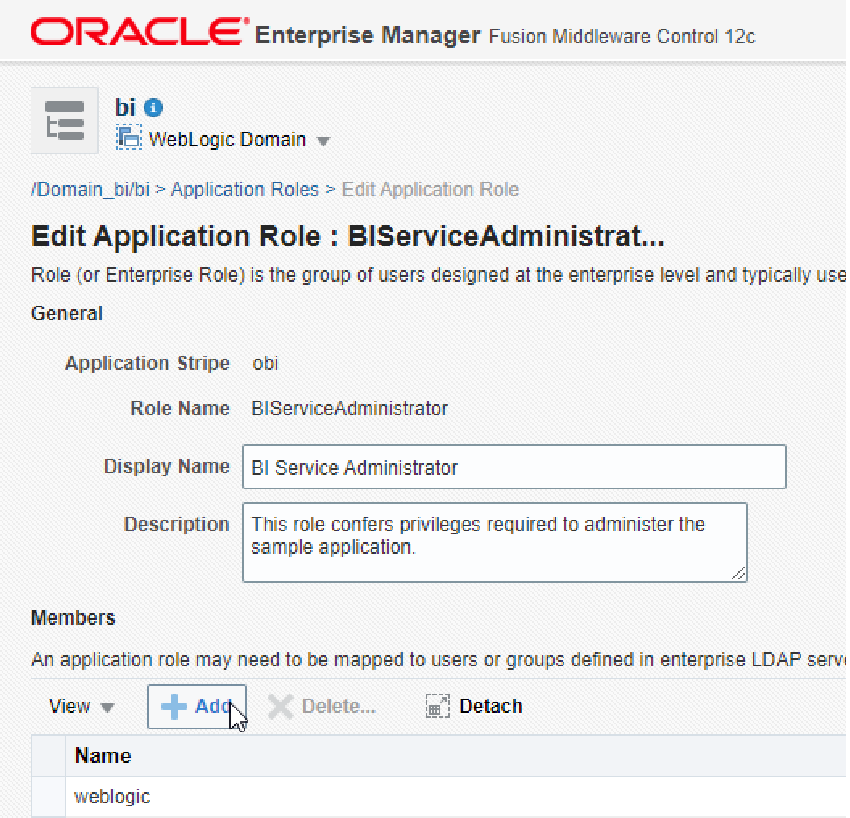
Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe: obi

Role Name: Starts With

Role Name	Display Name	Description
BIDataModelAuthor	BI Data Model Author	Users with this role can author
DVConsumer	DV Consumer	Users granted this role can co
BIContentAuthor	BI Content Author	Users with this role can create
BIDataLoadAuthor	BI Dataload Author	Users with this role can author
DVContentAuthor	DV Content Author	Users with this role can create
BIConsumer	BI Consumer	Users granted this role can co
BIServiceAdministrator	BI Service Administrator	This role confers privileges re

Step 4 - Part 6 – Press Add



/Domain_bi/bi > Application Roles > Edit Application Role

Edit Application Role : BIServiceAdministrat...

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically use

General

Application Stripe: obi

Role Name: BIServiceAdministrator

Display Name: BI Service Administrator

Description: This role confers privileges required to administer the sample application.

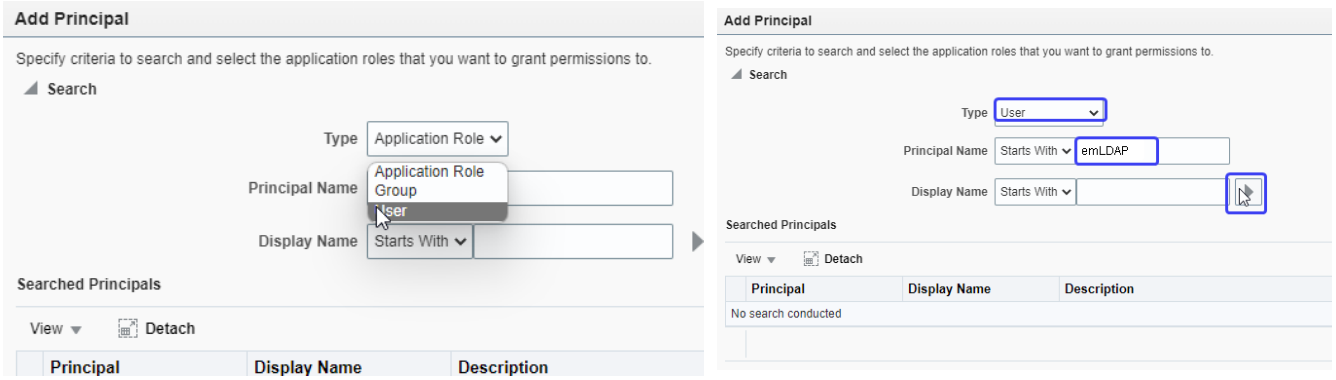
Members

An application role may need to be mapped to users or groups defined in enterprise LDAP serv

Name
weblogic

Step 4 - Part 7 - Add the required Principals

Enter a value for the Principal Name (for example, *emLDAPUser1*), and press the search arrow



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: Application Role (options: Application Role, Group, User)

Principal Name:

Display Name: Starts With

Searched Principals

Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: User

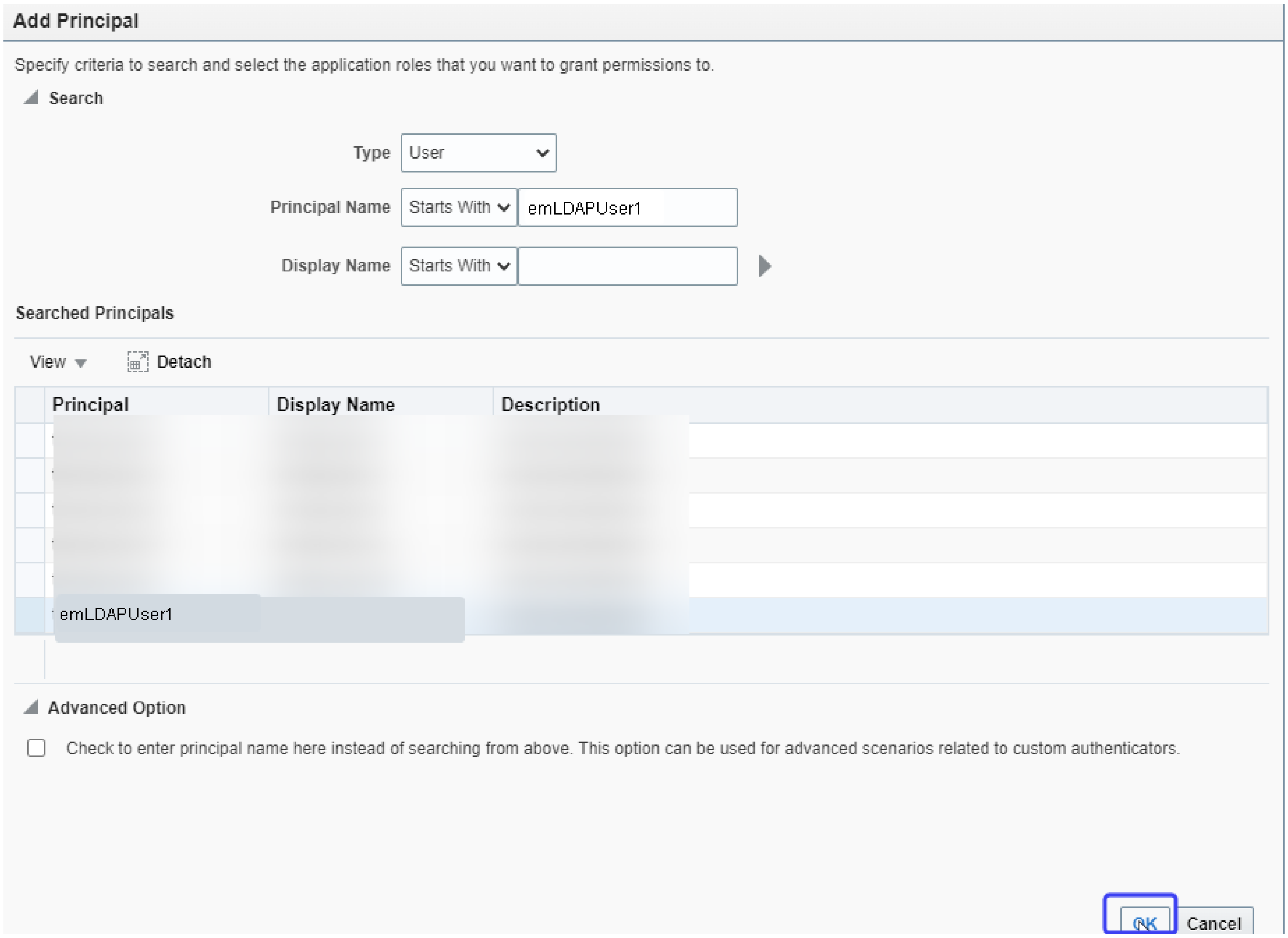
Principal Name: Starts With | emLDAP

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
No search conducted		

Step 4 - Part 8 - Select an LDAP user (for example, *emLDAPUser1)* and press OK in bottom right



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: User

Principal Name: Starts With | emLDAPUser1

Display Name: Starts With

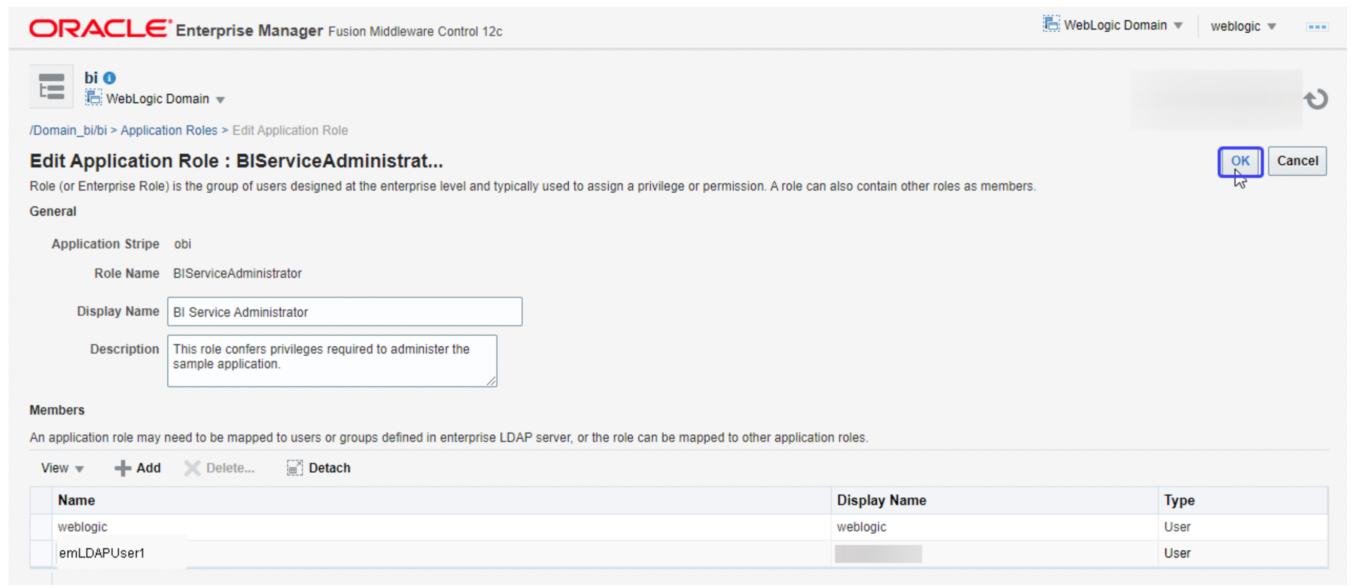
Searched Principals

Principal	Display Name	Description
emLDAPUser1		

Advanced Option

☐ Check to enter principal name here instead of searching from above. This option can be used for advanced scenarios related to custom authenticators.

Step 4 -Part 9 – Confirm the selection by pressing OK in the top right



/Domain_bi/bi > Application Roles > Edit Application Role

Edit Application Role : BIServiceAdministrat...

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically used to assign a privilege or permission. A role can also contain other roles as members.

General

Application Stripe: obi

Role Name: BIServiceAdministrator

Display Name: BI Service Administrator

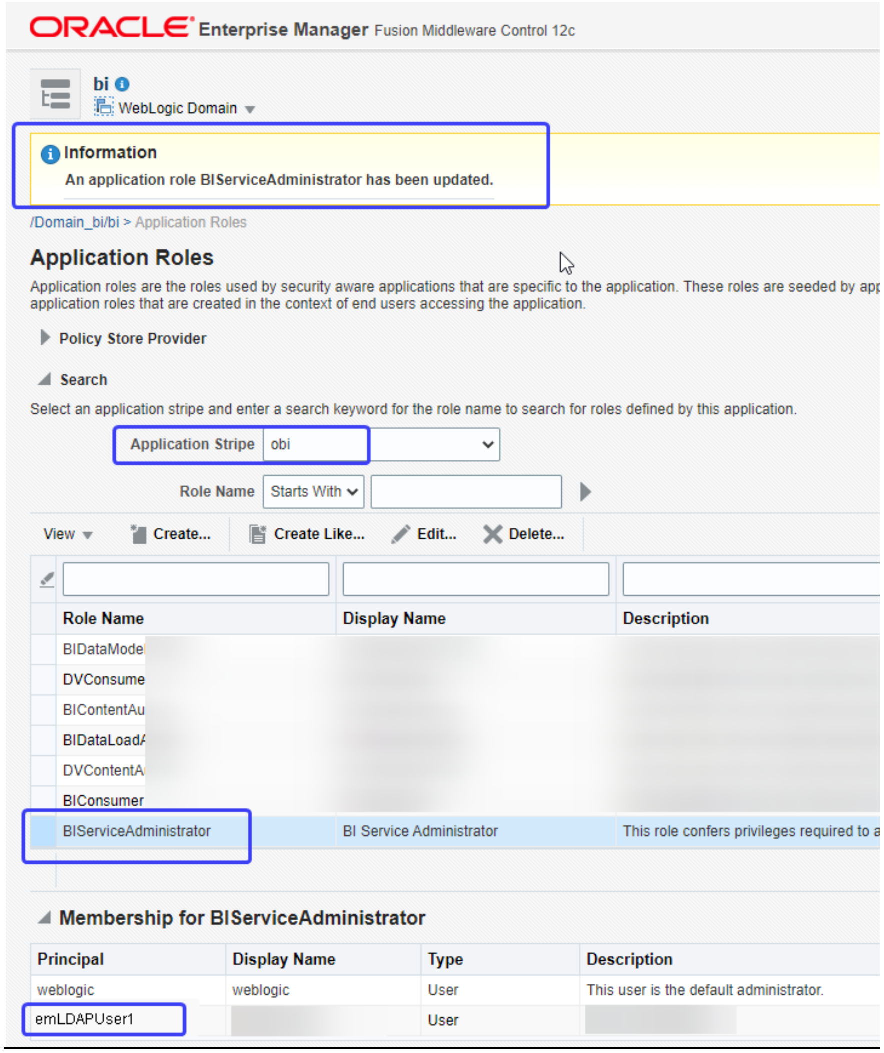
Description: This role confers privileges required to administer the sample application.

Members

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

Name	Display Name	Type
weblogic	weblogic	User
emLDAPUser1	[redacted]	User

Step 4 – Part 10 – Confirm the changes are complete



Information

An application role BIServiceAdministrator has been updated.

/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by app application roles that are created in the context of end users accessing the application.

Policy Store Provider

Search

Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe: obi

Role Name: Starts With

Role Name	Display Name	Description
BIDataMode	[redacted]	[redacted]
DVConsume	[redacted]	[redacted]
BIContentAu	[redacted]	[redacted]
BIDataLoadA	[redacted]	[redacted]
DVContentA	[redacted]	[redacted]
BIConsumer	[redacted]	[redacted]
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to a

Membership for BIServiceAdministrator

Principal	Display Name	Type	Description
weblogic	weblogic	User	This user is the default administrator.
emLDAPUser1	[redacted]	User	[redacted]

Step 4 - Part 11 - Push any changes to OBI stripe

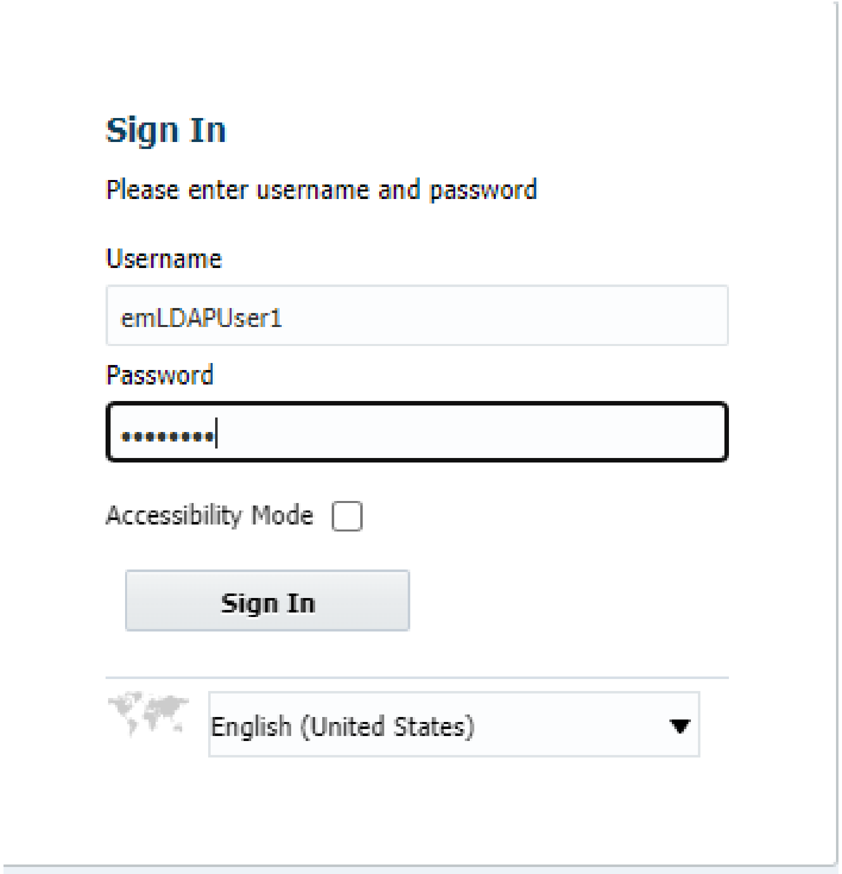
It can sometimes be necessary to bounce OAS for the changes to the OBI-stripe to propagate. To push the changes immediately:

- Bring Down OAS, the Admin Server, and the node manager:
  - Appendix C - Stopping the full OAS stack
- Start the full OAS stack:
  - Appendix B - Starting the full OAS stack

Step 4 – Part 12 - Confirm the operations from the prior step are complete

For final confirmation of the above steps, login to OAS as LDAP user that was just configured.

Step 4, Part 12, section 1 - Login to the OAS console as the user edited, for example emLDAPUser1



Sign In

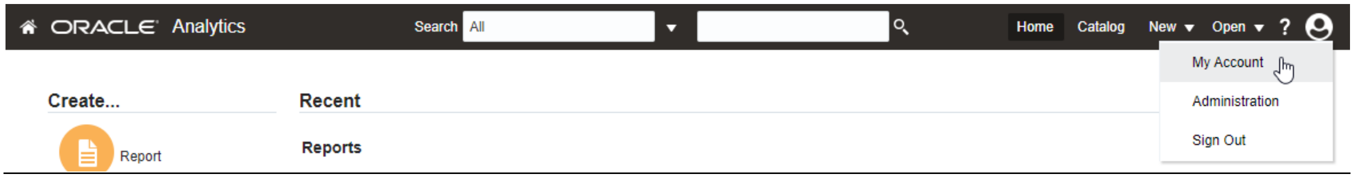
Please enter username and password

Username: emLDAPUser1

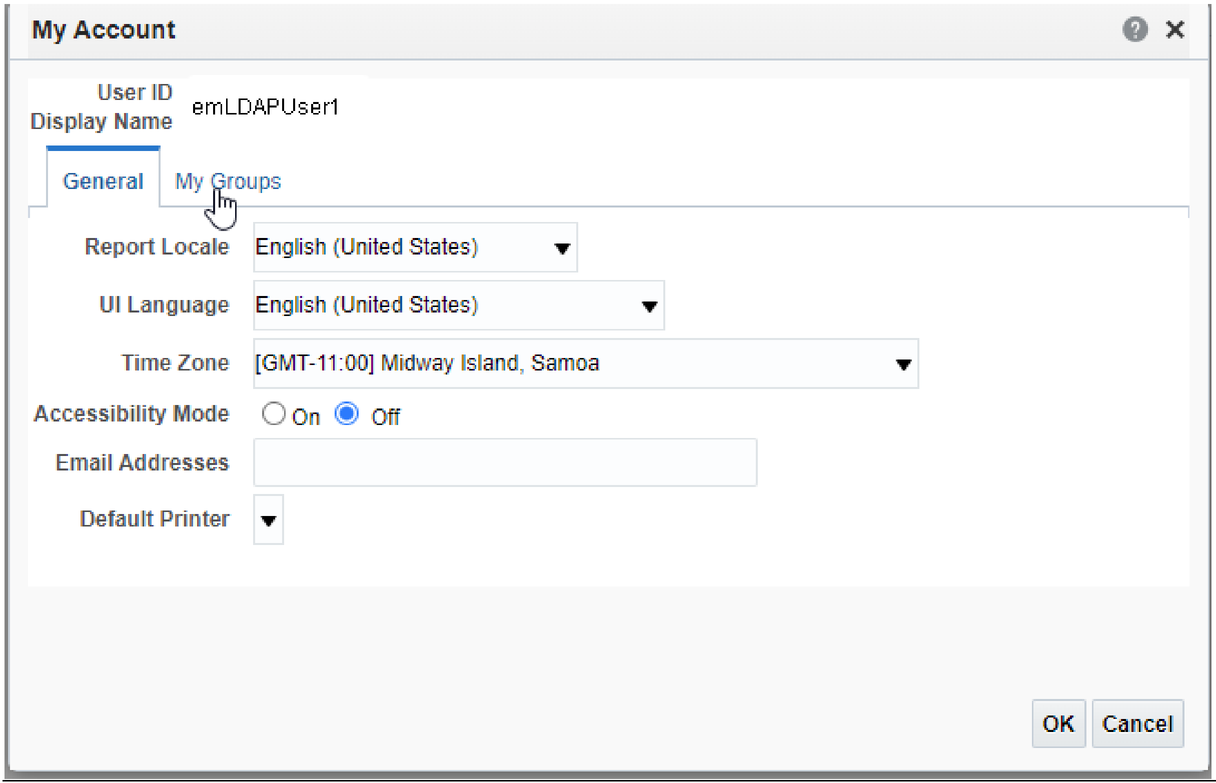
Password: ••••••••

Accessibility Mode □

Step 4, part 12, section 2 - In the top right hand of the screen, select the user's icon and My Account



Step 4, part 12, section 3 - Select the tab My Group



My Account

User ID
Display Name emLDAPUser1

Report Locale: English (United States)

UI Language: English (United States)

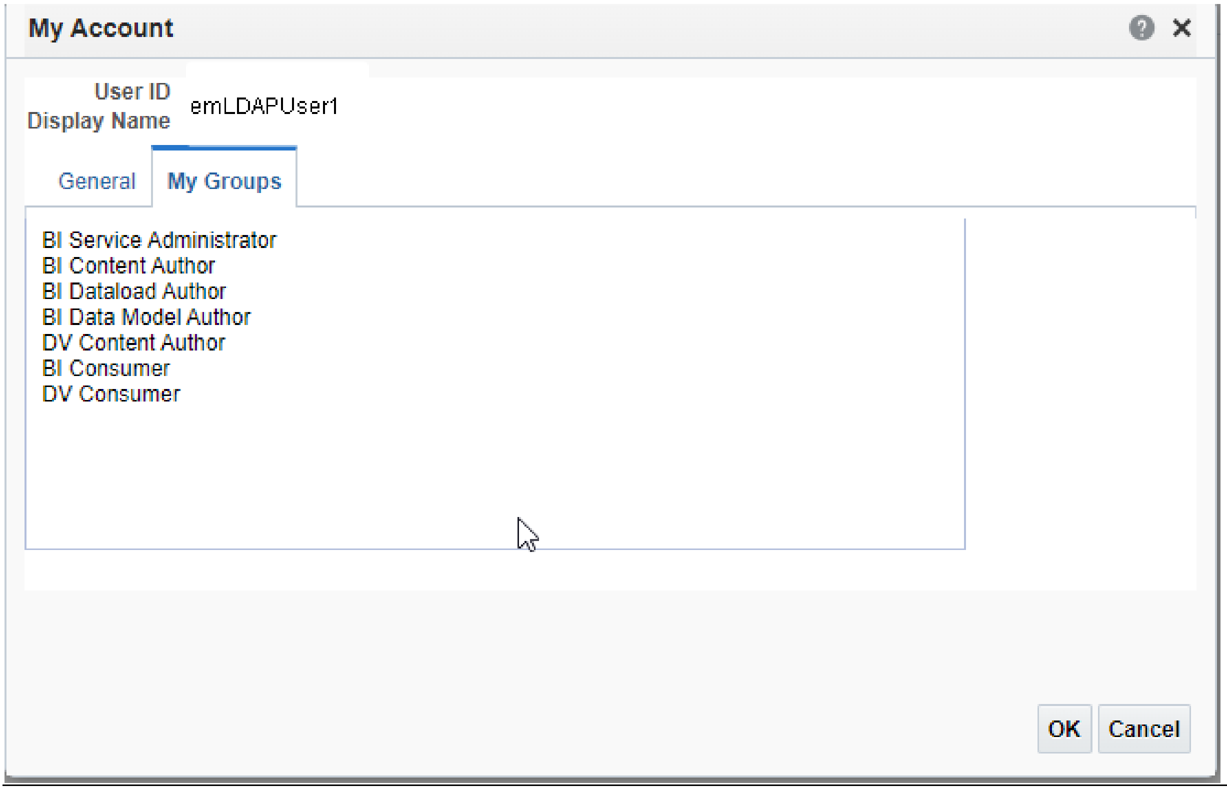
Time Zone: [GMT-11:00] Midway Island, Samoa

Accessibility Mode: ○ On ● Off

Email Addresses:

Default Printer:

Step 4, part 12, section 4 - Confirm the correct entries in My Groups



My Account

User ID
Display Name emLDAPUser1

BI Service Administrator
BI Content Author
BI Dataload Author
BI Data Model Author
DV Content Author
BI Consumer
DV Consumer

CHAPTER 6. CONFIGURATION OF REQUIRED OAS DATASOURCE(S)

After successfully configuring OAS for the desired Security Infrastructure, the Oracle Provided Reports, and any customized reports can be uploaded to OAS.

Before the Oracle provided Out of Box reports can be utilized, as well as any customized reports, it is necessary to configure one or more OAS Datasource(s). [16]

Each of these configured Datasource(s) are mapped one-to-one for each set of the Oracle provided Out of Box Reports.

Step 1 - For the first EM Host

The following command sets the password for the MGMT_VIEW user to the specified value. This is required so that the OAS Datasource (i.e., EMREPOS) can be properly configured.

```
emctl config oms -change_view_user_pwd -sysman_pwd •••••••• -user_pwd ••••••••
emctl stop oms -all
emctl start oms
```

Step 2 - OAS Datasource Configuration Steps

Use the following screenshots as an example of configuring an OAS Datasource.

Part 1 - Login to OAS as the appropriate user

When proceeding from ‘Chapter 4 - OAS For EM Repository-based Security’, login as the SYSMAN user.

When proceeding from Chapters 11 (and optionally 12 and 13), login as the ‘weblogic’ user.

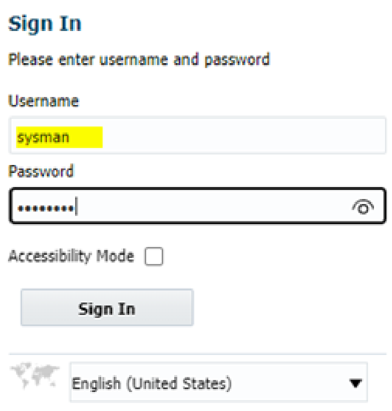
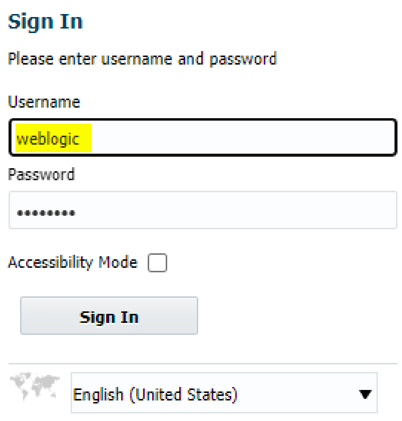
OAS for EM Repository-Based Security	OAS for LDAP Based Security
 **Sign In** Please enter username and password Username: sysman Password: •••••••• Accessibility Mode □ Sign In English (United States)	 **Sign In** Please enter username and password Username: weblogic Password: •••••••• Accessibility Mode □ Sign In English (United States)

Figure 19. Login as the **sysman** or **weblogic** user

Part 2 - Click on the Administration Link

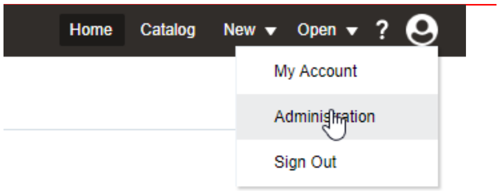
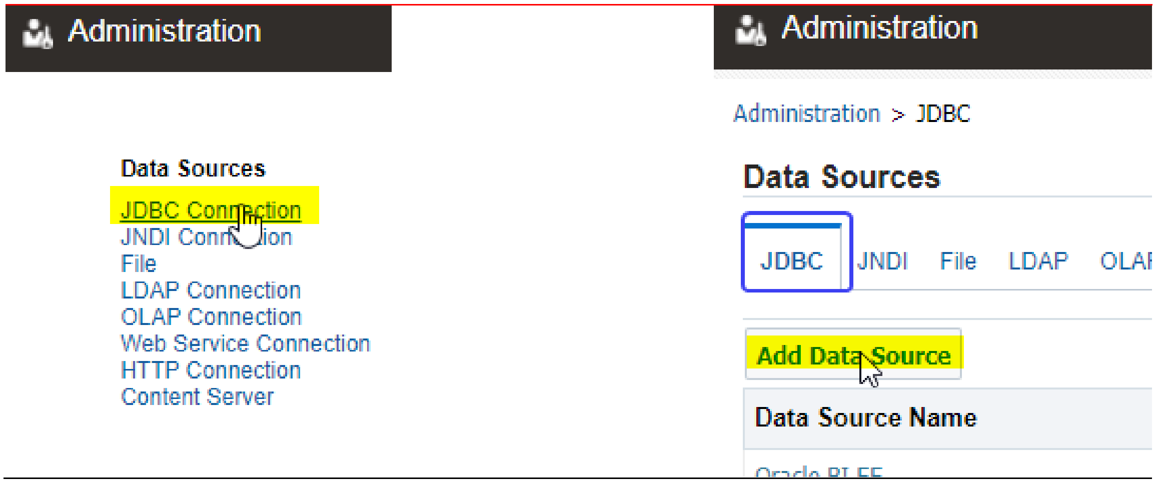


Figure 20. Click on the **Administration** link

[16] (Set Up Data Sources, 2024) Data Sources

Part 3 – Add a JDBC Data Source



Part 4 – Ensure that the MGMT_VIEW account has been setup properly

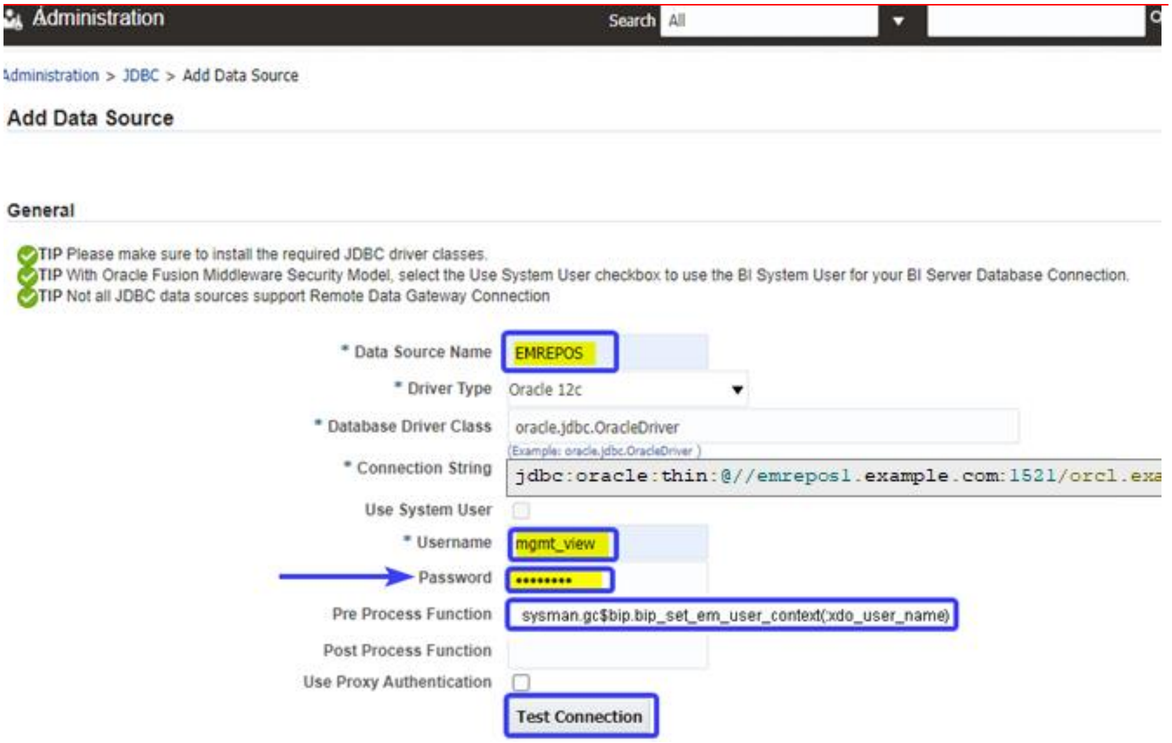
Make sure that the MGMT_VIEW user account has been set to a known password, for example:

```
$ emctl config oms -change_view_user_pwd
Oracle Enterprise Manager Cloud ...
Copyright (c) ....
Enter Repository User's Password :
Enter MGMT_VIEW User's Password :
Restart all the OMSs using 'emctl stop oms -all' and 'emctl start oms'.
Successfully changed MGMT_VIEW User's password.
```

Part 5 - Fill in the required details

```
             Name: EMREPOS
      Driver Type: Oracle 12c
   Database Class: oracle.jdbc.OracleDriver
Connection String: jdbc:oracle:thin:@//emrepos1.example.com:1521/orcl.example.com
  Use System User: Do Not Check
         Username: MGMT_VIEW
         Password: ●●●●●●●●

  Pre Process Function: sysman.gc$bip.bip_set_em_user_context(:xdo_user_name)
 Post Process Function: Leave Blank
    Client Certificate: Leave Blank
Use Proxy Authentication: Leave Blank
```

Part 6 - Review the newly defined Data Source



Administration Search All

Administration > JDBC > Add Data Source

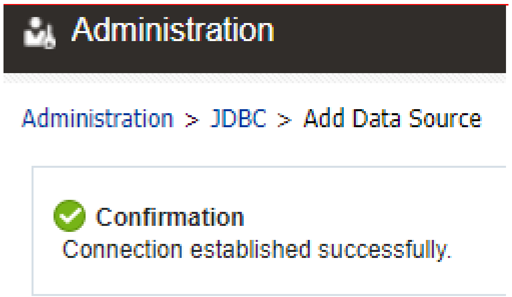
Add Data Source

General

TIP Please make sure to install the required JDBC driver classes.
TIP With Oracle Fusion Middleware Security Model, select the Use System User checkbox to use the BI System User for your BI Server Database Connection.
TIP Not all JDBC data sources support Remote Data Gateway Connection

* Data Source Name: EMREPOS
* Driver Type: Oracle 12c
* Database Driver Class: oracle.jdbc.OracleDriver
(Example: oracle.jdbc.OracleDriver)
* Connection String: jdbc:oracle:thin:@//emrepos1.example.com:1521/orcl.exa
Use System User: □
* Username: mgmt_view
Password: ••••••••
Pre Process Function: sysman.gc$bip.bip_set_em_user_context(:xdo_user_name)
Post Process Function:
Use Proxy Authentication: □

Part 7 - Positive Result of the Test

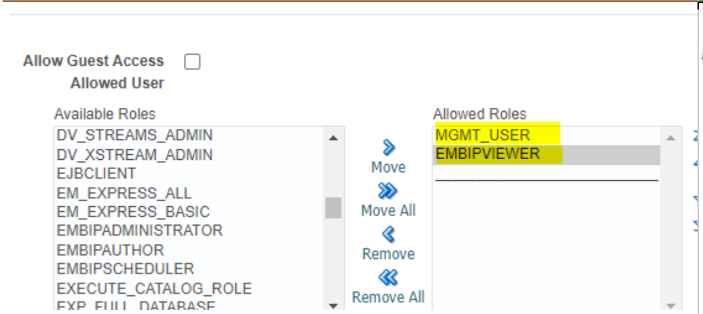
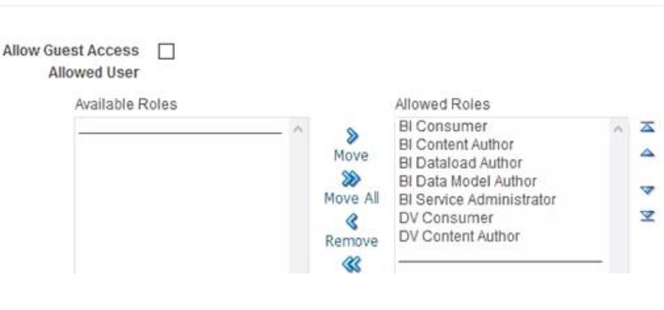


Administration

Administration > JDBC > Add Data Source

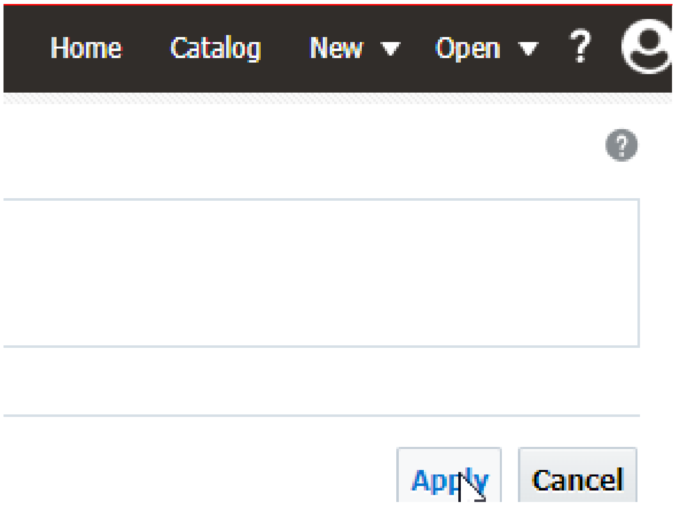
Confirmation
Connection established successfully.

Part 8 Granting Required Roles to OAS Datasource

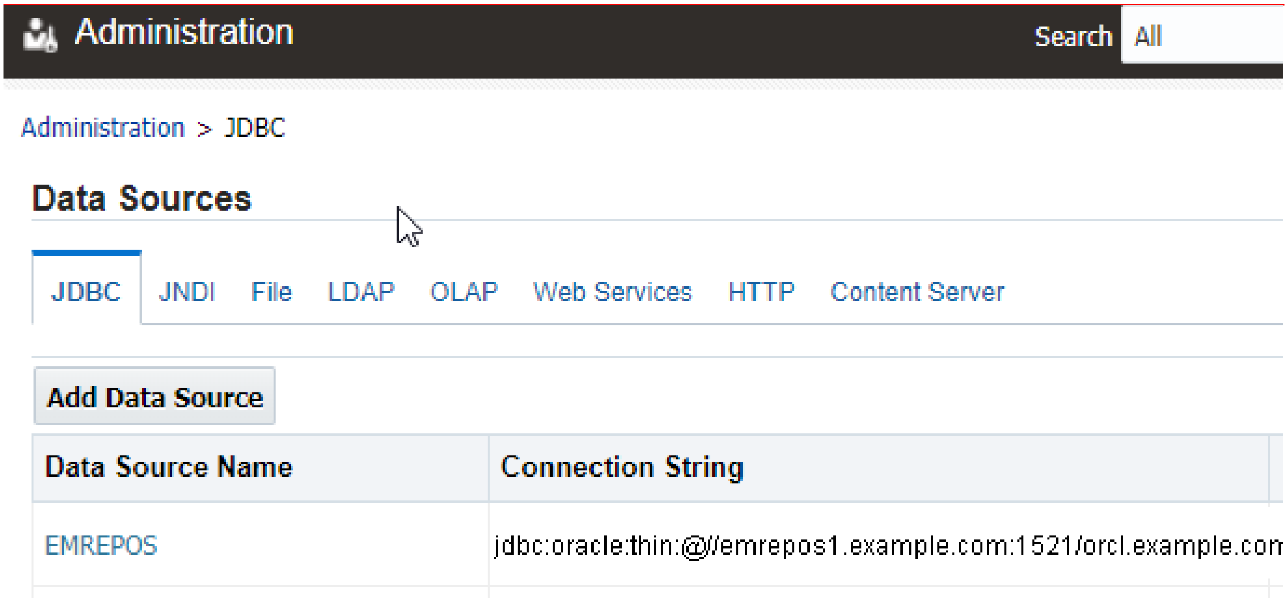
OAS for EM Repository-Based Security	OAS for LDAP Based Security
 Allow Guest Access □ Allowed User Available Roles: DV_STREAMS_ADMIN, DV_XSTREAM_ADMIN, EJBCLIENT, EM_EXPRESS_ALL, EM_EXPRESS_BASIC, EMBIPADMINISTRATOR, EMBIPAUTHOR, EMBIPSCHEDULER, EXECUTE_CATALOG_ROLE, EXP_FULL_DATABASE Allowed Roles: MGMT_USER, EMBIPVIEWER	 Allow Guest Access □ Allowed User Available Roles: Allowed Roles: BI Consumer, BI Content Author, BI Dataload Author, BI Data Model Author, BI Service Administrator, DV Consumer, DV Content Author

*In general, it is not appropriate to select the '**Allow Guest Access**' unless a specific use case has been identified to support the guest account.*

Part 9 - Press Apply



Part 10 – Completed List of JDBC Data Sources



Data Source Name	Connection String
EMREPOS	jdbc:oracle:thin:@//emrepos1.example.com:1521/orcl.example.com

CHAPTER 7. PREPARE FOR ORACLE PROVIDED OUT OF BOX REPORTS

Enterprise Manager 24c bundles a full set of the Oracle Provided out-of-box reports. This set of out-of-box reports is being delivered consistent with earlier releases of Enterprise Manager.

Per-requisite Step

There are several required steps to support the installation of Enterprise Manager Provided Out of Box Reports.

When utilizing the Database Security Model with OAS [Chapter 4 - OAS For EM Repository-based Security], the EMBIP* database roles would have been configured using the steps on page 15 ‘Preparation for upload of Oracle Provided Reports’.

When utilizing the Fusion Middleware Security Model, the built in OAS roles need to overlayed onto the required EMBIP* roles.

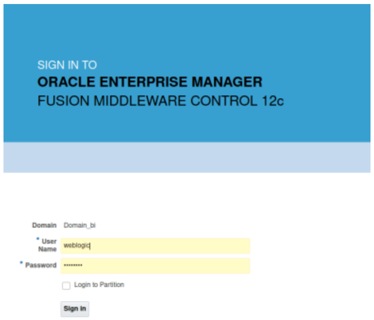
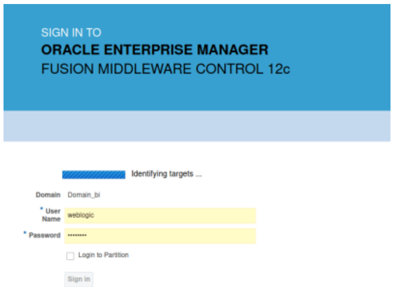
Proceed to 0 Migrating customized Reports from OAP 6.4.

7.1 OAS support for EM Provided Reports: Fusion Middleware Security Model

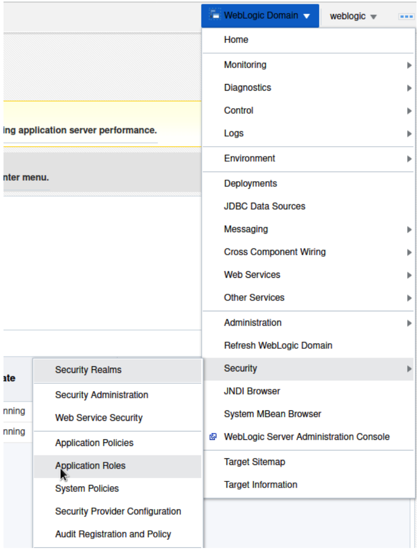
The steps to map the required EMBIP* roles for the Fusion Middleware Security Model are a bit more involved.

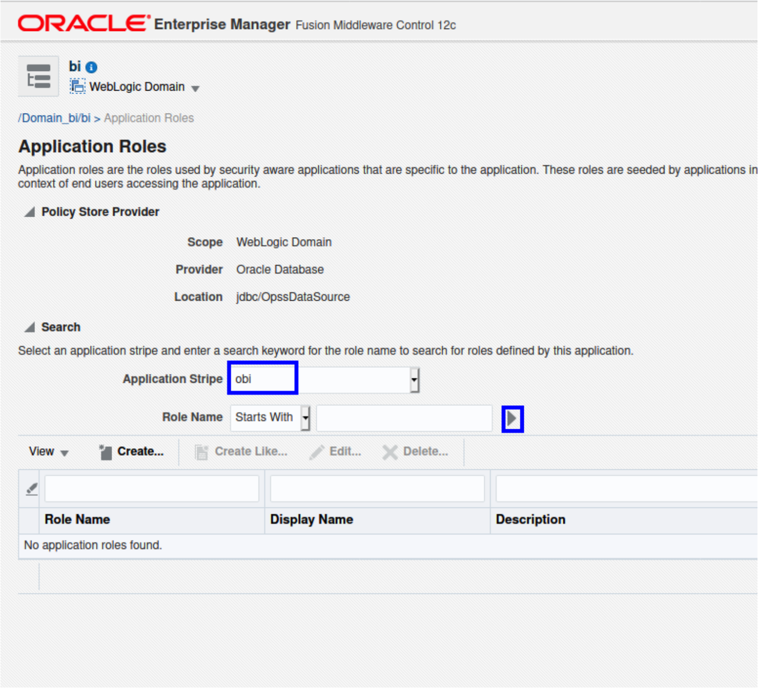
Step 1 - Create EMBIP* Roles as OBI-Stripe Roles

7.1.1.1 Step 1, Part 1 - Login to Fusion Middleware Control

 SIGN IN TO ORACLE ENTERPRISE MANAGER FUSION MIDDLEWARE CONTROL 12c Domain Domain_bi * User Name weblogic * Password •••••••• □ Login to Partition Sign In	 SIGN IN TO ORACLE ENTERPRISE MANAGER FUSION MIDDLEWARE CONTROL 12c Identifying targets ... Domain Domain_bi * User Name weblogic * Password •••••••• □ Login to Partition Sign In

Step 1, Part 2 - Create EMBIPADMINISTRATOR Role




ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in context of end users accessing the application.

Policy Store Provider

Scope WebLogic Domain

Provider Oracle Database

Location jdbc/OpssDataSource

Search

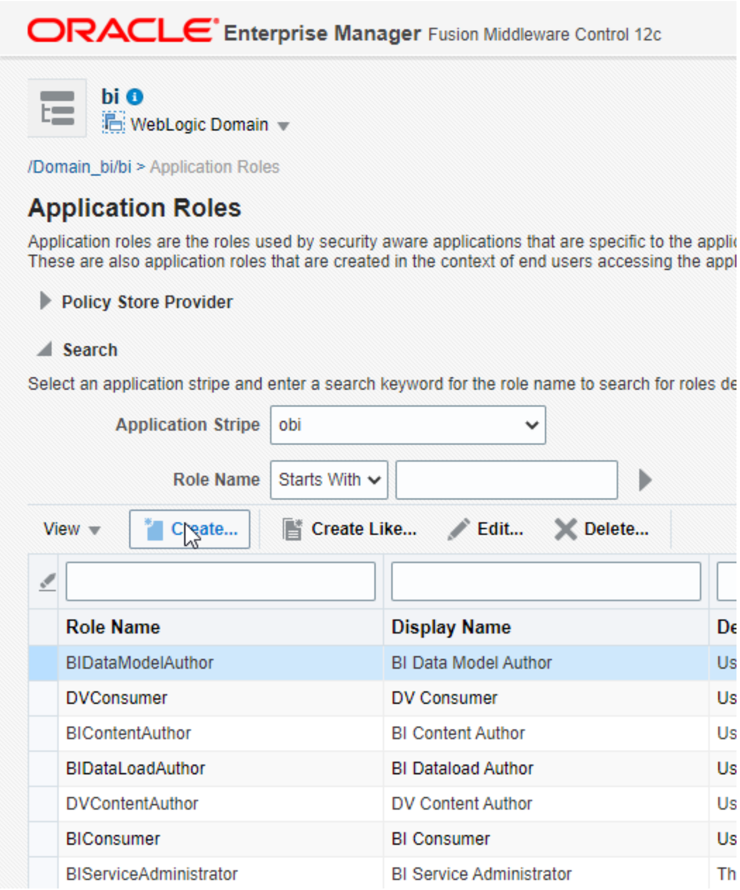
Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe obi

Role Name Starts With

Role Name	Display Name	Description
No application roles found.		

Step 1, Part 3 - Create EMBIPAdministrator and all EMBIP* Roles


ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the appli
These are also application roles that are created in the context of end users accessing the appl

Policy Store Provider

Search

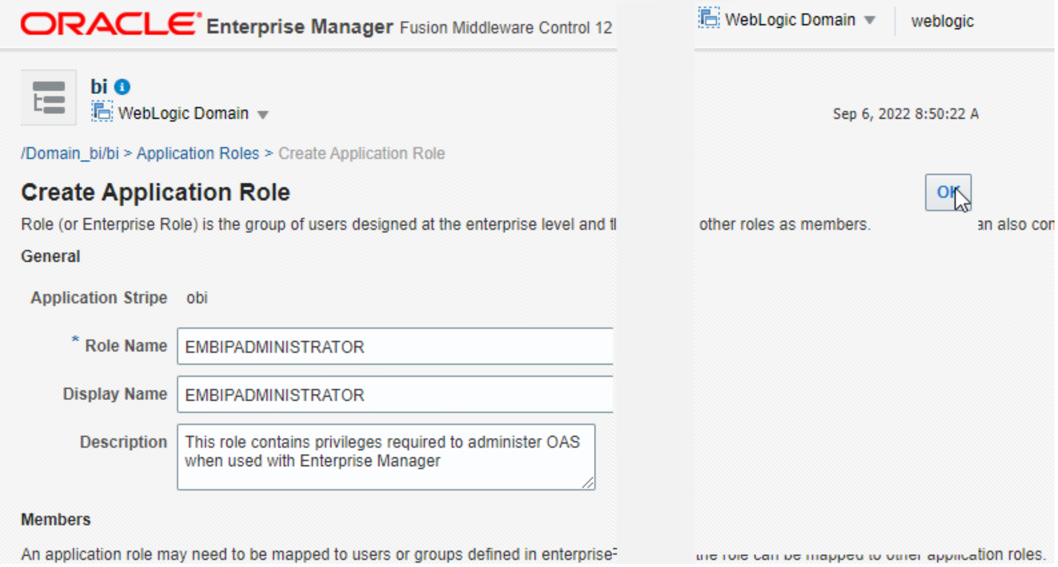
Select an application stripe and enter a search keyword for the role name to search for roles de

Application Stripe obi

Role Name Starts With

Role Name	Display Name	De
BIDataModelAuthor	BI Data Model Author	Us
DVConsumer	DV Consumer	Us
BIContentAuthor	BI Content Author	Us
BIDataLoadAuthor	BI Dataload Author	Us
DVContentAuthor	DV Content Author	Us
BIConsumer	BI Consumer	Us
BIServiceAdministrator	BI Service Administrator	Th

» Enter "EMBIPADMINISTRATOR" for the name and description, then press OK



ORACLE Enterprise Manager Fusion Middleware Control 12 — WebLogic Domain ▼ weblogic

bi — WebLogic Domain ▼ — Sep 6, 2022 8:50:22 A

/Domain_bi/bi > Application Roles > Create Application Role

Create Application Role

OK

Role (or Enterprise Role) is the group of users designed at the enterprise level and tl other roles as members. an also con

General

Application Stripe obi

* Role Name EMBIPADMINISTRATOR

Display Name EMBIPADMINISTRATOR

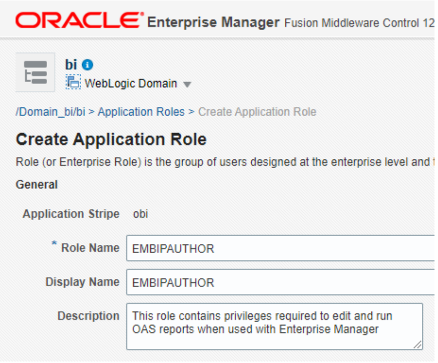
Description This role contains privileges required to administer OAS when used with Enterprise Manager

Members

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

Step 1, Part 4 - Repeat Above steps for the other three required roles

EMBIPAUTHOR



ORACLE Enterprise Manager Fusion Middleware Control 12

bi — WebLogic Domain ▼

/Domain_bi/bi > Application Roles > Create Application Role

Create Application Role

Role (or Enterprise Role) is the group of users designed at the enterprise level and t

General

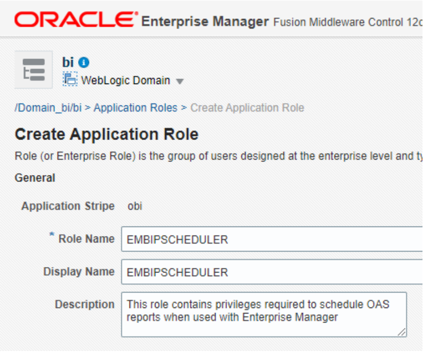
Application Stripe obi

* Role Name EMBIPAUTHOR

Display Name EMBIPAUTHOR

Description This role contains privileges required to edit and run OAS reports when used with Enterprise Manager

EMBIPSCHEDULER



ORACLE Enterprise Manager Fusion Middleware Control 12c

bi — WebLogic Domain ▼

/Domain_bi/bi > Application Roles > Create Application Role

Create Application Role

Role (or Enterprise Role) is the group of users designed at the enterprise level and t

General

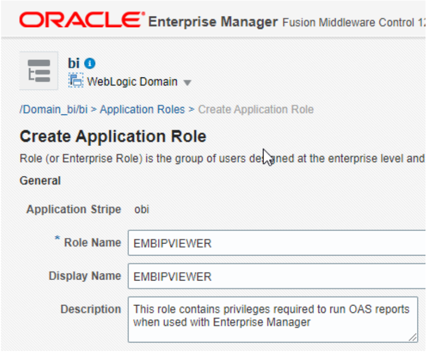
Application Stripe obi

* Role Name EMBIPSCHEDULER

Display Name EMBIPSCHEDULER

Description This role contains privileges required to schedule OAS reports when used with Enterprise Manager

EMBIPVIEWER



ORACLE Enterprise Manager Fusion Middleware Control 1

bi — WebLogic Domain ▼

/Domain_bi/bi > Application Roles > Create Application Role

Create Application Role

Role (or Enterprise Role) is the group of users designed at the enterprise level and

General

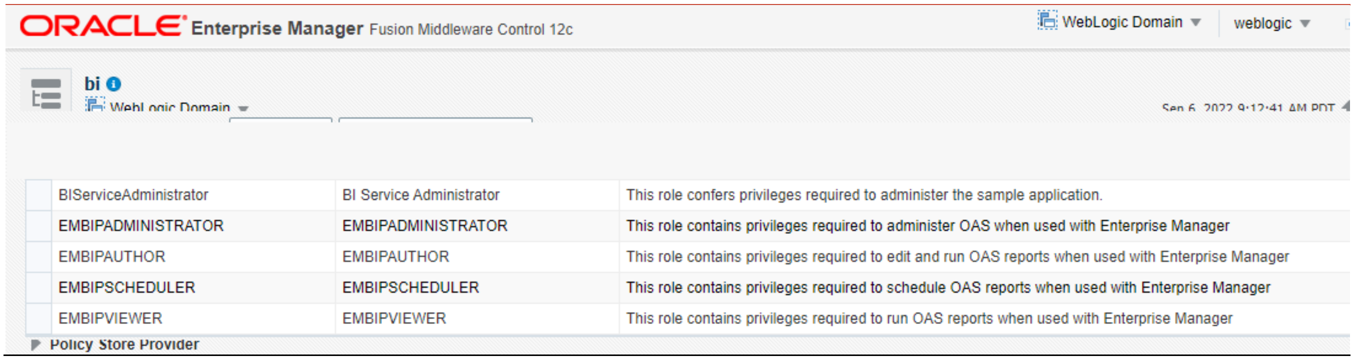
Application Stripe obi

* Role Name EMBIPVIEWER

Display Name EMBIPVIEWER

Description This role contains privileges required to run OAS reports when used with Enterprise Manager

Step 1 - Finished Result



ORACLE Enterprise Manager Fusion Middleware Control 12c — WebLogic Domain ▼ weblogic ▼

bi — WebLogic Domain ▼ — Sep 6, 2022 9:12:41 AM PDT

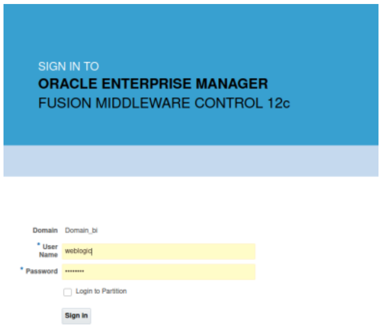
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer the sample application.
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	This role contains privileges required to administer OAS when used with Enterprise Manager
EMBIPAUTHOR	EMBIPAUTHOR	This role contains privileges required to edit and run OAS reports when used with Enterprise Manager
EMBIPSCHEDULER	EMBIPSCHEDULER	This role contains privileges required to schedule OAS reports when used with Enterprise Manager
EMBIPVIEWER	EMBIPVIEWER	This role contains privileges required to run OAS reports when used with Enterprise Manager

▶ Policy Store Provider

Step 2- Create Mapping of BI Service Administrator to EMBIPAdministrator

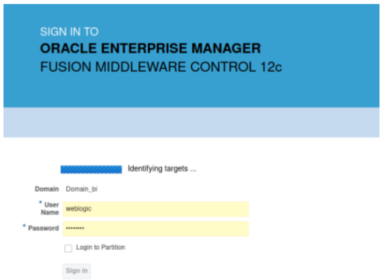
To achieve the mapping shown in **Error! Reference source not found.** - **Error! Reference source not found.**, th e following steps are required:

Step 2, Part 1 - Login to Fusion Middleware Control



SIGN IN TO
ORACLE ENTERPRISE MANAGER
FUSION MIDDLEWARE CONTROL 12c

Domain: Domain_bi
* User Name: weblogic
* Password: ********

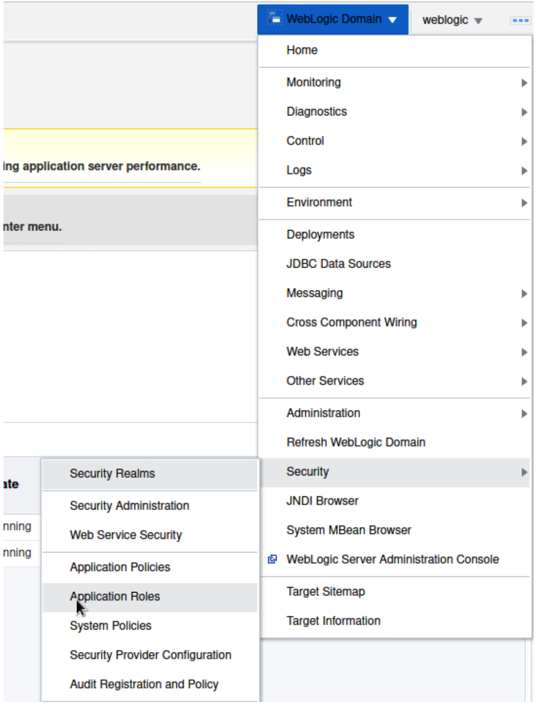


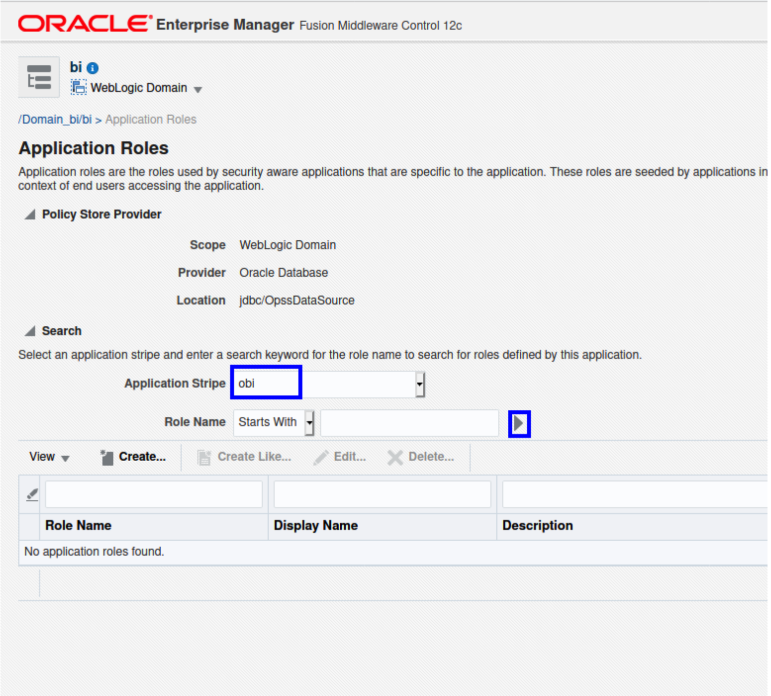
SIGN IN TO
ORACLE ENTERPRISE MANAGER
FUSION MIDDLEWARE CONTROL 12c

Identifying targets ...

Domain: Domain_bi
* User Name: weblogic
* Password: ********

Step 2, Part 2 - Navigate to OBI Application Stripe





ORACLE Enterprise Manager Fusion Middleware Control 12c
bi
WebLogic Domain
/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in context of end users accessing the application.

Policy Store Provider

Scope: WebLogic Domain
Provider: Oracle Database
Location: jdbc/OpsDataSource

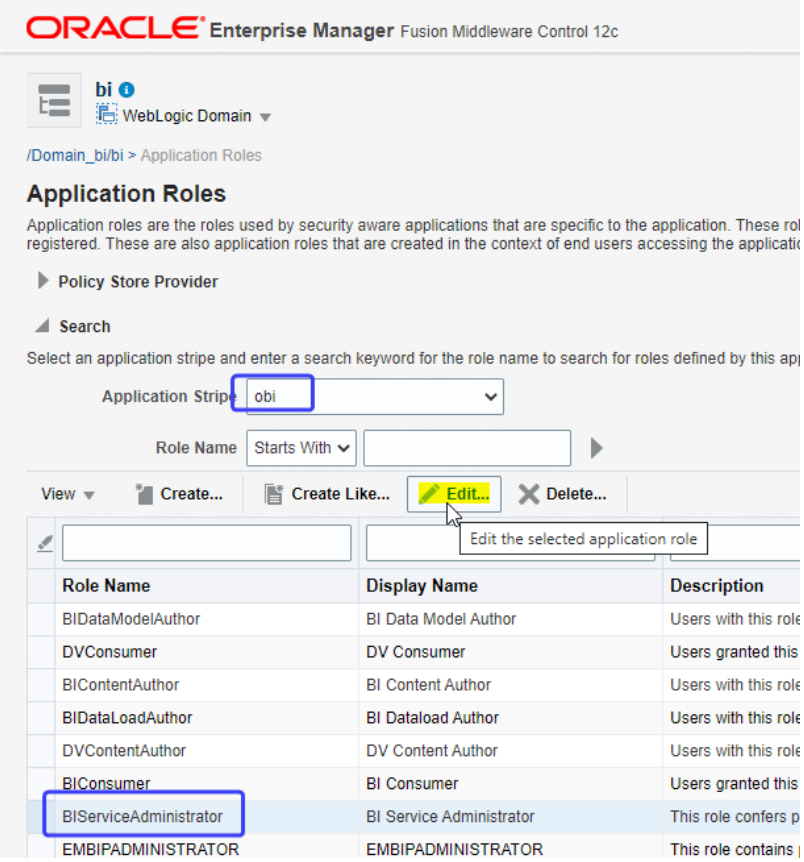
Search

Select an application stripe and enter a search keyword for the role name to search for roles defined by this application.

Application Stripe: obi
Role Name: Starts With

Role Name	Display Name	Description
No application roles found.		

Step 2, Part 3 - Edit the BIServiceAdministrator role



ORACLE Enterprise Manager Fusion Middleware Control 12c

bi

WebLogic Domain

/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These rol registered. These are also application roles that are created in the context of end users accessing the applicati

Policy Store Provider

Search

Select an application stripe and enter a search keyword for the role name to search for roles defined by this ap

Application Stripe: obi

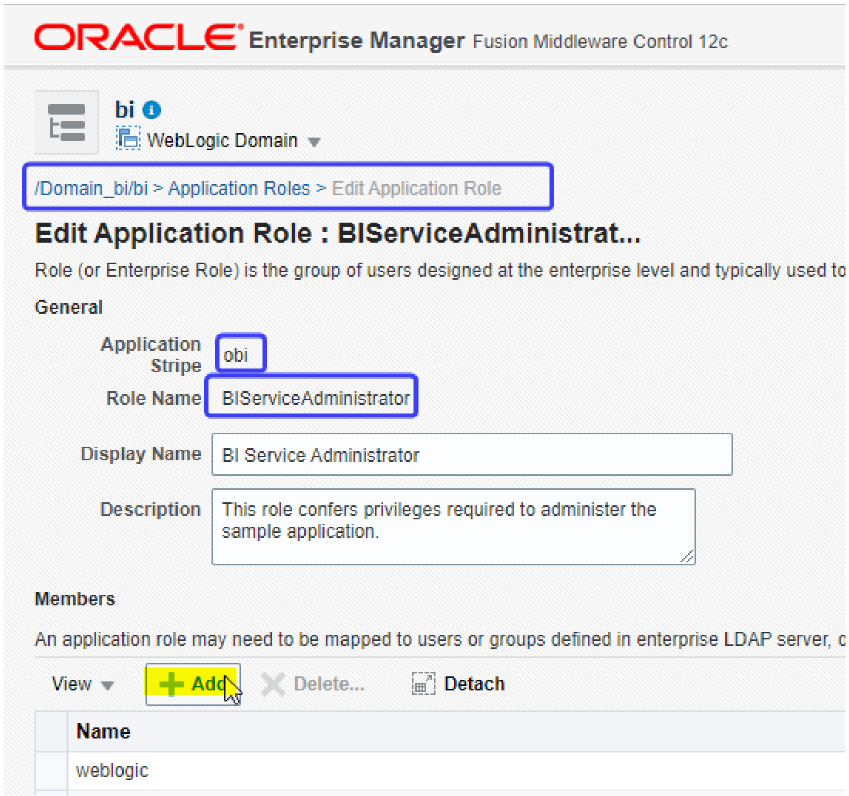
Role Name: Starts With

View ▾ | Create... | Create Like... | Edit... | Delete...

Edit the selected application role

Role Name	Display Name	Description
BIDataModelAuthor	BI Data Model Author	Users with this role
DVConsumer	DV Consumer	Users granted this
BIContentAuthor	BI Content Author	Users with this role
BIDataLoadAuthor	BI Dataload Author	Users with this role
DVContentAuthor	DV Content Author	Users with this role
BIConsumer	BI Consumer	Users granted this
BIServiceAdministrator	BI Service Administrator	This role confers p
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	This role contains

Step 2, Part 4 - Click Add to add a role mapping



ORACLE Enterprise Manager Fusion Middleware Control 12c

bi

WebLogic Domain

/Domain_bi/bi > Application Roles > Edit Application Role

Edit Application Role : BIServiceAdministrat...

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically used to

General

Application Stripe: obi

Role Name: BIServiceAdministrator

Display Name: BI Service Administrator

Description: This role confers privileges required to administer the sample application.

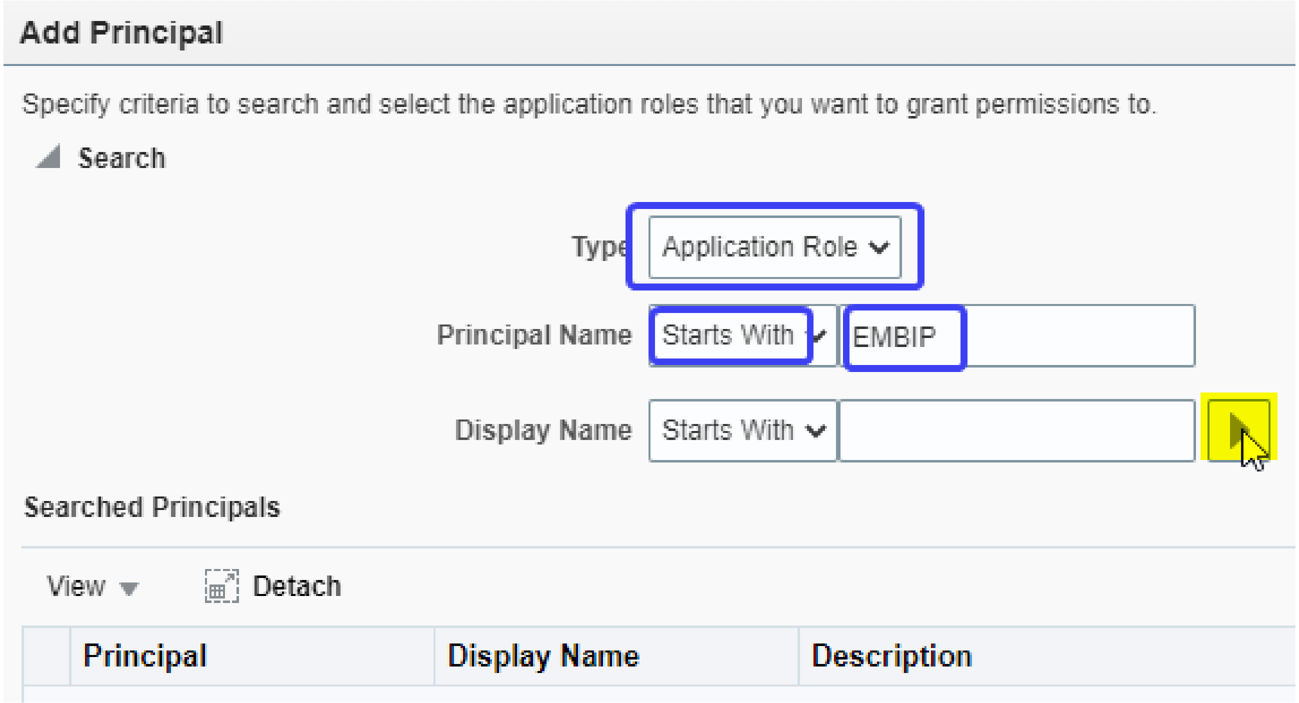
Members

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

View ▾ | Add | Delete... | Detach

Name
weblogic

Step 2, Part 5 - Search for the EMBIP roles



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: Application Role

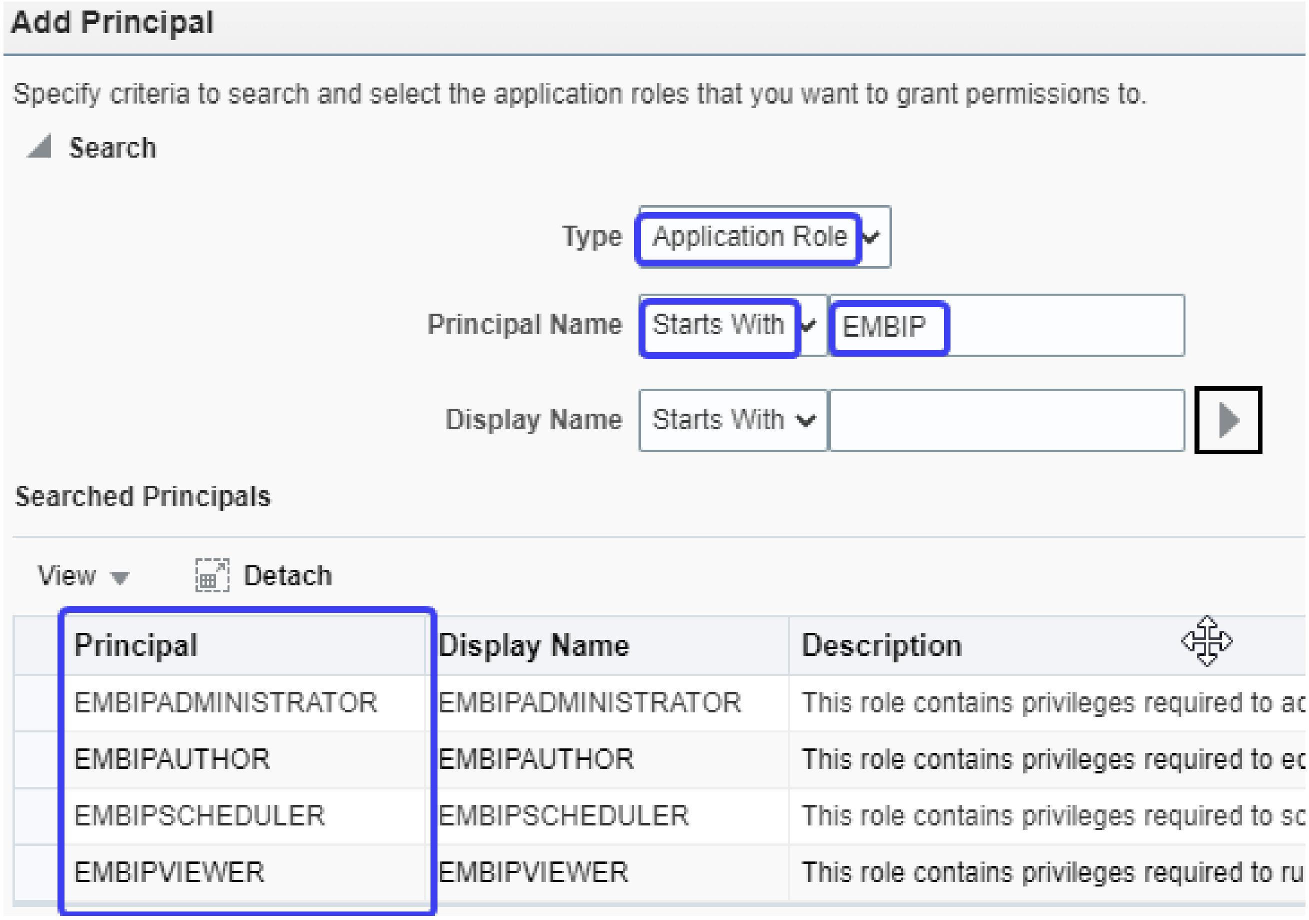
Principal Name: Starts With, EMBIP

Display Name: Starts With

Searched Principals

Principal	Display Name	Description

Step 2, Part 6 - Results of the search



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: Application Role

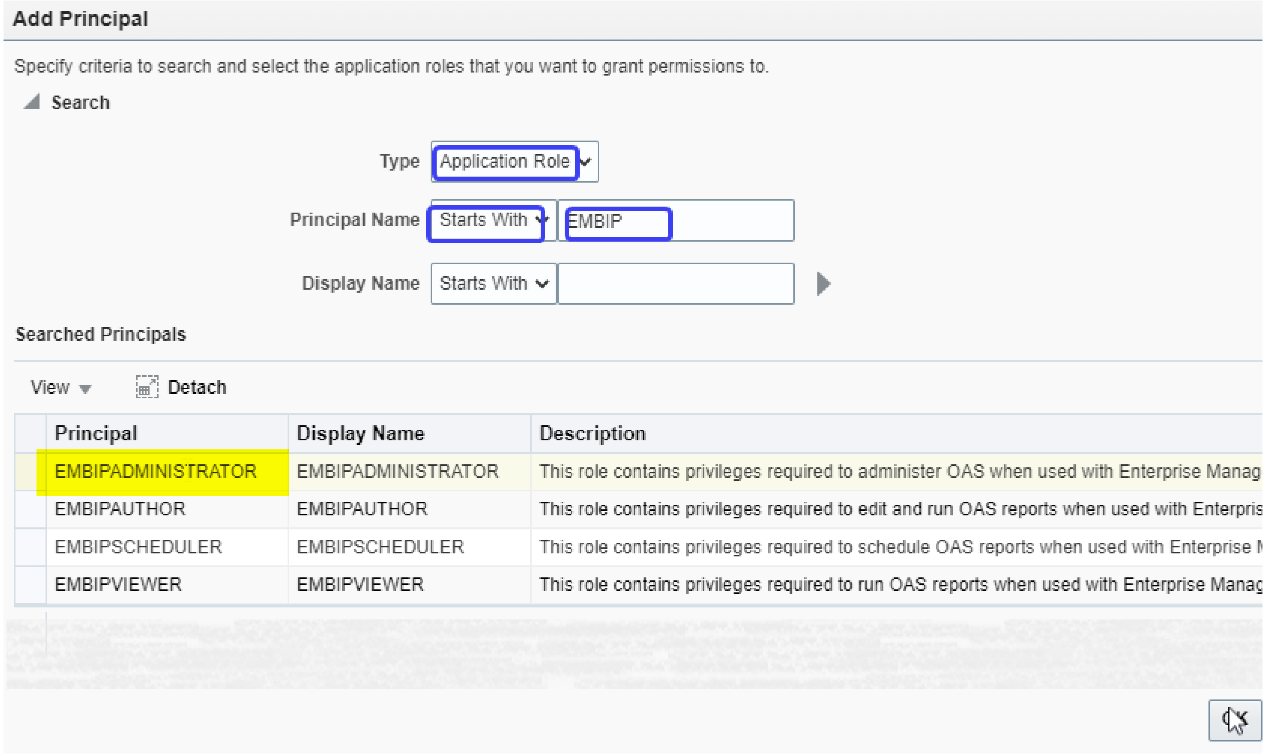
Principal Name: Starts With, EMBIP

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	This role contains privileges required to ac
EMBIPAUTHOR	EMBIPAUTHOR	This role contains privileges required to ec
EMBIPSCHEDULER	EMBIPSCHEDULER	This role contains privileges required to sc
EMBIPVIEWER	EMBIPVIEWER	This role contains privileges required to ru

Step 2, Part 7 - Select the EMBIPADMINISTRATOR role and click OK



Add Principal

Specify criteria to search and select the application roles that you want to grant permissions to.

Search

Type: Application Role

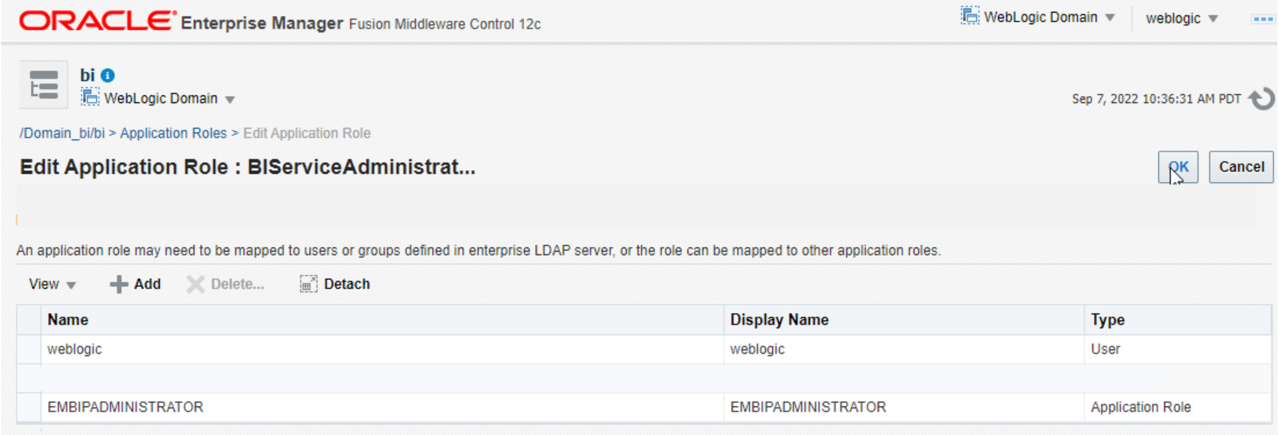
Principal Name: Starts With EMBIP

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	This role contains privileges required to administer OAS when used with Enterprise Manag
EMBIPAUTHOR	EMBIPAUTHOR	This role contains privileges required to edit and run OAS reports when used with Enterpris
EMBIPSCHEDULER	EMBIPSCHEDULER	This role contains privileges required to schedule OAS reports when used with Enterprise M
EMBIPVIEWER	EMBIPVIEWER	This role contains privileges required to run OAS reports when used with Enterprise Manag

Step 2, Part 8 - The New list is shown. press OK



Sep 7, 2022 10:36:31 AM PDT

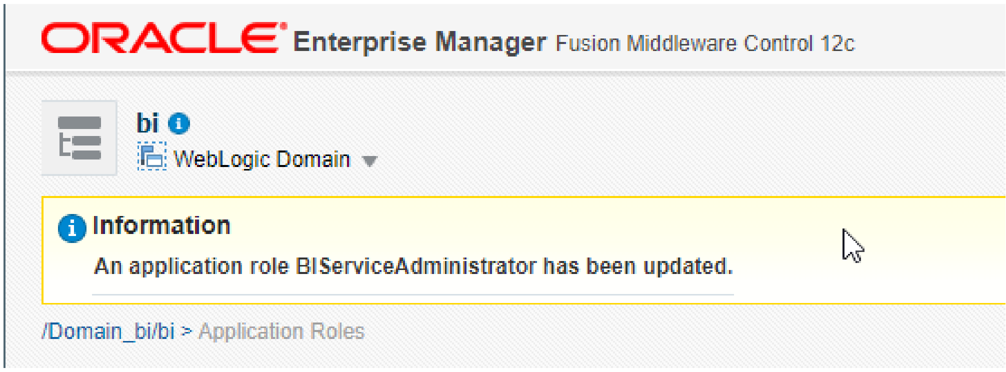
/Domain_bi/bi > Application Roles > Edit Application Role

Edit Application Role : BIServiceAdministrat...

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

Name	Display Name	Type
weblogic	weblogic	User
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	Application Role

Step 2, Part 9 - Confirmation



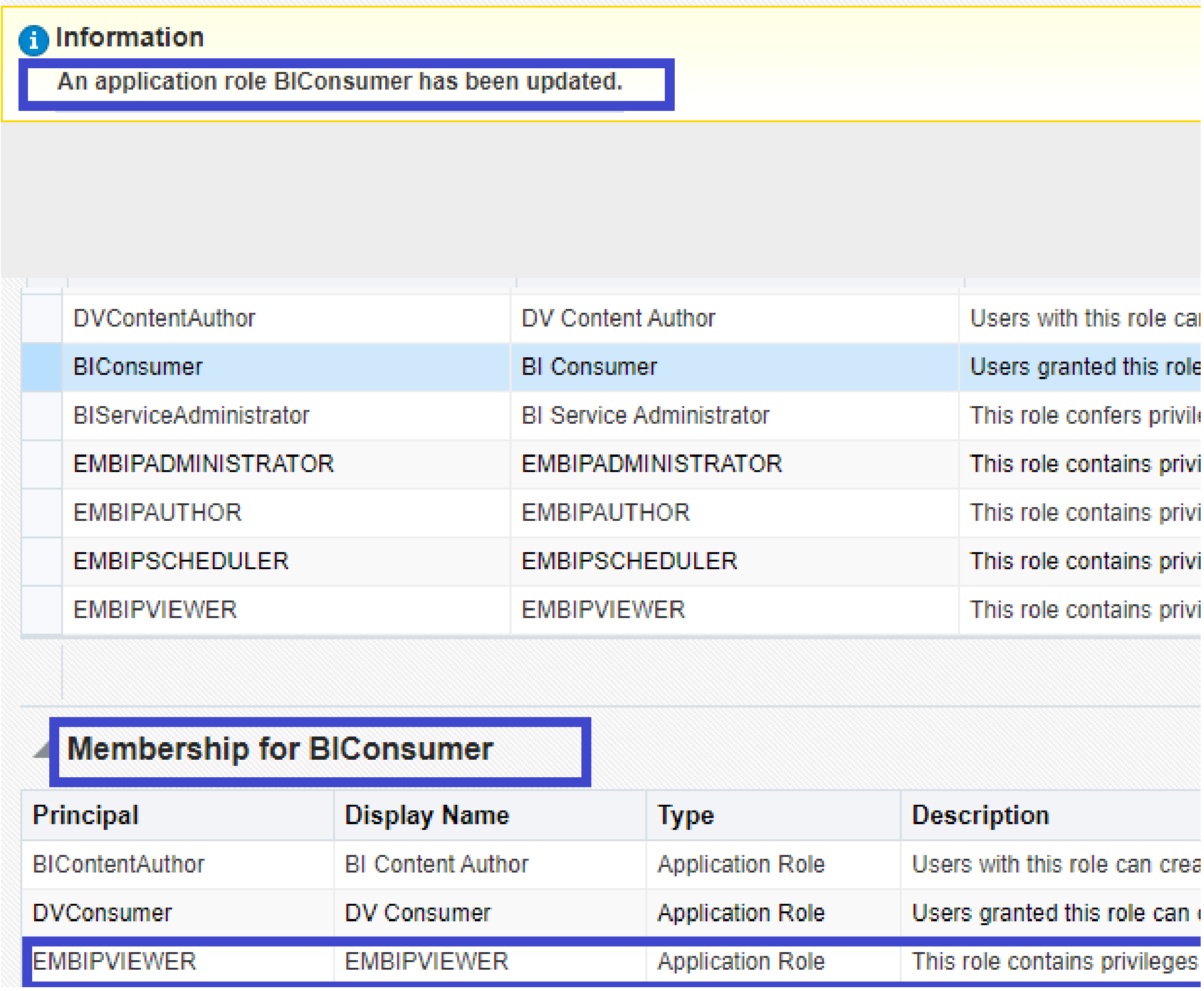
Information

An application role BIServiceAdministrator has been updated.

/Domain_bi/bi > Application Roles

Step 3 -Repeat step 2 twice more, for the other EMBIP roles: Completed Screen Shots Shown

1. EMBIPAUTHOR



Information

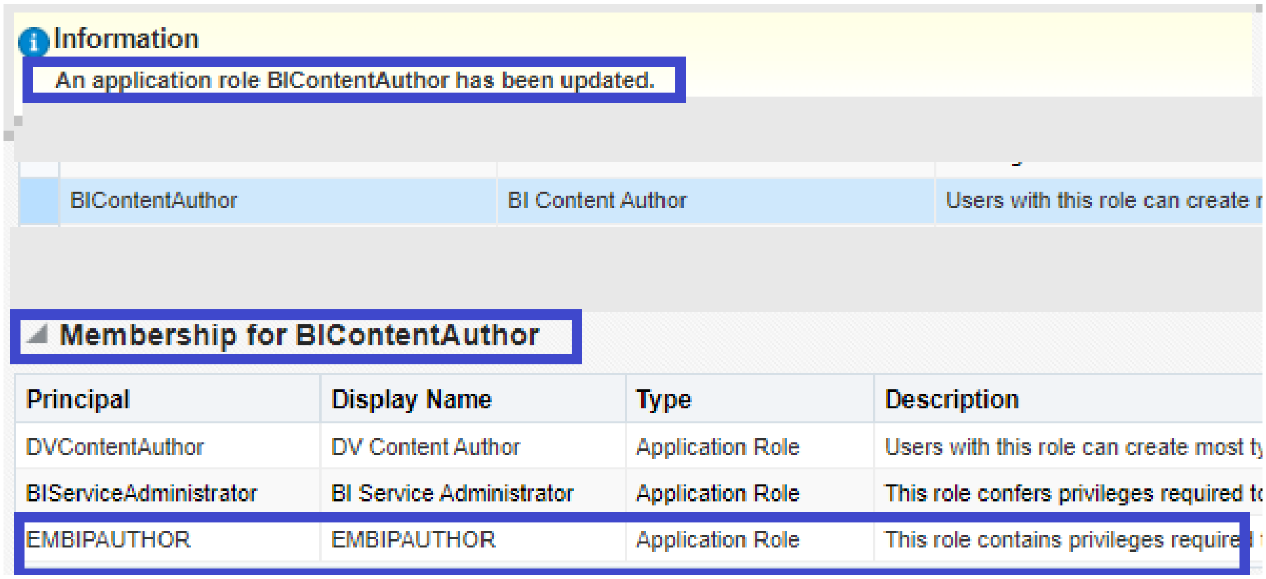
An application role BIConsumer has been updated.

DVContentAuthor	DV Content Author	Users with this role car
BIConsumer	BI Consumer	Users granted this role
BIServiceAdministrator	BI Service Administrator	This role confers privile
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	This role contains privi
EMBIPAUTHOR	EMBIPAUTHOR	This role contains privi
EMBIPSCHEDULER	EMBIPSCHEDULER	This role contains privi
EMBIPVIEWER	EMBIPVIEWER	This role contains privi

Membership for BIConsumer

Principal	Display Name	Type	Description
BIContentAuthor	BI Content Author	Application Role	Users with this role can crea
DVConsumer	DV Consumer	Application Role	Users granted this role can
EMBIPVIEWER	EMBIPVIEWER	Application Role	This role contains privileges

2. EMBIPVIEWER



Information

An application role BIContentAuthor has been updated.

BIContentAuthor	BI Content Author	Users with this role can create r

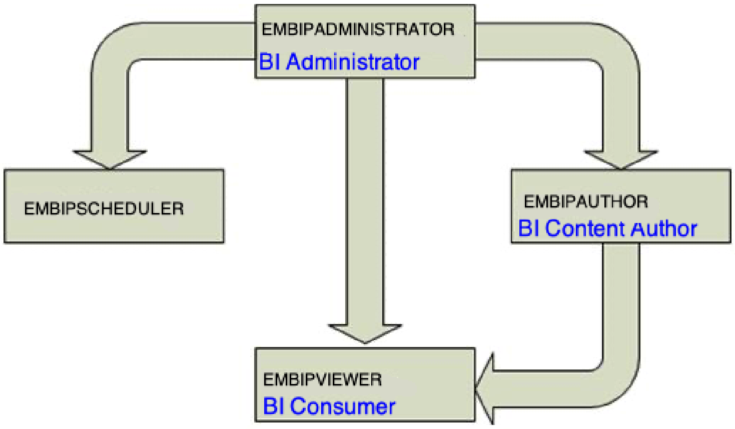
Membership for BIContentAuthor

Principal	Display Name	Type	Description
DVContentAuthor	DV Content Author	Application Role	Users with this role can create most ty
BIServiceAdministrator	BI Service Administrator	Application Role	This role confers privileges required to
EMBIPAUTHOR	EMBIPAUTHOR	Application Role	This role contains privileges required

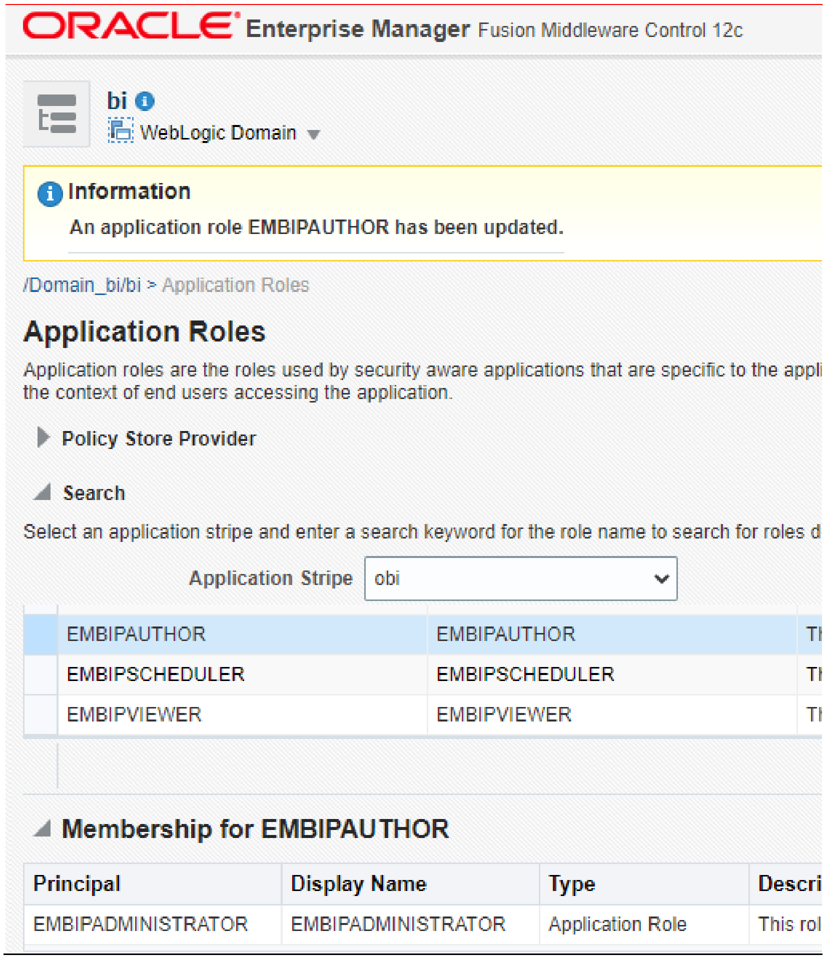
Step 4 – Configure Role Hierarchy for EM roles (EMBIP*)

Referring to '**Error! Reference source not found.**- **Error! Reference source not found.**', the roles created in the prior step need to be repeated for the specific EMBIP* roles.

```
  EMBIPAUTHOR role       requires EMBIPADMINISTRATOR           as a member.
EMBIPSCHEDULER role       requires EMBIPADMINISTRATOR           as a member.
  EMBIPVIEWER role       requires EMBIPAUTHOR                  as a member.
```



An example showing the proper membership for the EMBIPAUTHOR role is shown below:



Information

An application role EMBIPAUTHOR has been updated.

/Domain_bi/bi > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the appli
the context of end users accessing the application.

Policy Store Provider

Search

Select an application stripe and enter a search keyword for the role name to search for roles d

Application Stripe: obi

EMBIPAUTHOR	EMBIPAUTHOR	Th
EMBIPSCHEDULER	EMBIPSCHEDULER	Th
EMBIPVIEWER	EMBIPVIEWER	Th

Membership for EMBIPAUTHOR

Principal	Display Name	Type	Descri
EMBIPADMINISTRATOR	EMBIPADMINISTRATOR	Application Role	This rol

Step 5 – Summary

Allowing additional Enterprise Manager Administrators access to Oracle Analytics Publisher

Once all the prior steps are completed, the basic role hierarchy that is required for proper management and execution of the Oracle provided reports that are installed alongside Enterprise Manager 24ai.

However, for individual Enterprise Manager administrators to have access to the various required permissions, these Enterprise Manager administrators need to be granted membership in one of the specified roles.

As a simple example, if the EM administrator named EMBIP_VIEWER1 needs to be able to execute Oracle provided reports, then EM administrator EMBIP_VIEWER1 needs to be granted membership in the EMBIPVIEWER application role.

Likewise, if the EM administrator named EMBIP_AUTHOR1 needs to be able to edit and create private reports, then the EM administrator EMBIP_AUTHOR1 needs to be granted membership in the EMBIPAUTHOR role.

Migrating customized Reports from OAP 6.4

In addition to support for the Oracle provided out of box reports, customized reports developed in OAS 6.4, for use with EM 13.5, can be migrated to OAS 24 (7.6)

The standard process for this, using BIP or OAS, is to download the report from the prior release, and upload the report to the current release.

CHAPTER 8. UPLOADING ENTERPRISE MANAGER PROVIDED REPORTS

Framework Reports

The Enterprise Manager Provided Reports for the base framework will be in the MW_HOME in which EM 24 is installed.

```
$ ls -sh $MW_HOME/sysman/jlib/Enterprise\ Manager\ Cloud\ Control.xdrz
2.5M ..../sysman/jlib/Enterprise Manager Cloud Control.xdrz
```

Plugin Reports

Each EM plugin that is bundled with EM Provided Out of Box Reports, whether installed during the initial install/upgrade of EM 24, or subsequently installed via self-update or other mechanism, will follow this pattern:

```
$ ls -sh $MW_HOME/plugins/oracle.sysman.*.plugin_24*/metadata/bipublisherreport/emreports/*.xdrz
2.0M '../plugins/oracle.sysman.../bipublisherreport/emreports/Enterprise Manager Cloud Control.xdrz'
216K '../plugins/oracle.sysman.../bipublisherreport/emreports/Enterprise Manager Cloud Control.xdrz'
...  ...
```

Common File name for all Oracle Provided Out of Box Reports

Each set of these out-of-box reports has the name below, which facilitates straightforward upgrades to the standalone OAS installation:

```
Enterprise Manager Cloud Control.xdrz
```

Bundle Enterprise Manager 24 Out of Box Reports

In preparation for uploading the EM provided reports, copy all instances of files named **`Enterprise Manager Cloud Control.xdrz`** from the EM 13.5 MW_HOME, to your local desktop (i.e., using putty, scp, etc…).

On Linux systems, these files can be located using these commands:

```
cd $MW_HOME
tar cvf $HOME/emreports.tar "`find . -name Enterprise\ Manager\ Cloud\ Control.xdrz`"
./sysman/jlib/Enterprise Manager Cloud Control.xdrz
./plugins/oracle.sysman.cfw.oms.plugin_24.1.1.0.0/metadata/bipublisherreport/emreports/Enterprise Manager Cloud Control.xdrz
...
...
./plugins/oracle.sysman.db.oms.plugin_24.1.1.0.0/metadata/bipublisherreport/emreports/Enterprise Manager Cloud Control.xdrz
```

Figure 21. Locating Oracle Provided BI Publisher Reports in Enterprise Manager 13.5 Oracle Home

Once all XDRZ files are copied to your local desktop, one may see the following structure

```
.
├── [     8]  plugins
│   ├── [     3]  oracle.sysman.am.oms.plugin_24.1.1.0.0
│   │   └── [     3]  metadata
│   │       └── [     3]  bipublisherreport
│   │           └── [     3]  emreports
│   │               └── [ 1.9M]  Enterprise\ Manager\ Cloud\ Control.xdrz
│   ├── [     3]  oracle.sysman.cfw.oms.plugin_24.1.1.0.0
│   │   └── [     3]  metadata
│   │       └── [     3]  bipublisherreport
│   │           └── [     3]  emreports
│   │               └── [ 215K]  Enterprise\ Manager\ Cloud\ Control.xdrz
│   ├── [     3]  oracle.sysman.db.oms.plugin_24.1.1.0.0
│   │   └── [     3]  metadata
│   │       └── [     3]  bipublisherreport
│   │           └── [     3]  emreports
│   │               └── [ 1.4M]  Enterprise\ Manager\ Cloud\ Control.xdrz
│   ├── [     3]  oracle.sysman.emas.oms.plugin_24.1.1.0.0
│   │   └── [     3]  metadata
│   │       └── [     3]  bipublisherreport
│   │           └── [     3]  emreports
│   │               └── [ 3.1M]  Enterprise\ Manager\ Cloud\ Control.xdrz
│   ├── [     3]  oracle.sysman.emct.oms.plugin_24.1.1.0.0
│   │   └── [     3]  metadata
│   │       └── [     3]  bipublisherreport
│   │           └── [     3]  emreports
│   │               └── [ 460K]  Enterprise\ Manager\ Cloud\ Control.xdrz
│   └── [     3]  oracle.sysman.xa.oms.plugin_24.1.1.0.0
│       └── [     3]  metadata
│           └── [     3]  bipublisherreport
│               └── [     3]  emreports
│                   └── [ 1.5M]  Enterprise\ Manager\ Cloud\ Control.xdrz
└── [     3]  sysman
    └── [     3]  jlib
        └── [ 2.4M]  Enterprise\ Manager\ Cloud\ Control.xdrz

27 directories, 7 files
```

Figure 22. Example layout of Enterprise Manager 13.5 Provided Out-of-Box Reports

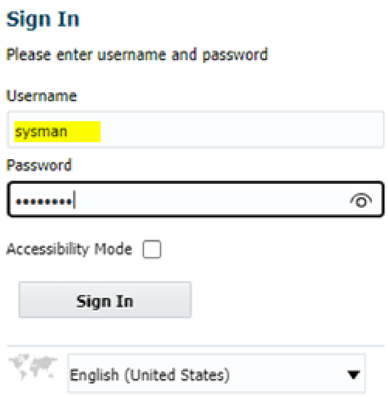
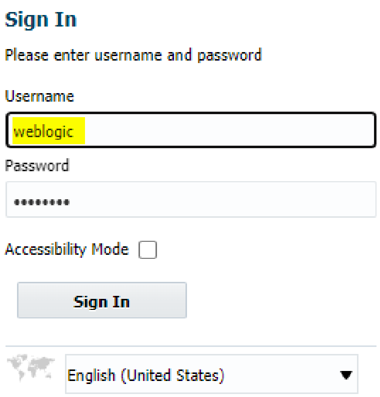
Once the example layout above is created on your local desktop system, these set(s) can then be directly uploaded to the new OAS installation using the standard OAS upload process.

Any subsequent updates or patching of Enterprise Manager out-of-box reports would be done using the standard OAS user interface, against one or more reports.

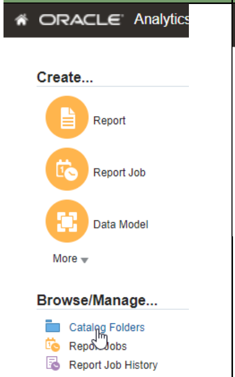
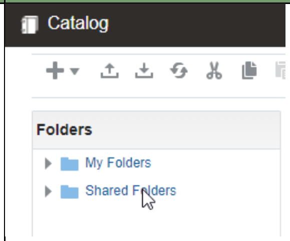
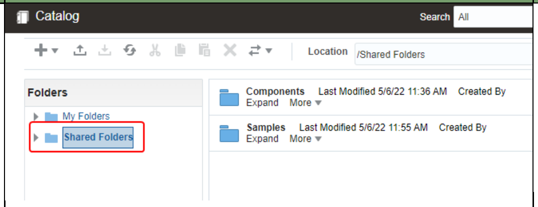
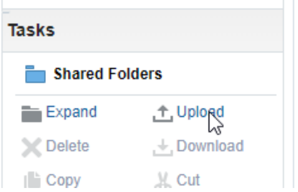
The following screenshots demonstrate some examples of uploading these out-of-box reports.

8.1 Upload Oracle Provided Out-of-box Reports to standalone OAS

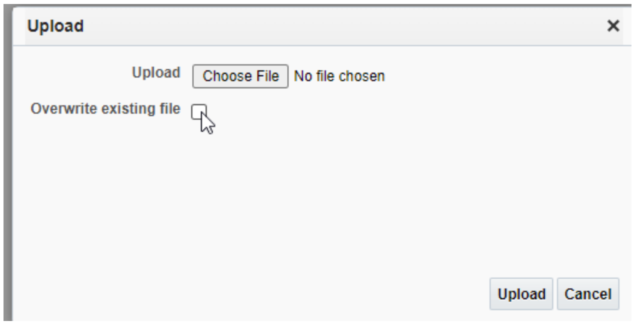
Step 1 - Login to the standalone OAS as a user with OAS Administrator privileges.

OAS for EM Repository-Based Security	OAS for LDAP Based Security
	
Sign In Please enter username and password Username: sysman Password: •••••••• Accessibility Mode □ Sign In English (United States)	Sign In Please enter username and password Username: weblogic Password: •••••••• Accessibility Mode □ Sign In English (United States)

Steps 2 through 5 - Prepare to Upload to Shared Folders

1. Navigate to Catalog	2. Navigate to Shared Folders	3. Make sure Shared Folders is highlighted	4. Select Upload
			

Steps 5 and 6 – Choose to upload the Reports - Ensure to select 'Overwrite Existing file'

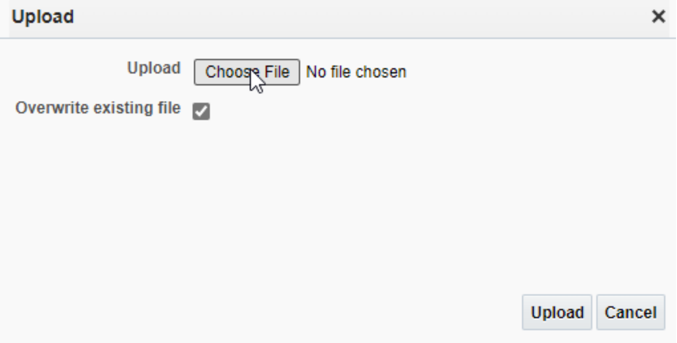


Upload

Upload: Choose File No file chosen

Overwrite existing file □

Upload Cancel



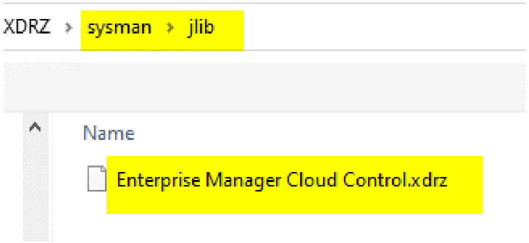
Upload

Upload: Choose File No file chosen

Overwrite existing file ☑

Upload Cancel

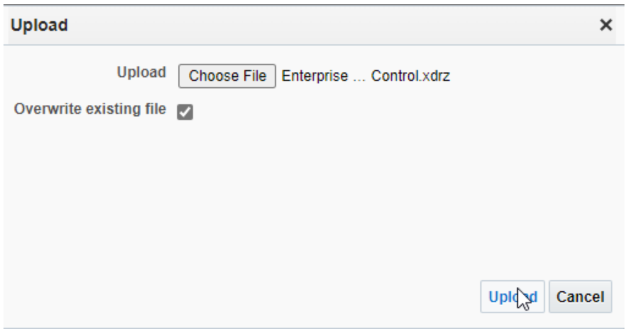
Step 7 and 8 – Choose the Platform Reports



XDRZ › sysman › jlib

Name

Enterprise Manager Cloud Control.xdrz

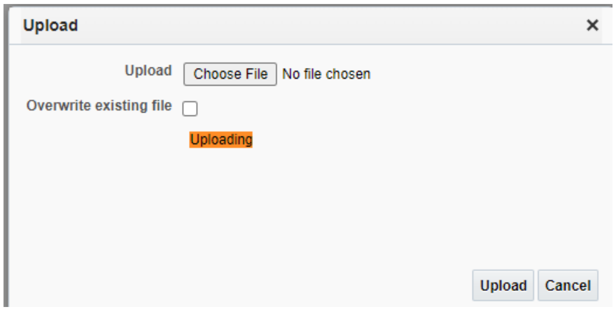


Upload

Upload: Choose File Enterprise ... Control.xdrz

Overwrite existing file ☑

Steps 9 and 10 - Uploading status is shown, and in a few minutes, Upload Completed is shown.

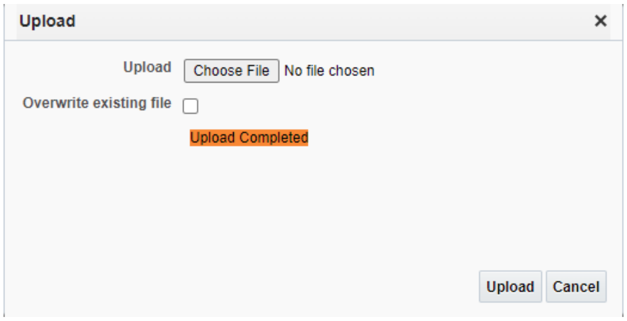


Upload

Upload: Choose File No file chosen

Overwrite existing file □

Uploading



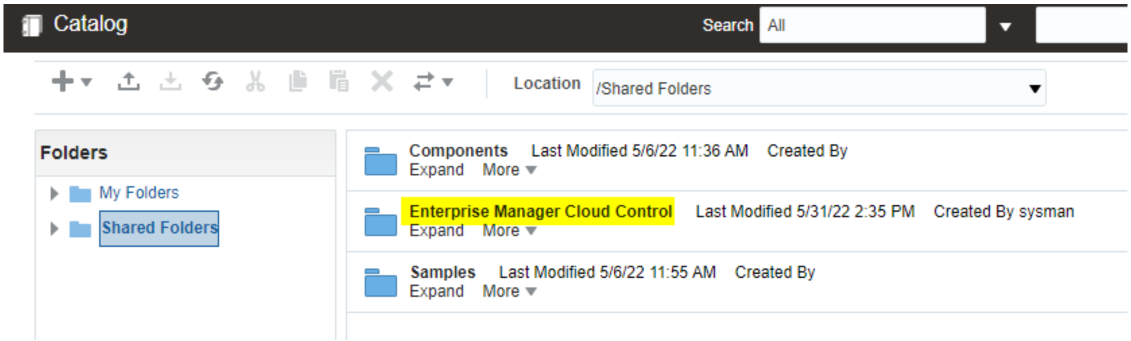
Upload

Upload: Choose File No file chosen

Overwrite existing file □

Upload Completed

Step 11 – Operation Completed



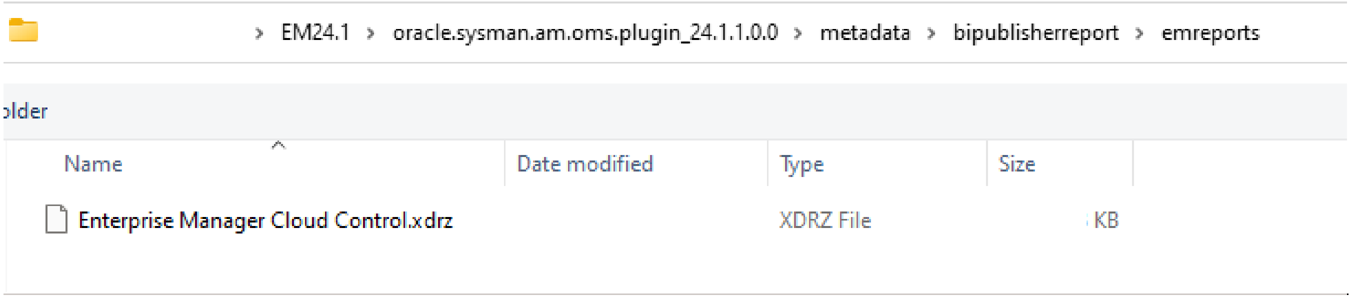
Location /Shared Folders

Components Last Modified 5/6/22 11:36 AM Created By
Expand More

Enterprise Manager Cloud Control Last Modified 5/31/22 2:35 PM Created By sysman
Expand More

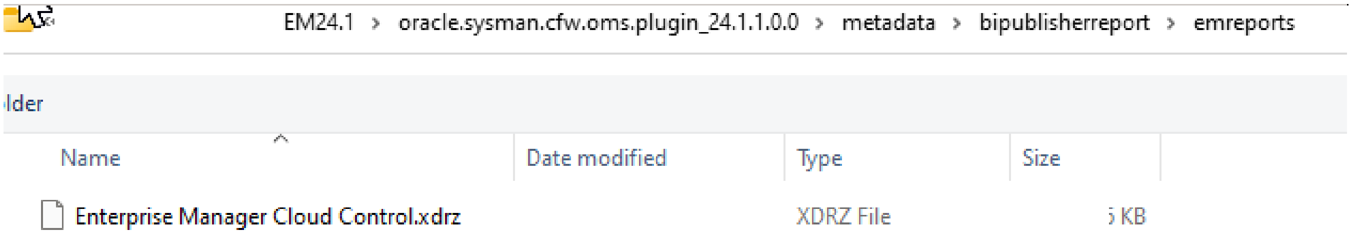
Samples Last Modified 5/6/22 11:55 AM Created By
Expand More

Repeat the above procedure for each EM plugin



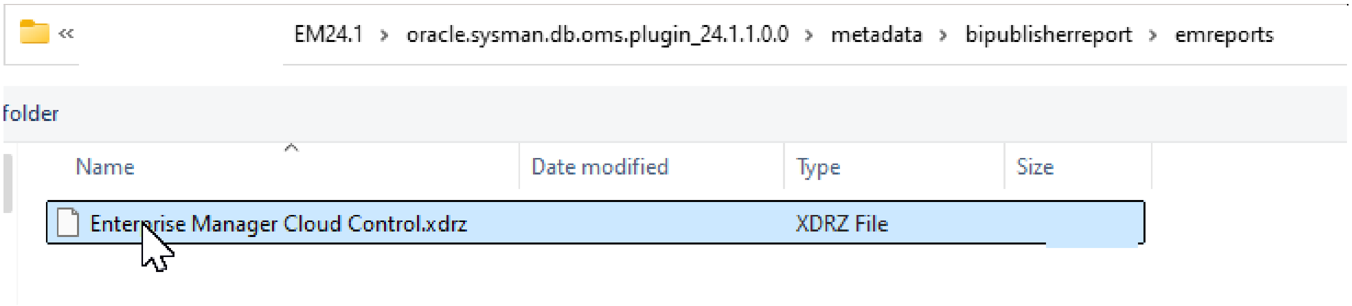
› EM24.1 › oracle.sysman.am.oms.plugin_24.1.1.0.0 › metadata › bipublisherreport › emreports

Name	Date modified	Type	Size
Enterprise Manager Cloud Control.xdrz		XDRZ File	KB



EM24.1 › oracle.sysman.cfw.oms.plugin_24.1.1.0.0 › metadata › bipublisherreport › emreports

Name	Date modified	Type	Size
Enterprise Manager Cloud Control.xdrz		XDRZ File	5 KB



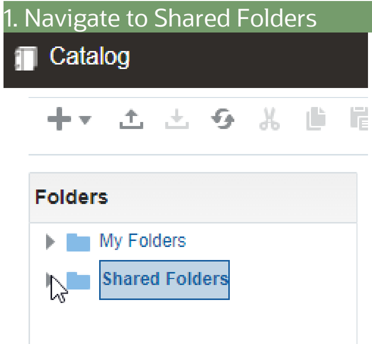
EM24.1 › oracle.sysman.db.oms.plugin_24.1.1.0.0 › metadata › bipublisherreport › emreports

Name	Date modified	Type	Size
Enterprise Manager Cloud Control.xdrz		XDRZ File	

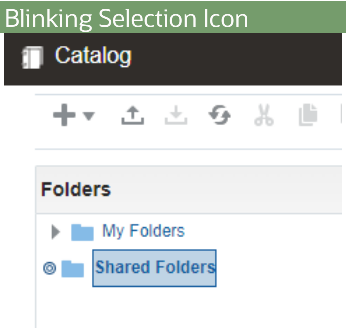
Verify Sample Report

- This series of 4 steps demonstrate testing the sample report.

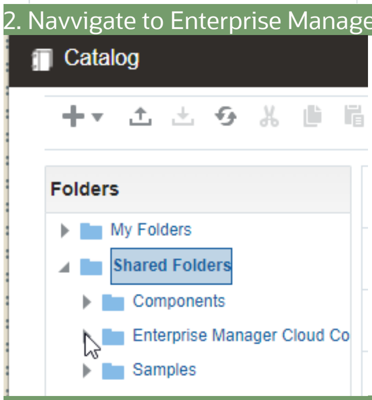
1. Navigate to Shared Folders



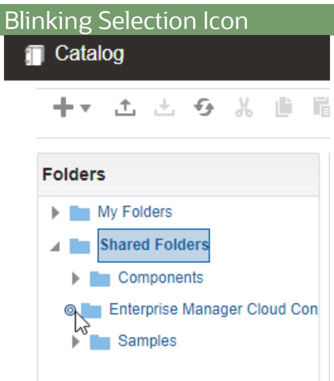
Blinking Selection Icon



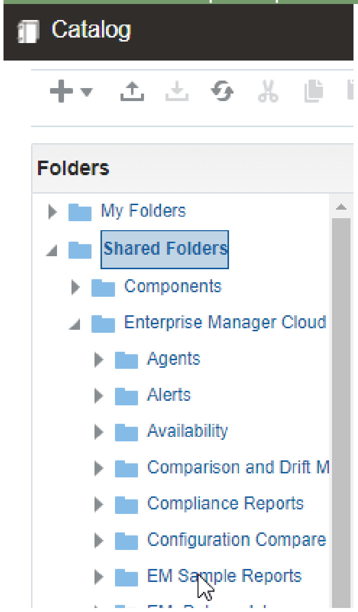
2. Navvigate to Enterprise Manager Cloud Control Folder



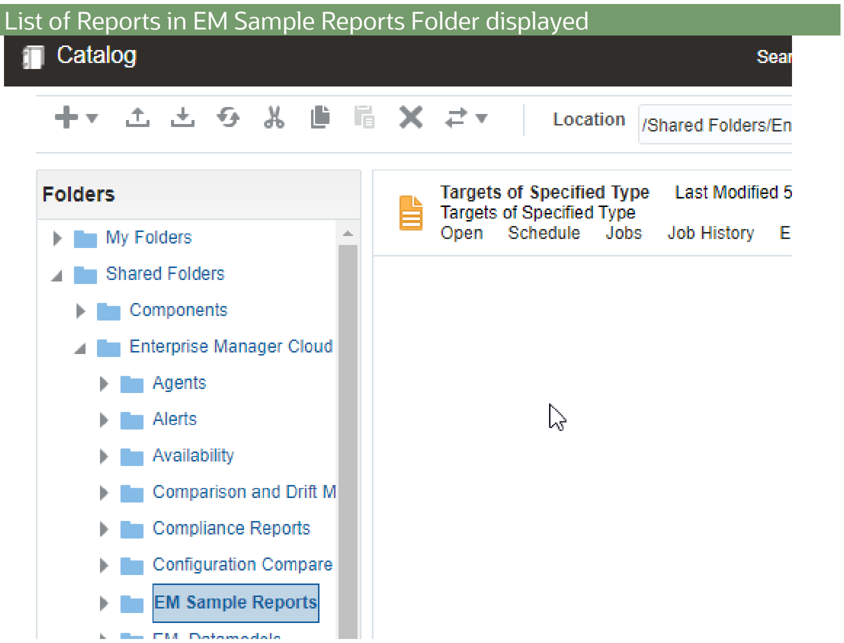
Blinking Selection Icon



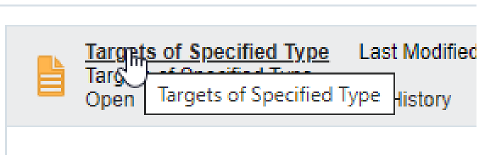
3. Click on EM Sample Reports



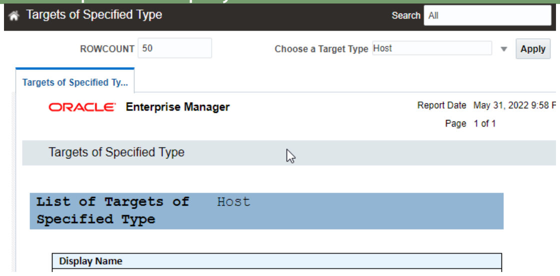
List of Reports in EM Sample Reports Folder displayed



4. Click on the "Targets of Specified Type" Report



The Report is Displayed



8.2 Steps to complete after uploading the Enterprise Manager Provided Reports

In certain circumstances, the OAS catalog's root folder, which is displayed in the user interface via the Shared Folders icon, does not have the correct permissions.

The symptom of this would be for OAS users without the Super Admin privilege (either BI Administrator, EMBIPADMINISTRATOR, or XMLP_ADMIN, depending on the security model) will be unable to see the reports that were just uploaded.

There can be circumstances that arise from time to time when the same behavior can be exhibited for customized reports that are either developed directly in OAS, or uploaded to OAS, show this same behavior.

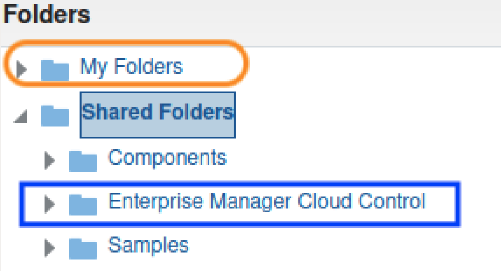
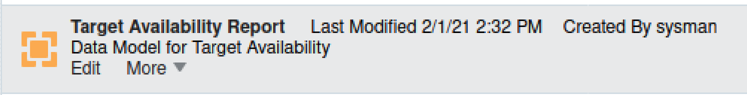
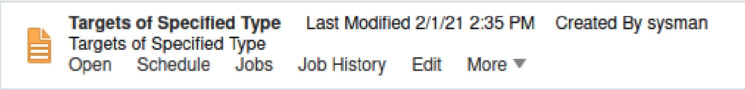
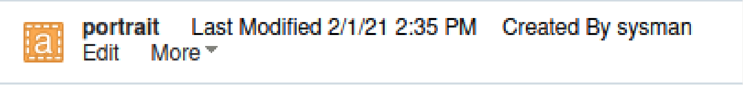
In order to repair or set appropriate permissions for an OAS Catalog Object, note the four types of Catalog Objects that are available.

OAS Catalog Object Types

Every OAS catalog Object has an associated set of permissions, which are derived from the set of available roles.

Note that the roles are stored as appropriate, depending on the OAS Security Model.

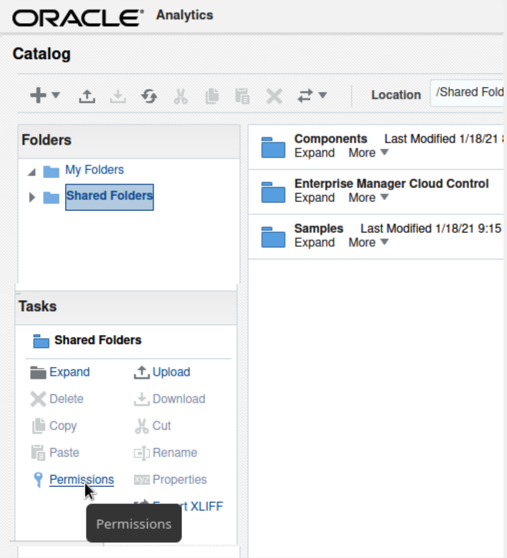
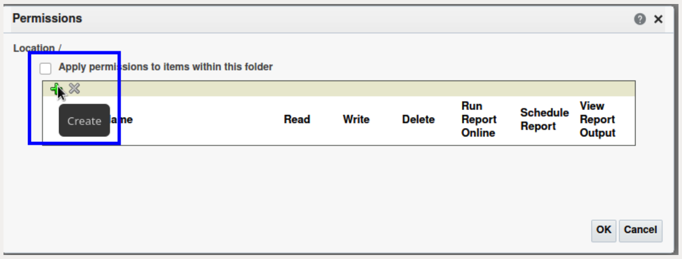
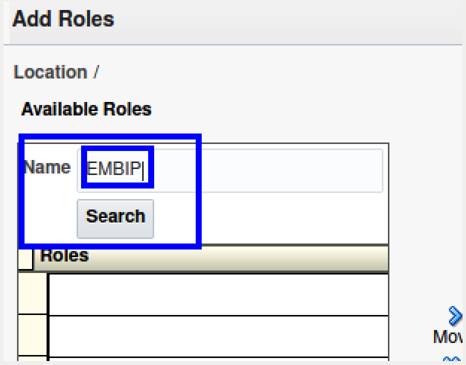
Review '**Error! Reference source not found.**- **Error! Reference source not found.**' for review.

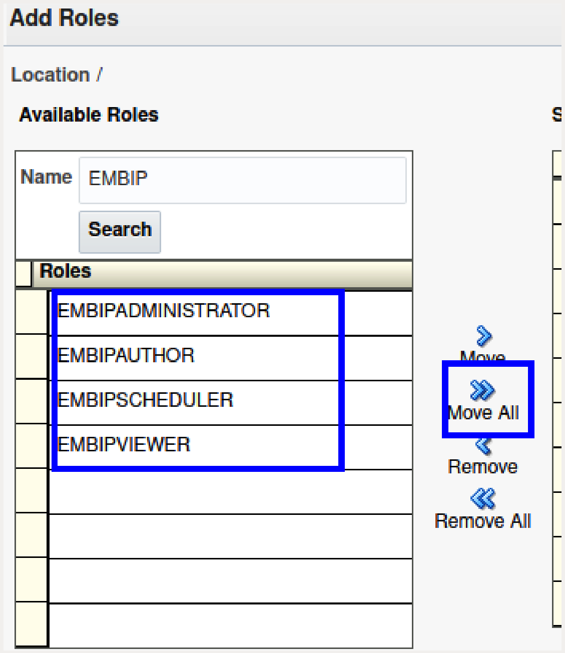
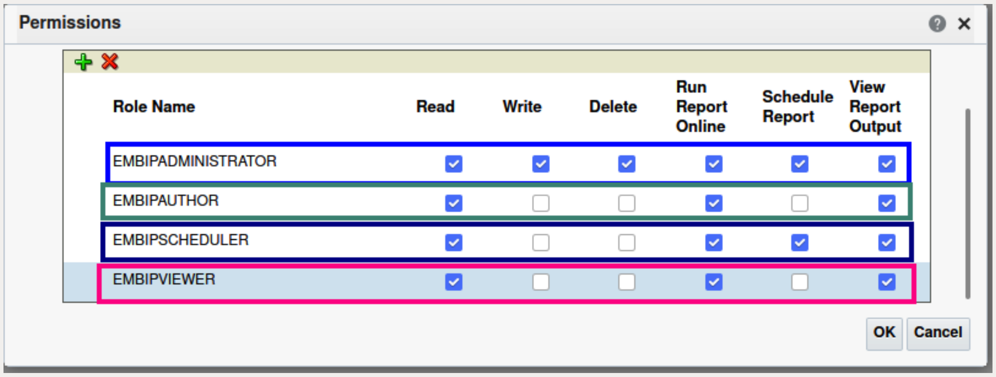
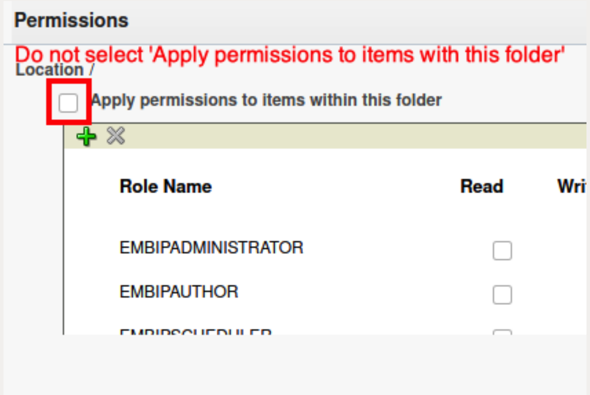
Object	**Comment**	**Screenshot**
Folder	Root of My Folders tree. A subfolder of Shared Folders.	 Folders My Folders Shared Folders Components Enterprise Manager Cloud Control Samples
Datamodel	SQL Queries against EM repository data.	 **Target Availability Report** Last Modified 2/1/21 2:32 PM Created By sysman Data Model for Target Availability Edit More
Report	Layout and properties for viewing report content.	 **Targets of Specified Type** Last Modified 2/1/21 2:35 PM Created By sysman Targets of Specified Type Open Schedule Jobs Job History Edit More
Subtemplate	Can be included by Report's (i.e., for headers/footers).	 **portrait** Last Modified 2/1/21 2:35 PM Created By sysman Edit More

Resolving Permissions issues against one or more OAS Catalog Object(s)

As a user with OAS super admin privileges (i.e., sysman, weblogic, etc...), navigate to the OAS Catalog Object that needs to have its catalog permissions set or reset.

For this example, The Shared Folders OAS Catalog Object is demonstrated:

Step	Screenshot
1. Select Shared Folders **2. Do not highlight any other items.** 3. Press Permissions link.	 Location /Shared Fold ORACLE Analytics Catalog Location Folders My Folders Shared Folders Components Last Modified 1/18/21 Expand More Enterprise Manager Cloud Control Expand More Samples Last Modified 1/18/21 9:15 Expand More Tasks Shared Folders Expand Upload Delete Download Copy Cut Paste Rename Permissions Properties rt XLIFF Permissions
4. An empty list. 5. Press the **+** sign.	 Location / □ Apply permissions to items within this folder Permissions Create ame Read Write Delete Run Report Online Schedule Report View Report Output OK Cancel
6. Enter EMBIP in Name. 7. Press Search button.	 Location / Name EMBIP

Step	Screenshot
8. List shown. 9. Press Move All	 Add Roles Location / Available Roles Name EMBIP Search Roles EMBIPADMINISTRATOR EMBIPAUTHOR EMBIPSCHEDULER EMBIPVIEWER Move Move All Remove Remove All
10. Fill to match the screen shot.	 Permissions Role Name — Read — Write — Delete — Run Report Online — Schedule Report — View Report Output EMBIPADMINISTRATOR ☑ ☑ ☑ ☑ ☑ ☑ EMBIPAUTHOR ☑ ☐ ☐ ☑ ☐ ☑ EMBIPSCHEDULER ☑ ☐ ☐ ☑ ☑ ☑ EMBIPVIEWER ☑ ☐ ☐ ☑ ☐ ☑ OK Cancel
11. If this checkbox is selected, the catalog operation can take significantly more time. 12. Only select this checkbox if it is required.	 Permissions Do not select 'Apply permissions to items with this folder' Location / ☐ Apply permissions to items within this folder Role Name — Read — Wri EMBIPADMINISTRATOR ☐ EMBIPAUTHOR ☐

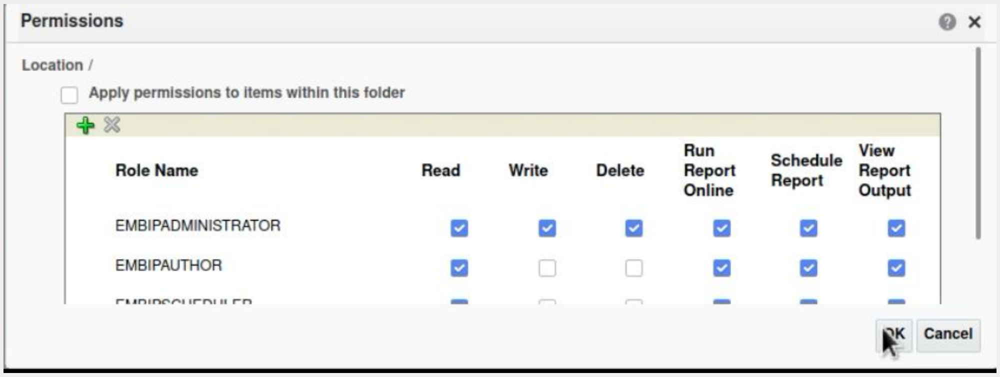
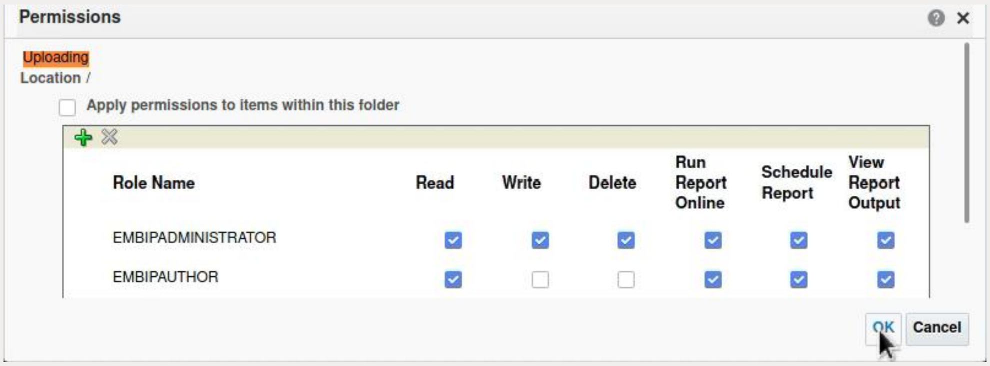
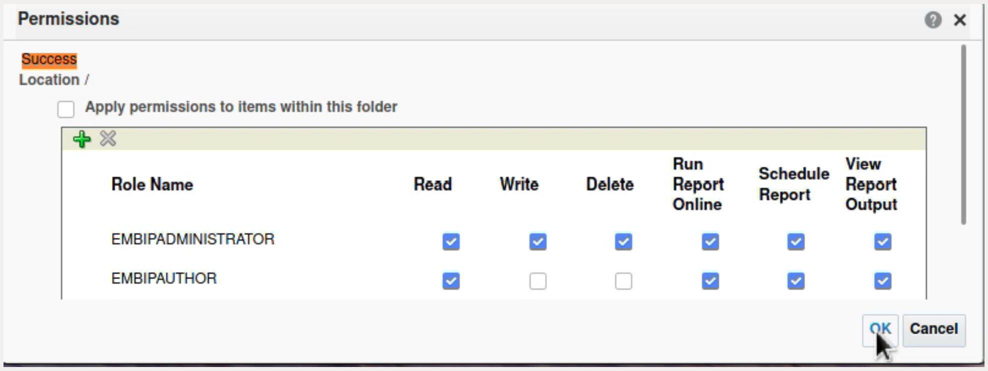
Step	Screenshot
13. Press OK	 Permissions Location / □ Apply permissions to items within this folder Role Name — Read — Write — Delete — Run Report Online — Schedule Report — View Report Output EMBIPADMINISTRATOR ☑ ☑ ☑ ☑ ☑ ☑ EMBIPAUTHOR ☑ □ □ ☑ ☑ ☑ OK Cancel
14. Uploading	 Permissions Uploading Location / □ Apply permissions to items within this folder Role Name — Read — Write — Delete — Run Report Online — Schedule Report — View Report Output EMBIPADMINISTRATOR ☑ ☑ ☑ ☑ ☑ ☑ EMBIPAUTHOR ☑ □ □ ☑ ☑ ☑ OK Cancel
15. Success	 Permissions Success Location / □ Apply permissions to items within this folder Role Name — Read — Write — Delete — Run Report Online — Schedule Report — View Report Output EMBIPADMINISTRATOR ☑ ☑ ☑ ☑ ☑ ☑ EMBIPAUTHOR ☑ □ □ ☑ ☑ ☑ OK Cancel

Table 7. Ensure correct Catalog Permissions for OAS Shared Folder

8.3 Reminder On Required Roles for EM Administrators

Anytime that a new Enterprise Manager Administrator is configured, refer to the relevant section, depending on whether Repository Based Authentication, or LDAP Based Authentication, for the steps to provide access to this new EM user.

CHAPTER 9. MIGRATING BIP SCHEDULES FROM STANDALONE OAS 6.4

The standalone OAS provides a script to perform this migration.

They are fully documented in the respective OAS documentation. *** ADD REFERENCE ****

Arguments for OAS Scheduler Migration Script

Context	Argument Value (color coded)	Comments
SQL*plus invocation	sys	The sysdba username usually "sys"
SQL*plus invocation	●●●●●●●●	SYSDBA Password
SQL*plus invocation	@oasrepos.example.com:1521/orcl	The connect descriptor would be the value of the "**Simple connect string**" in the screenshot above, reformatted for use with SQL*plus. oasrepos.example.com:1521/orcl
SQL Script Execution	sysman_biplatform	EM 13.4 Embedded BIP Schema Username.
SQL Script Execution	●●●●●●●	The "**sysman**" User's password.
SQL Script Execution	emrepos1.example.com:1521/orcl.example.com	This value would the same as entered in highlighted value from "0- Part 5 - Fill in the required details": Connection String: jdbc:oracle:thin:@//**emrepos1.example.com:1521/orclpdb.example.com**
SQL Script Execution	oas_biplatform	The actual username will be the prefixed with the value from the "**Schema prefix**" field in the screenshot: "*Schema_prefix*" + "_" + "BIPLATFORM" In this case, the complete username is: OAS_BIPLATFORM

Table 8. Arguments for OAS Scheduler Migration Script

Example execution of OAS Scheduler Migration Script using example values

Change to the directory appropriate for your platform:

```
cd /u01/oracle/OAS/bi/modules/oracle.bi.publisher/upgradeutil
```

Using the table above as an example, and the color coding in the table, execute the script as follows:

```
$ sqlplus sys/••••••••@oasrepos.example.com:1521/orcl as sysdba
```

Run the bip_12c_scheduler_migration.sql script

Pass in the command-line parameters, using the color coding from the table.

```
SQL> @bip_12c_scheduler_migration.sql  sysman_biplatform  ●●●●●●●
emrepos1.example.com:1521/orcl.example.com oas_biplatform
old 1: &&1 new 1: sysman_biplatform
old 2: &&2 new 2:  ●●●●●●●
old 3: '&&3' new 3: emrepos1.example.com:1521/orcl.example.com
old 4: '&&4' new 4: oas_biplatform
12C_BIPLATFROM_SCHEMA_NAME Database link created.
9979 rows created.
9769 rows created.
9739 rows created.
4159 rows created.
6 rows created.
6 rows created.
6 rows created.
Commit complete.
Database link dropped.
SQL> exit;
```

Appendix A. Determine the status of OAS

Full details on OAS lifecycles commands are detailed in the below document:

Oracle® Analytics
Administering Oracle Analytics Server

Utilize the scripts provided by OAS to determine the full status of the OAS stack

```
$ cd DOMAIN_HOME/bitools/bin
$ ./status.sh
Domain status; Using domainHome: ..../user_projects/domains/bi ...
Initializing WebLogic Scripting Tool (WLST) ...
...
/Servers/AdminServer/ListenPort=9500
Accessing admin server using URL t3://oas.example.com:9500
Status of Domain: /home/oracle/OASMW/user_projects/domains/bi

NodeManager (oas.example.com:9506:SSL): RUNNING

Name            Type            Machine                    Restart Int Max Restart  Status
----            ----            -------                    ----------- -----------  ------
AdminServer     Server          oas.example.com            unknown     unknown      Unknown
bi_server1      Server          oas.example.com            unknown     unknown      Unknown
```

Appendix B. Starting the full OAS stack

Full details on OAS lifecycles commands are detailed in the below document:

Oracle® Analytics
Administering Oracle Analytics Server

Utilize the scripts provided by OAS to start the full OAS stack

```
$ cd DOMAIN_HOME/bitools/bin
$ ./start.sh
Starting domain; Using domainHome: .../user_projects/domains/bi ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() ...
...
Node manager not running. Starting it...
NMProcess: NODEMGR_HOME is already set to .../user_projects/domains/bi/nodemanager
NMProcess: ...
...
NodeManager started
Reading domain...
/Servers/AdminServer/ListenPort=9500
Accessing admin server using URL t3://oas.example.com:9500
Starting AdminServer ...
nmStart(AdminServer) succeeded
Setting restart interval for all ...
Setting max restart for ...
Starting all servers ...
Starting bi_server1 (Original State:SHUTDOWN) ...
...
Started bi_server1
Set runtime log level...
Setting oracle.wsm log level to WARNING:1 for server: bi_server1
Finished starting servers

./status.sh
Domain status; Using domainHome: ..../user_projects/domains/bi ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() ...
...
/Servers/AdminServer/ListenPort=9500
Accessing admin server using URL t3://oas.example.com:9500
AdminServer already running

Status of Domain: /home/oracle/OASMW/user_projects/domains/bi
NodeManager (oas.example.com:9506:SSL): RUNNING

Name            Type            Machine                   Restart Int Max Restart  Status
----            ----            -------                   ----------- -----------  ------
AdminServer     Server          oas.example.com           unknown     unknown      RUNNING
bi_server1      Server          oas.example.com           unknown     unknown      RUNNING
```

Appendix C. Stopping the full OAS stack

Full details on OAS lifecycles commands are detailed in the below document:

Oracle® Analytics
Administering Oracle Analytics Server

Utilize the scripts provided by OAS to stop the full OAS stack

```
$ cd DOMAIN_HOME/bitools/bin
$ ./stop.sh
Stopping domain; Using domainHome: /home/oracle/OASMW/user_projects/domains/bi ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() ...
...
Reading domain...
/Servers/AdminServer/ListenPort=9500
Accessing admin server using URL t3://oas.example.com:9500
AdminServer already running
Stopping all managed servers and system components ...
Stopping bi_server1 (Original State:RUNNING) ...
......
Stopped bi_server1
Finished stopping managed servers and system components
Stopping AdminServer (Original State:RUNNING) ...
.Stopped AdminServer
Stopping NodeManager...


./status.sh
Domain status; Using domainHome: ..../user_projects/domains/bi ...
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
Type help() ...
...
/Servers/AdminServer/ListenPort=9500
Accessing admin server using URL t3://oas.example.com:9500
AdminServer already running

Status of Domain: /home/oracle/OASMW/user_projects/domains/bi
NodeManager (oas.example.com:9506:SSL): RUNNING

Name            Type            Machine                   Restart Int Max Restart  Status
----            ----            -------                   ----------- -----------  ------
AdminServer     Server          oas.example.com           unknown     unknown      RUNNING
bi_server1      Server          oas.example.com           unknown     unknown      RUNNING
```

Confirm the full stack is down by following the procedures in 'Appendix A - Determine the status of OAS'.

Appendix D. Recovering from a failed installation/configuration of OAS

The steps below can be utilized to recover from a failed installation/configuration of OAS:

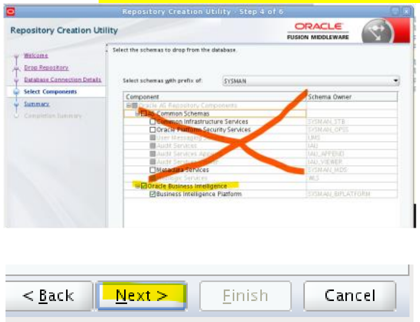
1. Stop any running WebLogic Processes:
   – Utilize 'Appendix C - Stopping the full OAS stack'
2. Clean up all related OAS artifacts from both DBMS and WebLogic:
   a. Run the RCU utility from the OAS $MW_HOME

```
$MW_HOME/oracle_common/bin/rcu
```

   b. On the first pages of the RCU utility, choose to drop a schema.
      - Ensure to specify the correct schema prefix (i.e. OAS).
   c. Delete the OAS schema using RCU.
   d. Delete the Domain for OAS in the $MW_HOME for OAS:

```
rm -rf $MW_HOME/user_projects/domains/bi
```

3. It is not necessary, nor desirable, to delete the OAS `$MW_HOME`.
4. Ensure to unckeck the entry for 'AS Common Schemas'
5. Make sure to select 'Oracle Business Intelligence'



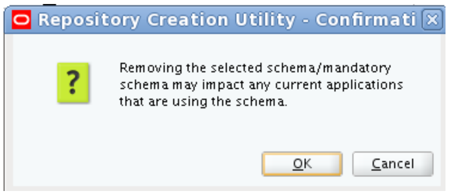
Repository Creation Utility - Step 4 of 6

Repository Creation Utility

Select the schemas to drop from the database.

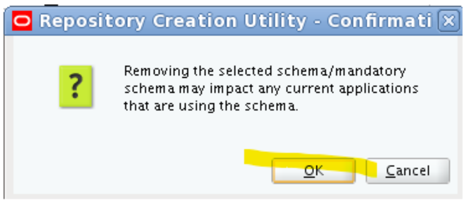
Select schemas with prefix of: SYSMAN

Component	Schema Owner
Oracle AS Repository Components	
□ AS Common Schemas	
□ Common Infrastructure Services	SYSMAN_STB
□ Oracle Platform Security Services	SYSMAN_OPSS
User Messaging Service	UMS
Audit Services	IAU
Audit Services Append	IAU_APPEND
Audit Services Viewer	IAU_VIEWER
□ Metadata Services	SYSMAN_MDS
Weblogic Services	WLS
☑ Oracle Business Intelligence	
☑ Business Intelligence Platform	SYSMAN_BIPLATFORM



Repository Creation Utility - Confirmati

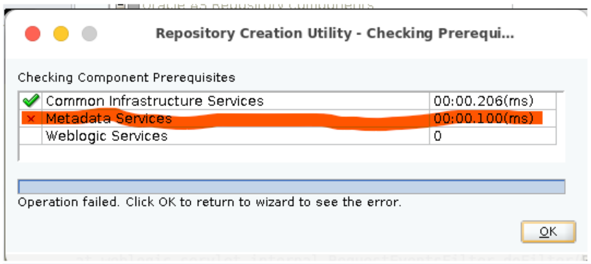
Removing the selected schema/mandatory schema may impact any current applications that are using the schema.



Repository Creation Utility - Confirmati

Removing the selected schema/mandatory schema may impact any current applications that are using the schema.

1) Take special note of the warning, and when sure, select ok:

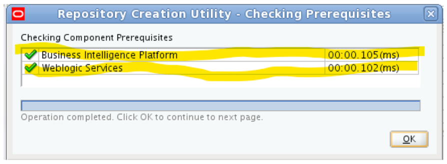


Repository Creation Utility - Checking Prerequi...

Checking Component Prerequisites

	Component	Time
✓	Common Infrastructure Services	00:00.206(ms)
✗	Metadata Services	00:00.100(ms)
	Weblogic Services	0

Operation failed. Click OK to return to wizard to see the error.

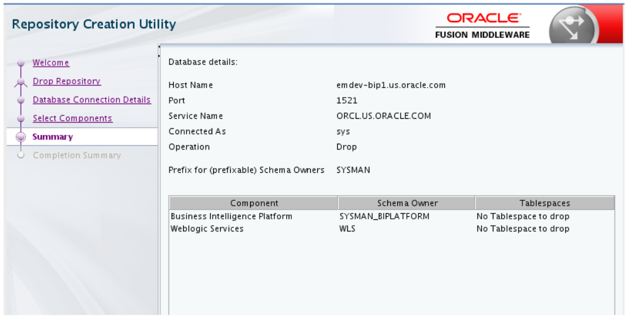


Repository Creation Utility - Checking Prerequisites

Checking Component Prerequisites

	Component	Time
✓	Business Intelligence Platform	00:00.105(ms)
✓	Weblogic Services	00:00.102(ms)

Operation completed. Click OK to continue to next page.



Repository Creation Utility

Database details:

Host Name emdev-bip1.us.oracle.com
Port 1521
Service Name ORCL.US.ORACLE.COM
Connected As sys
Operation Drop

Prefix for (prefixable) Schema Owners SYSMAN

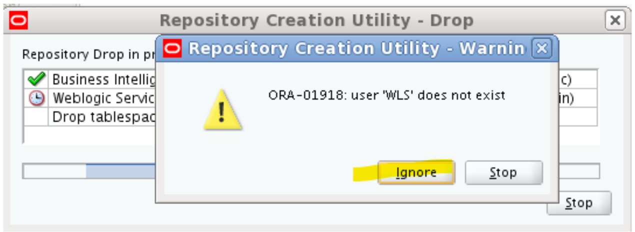
Component	Schema Owner	Tablespaces
Business Intelligence Platform	SYSMAN_BIPLATFORM	No Tablespace to drop
Weblogic Services	WLS	No Tablespace to drop

6. If you see an error, please follow the instructions, and start over:
7. You should see this screen

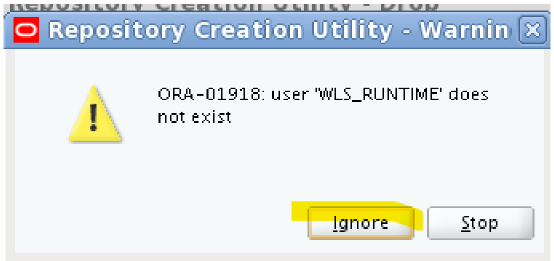
And when you hit 'OK' you should see this screen:

8. It is safe to ignore the warnings:

9. Choose ‘Ignore’ twice:

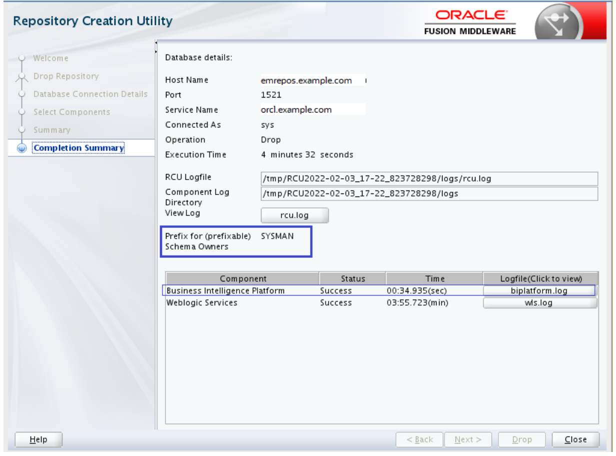


ORA-01918: user 'WLS' does not exist


Repository Creation Utility - Drop
Repository Creation Utility - Warnin
Ignore
Stop

ORA-01918: user 'WLS_RUNTIME' does not exist

10. Completion Status



Database details:

Host Name	emrepos.example.com
Port	1521
Service Name	orcl.example.com
Connected As	sys
Operation	Drop
Execution Time	4 minutes 32 seconds
RCU Logfile	/tmp/RCU2022-02-03_17-22_823728298/logs/rcu.log
Component Log Directory	/tmp/RCU2022-02-03_17-22_823728298/logs
View Log	rcu.log
Prefix for (prefixable) Schema Owners	SYSMAN

Component	Status	Time	Logfile(Click to view)
Business Intelligence Platform	Success	00:34.935(sec)	biplatform.log
Weblogic Services	Success	03:55.723(min)	wls.log

Appendix E. Details on the JDBC Simple Connect Descriptor

The JDBC Simple Connect descriptor is used by a Java application, such as Oracle Analytics Server, to connect to a remote Oracle Database.

Some of the common elements in all JDBC Simple Connect Descriptors are:

- Host Name
- TCP/IP Port
- Service Name (or deprecated Oracle SID)

In addition to the above standard elements, many other elements and options can be specified as part of a JDBC Simple Connect Descriptor.

A few examples of this includes:

- Oracle Secure TCPs Wallet
- Oracle RAC Database 'Scan' addresses

There are many other options and capabilities that are available.

Since the JDBC Simple Connect Descriptor is a standardized mechanism for any Java application to connect to an Oracle Database, a small set of tools is being developed to assist with determining the correct value to utilize.

In the meantime, the following Oracle developers Blog can provide more insights:

FOUR FACETS OF DATABASE CONNECTIVITY FOR JAVA APPLICATIONS

Once a valid JDBC Simple Connect Descriptor is determined, either using the tool above, or other standard procedures, this string can be used in most, but not all, dialogs in which OAS requires a 'JDBC Simple Connect Descriptor' entry.

See the next appendix for one known dialog that does not function correctly, and a procedure to workaround this limitation.

Appendix F. Oracle Analytics Publisher Login Flow

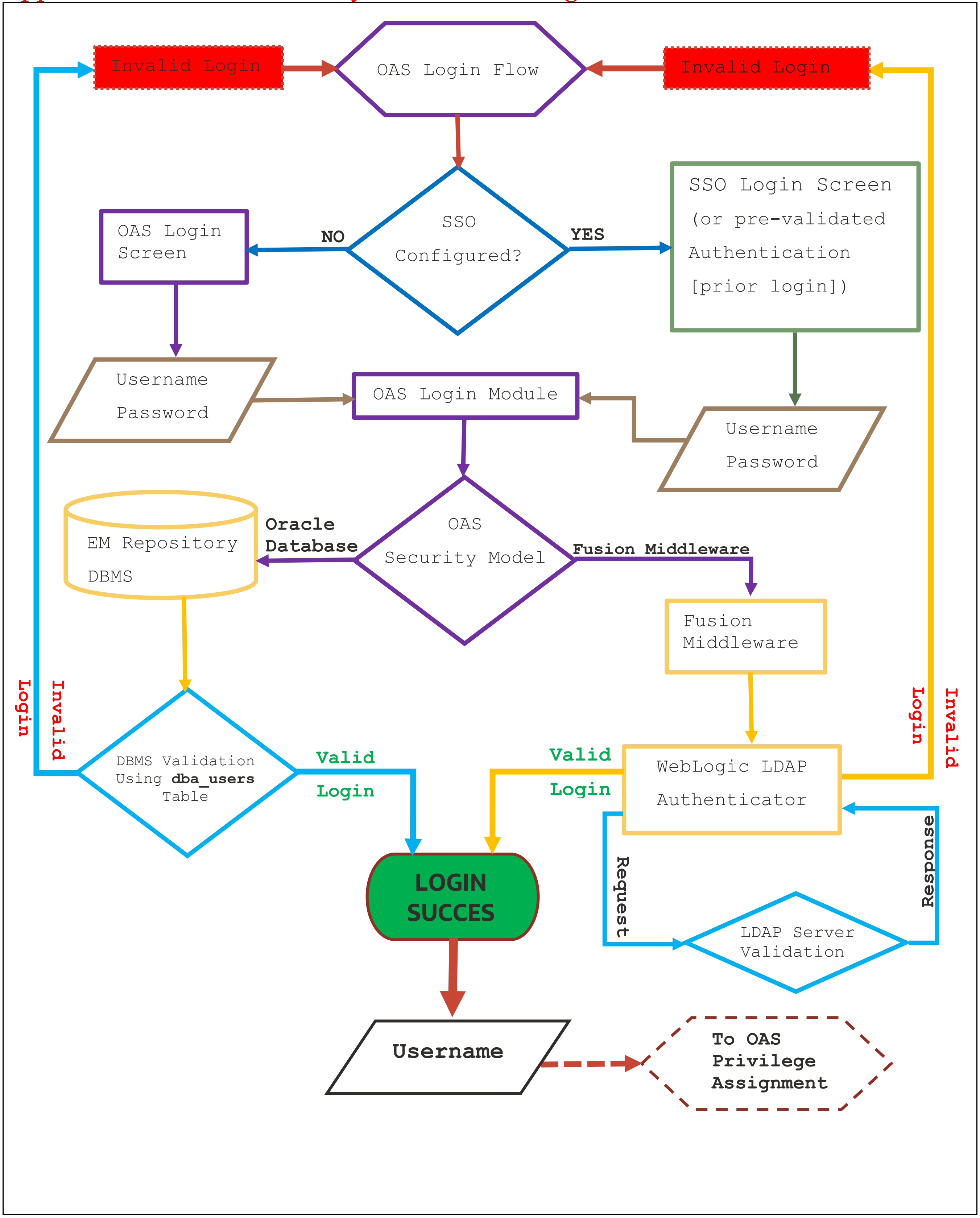


Figure 23. OAS Login Flow

Appendix G. OAS Privilege Assignment

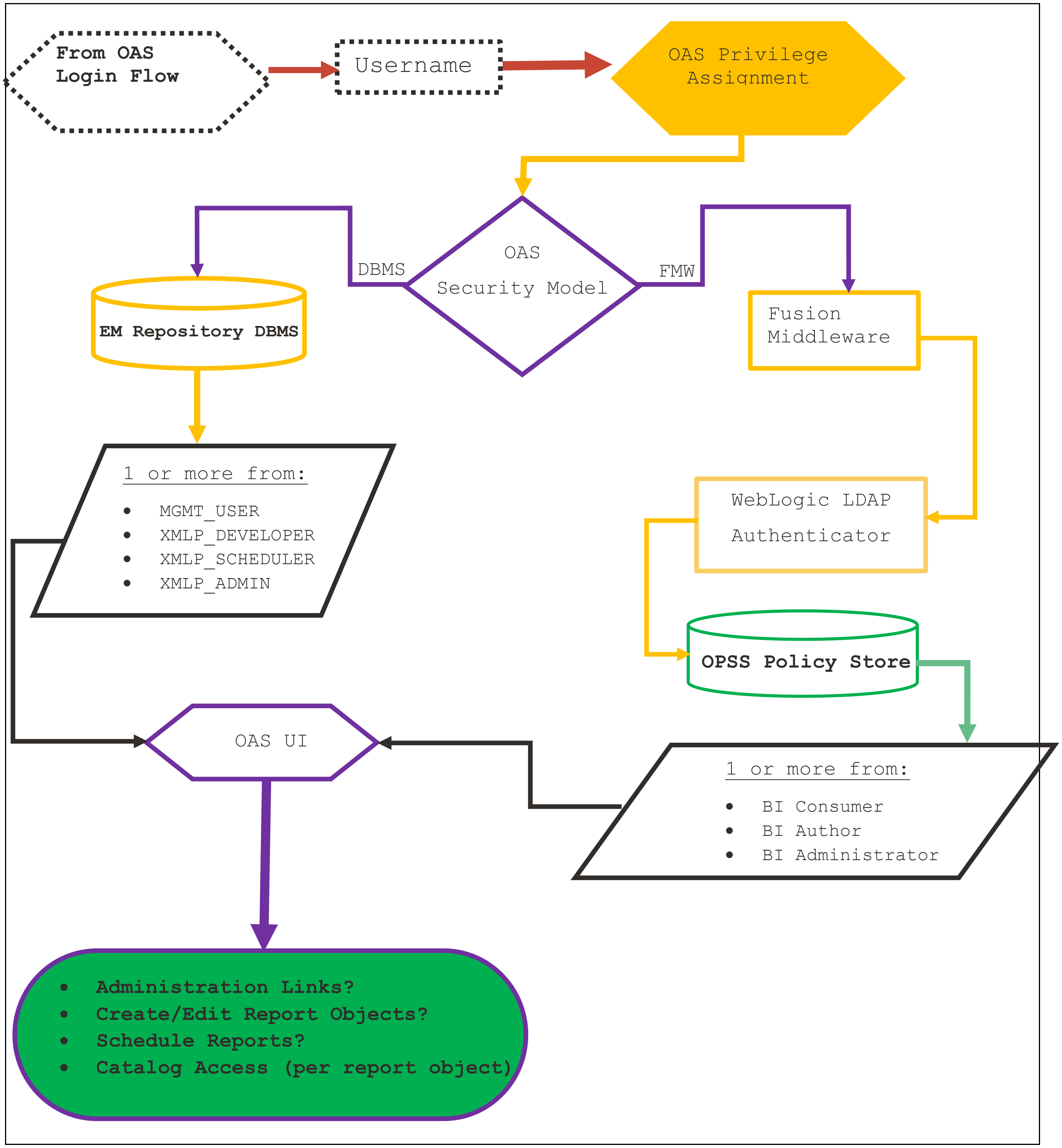


Figure 24. OAS Privilege Assignment

CHAPTER 10. REFERENCES

Configuring Oracle Analytics Server. (2021, March). Retrieved from Installing and Configuring Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/configuring-product.html

Corporation, O. (n.d.). *Configuring the Oracle Analytics Server Domain with the Configuration Assistant*. Retrieved from Installing and Configuring Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/configuring-oracle-analytics-server-domain-configuration-assistant.html#GUID-72B6F4ED-C66E-45E0-87F1-6DA73276024E

EM - Security Features : Supported Authentication Schemes. (2021, March). Retrieved from Enterprise Manager Cloud Control Security Guide: https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.4/emsec/security-features.html#GUID-8FF7D1AE-2BF8-4359-818C-E323AEF818B5

Google Search. (n.d.). Retrieved from https://google.com

Java Platform, Standard Edition - Release 8. (2020, July). Retrieved from Installation Guide - Release 8: https://docs.oracle.com/javase/8/docs/technotes/guides/install/toc.html

Migrating Scheduler Jobs and Job History. (2021, March). Retrieved from Migrating and Upgrading to Oracle Analytics Server - F27231-04: https://docs.oracle.com/en/middleware/bi/analytics-server/migrate-upgrade-oas/migration-steps-oracle-bi-ee.html#GUID-CCC0A118-0AE4-47AE-89E0-473B5DAB6572

OAS - About Alternative Security Options. (2021, March). Retrieved from Administering Oracle Analytics Publisher in Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/administer-publisher-oas/alternative-security-options.html#GUID-2F2D945F-C5AB-447E-AA1B-B34ACFAAF8CC

OAS - Configure Oracle Fusion Middleware Security Model. (2021, March). Retrieved from Administering Oracle Analytics Publisher in Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/administer-publisher-oas/configure-oracle-fusion-middleware-security-model.html#GUID-8F5033A3-E912-4407-BF15-E23E3A13F154

OAS - Installing the Oracle Analytics Server Software. (n.d.). Retrieved from Installing and Configuring Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/install-config-oas/installing-product-software.html#GUID-D5AFD830-8A7D-42CC-8C22-CE68C452CF4A

OAS - Integrate with Oracle Database Security. (2021, March). Retrieved from Administering Oracle Analytics Publisher in Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/administer-publisher-oas/integrate-oracle-database-security.html#GUID-24D00B59-951C-44FD-A046-7386EF2199FF

OAS - Set Up Data Sources. (2021, March). Retrieved from Administering Oracle Analytics Publisher in Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/administer-publisher-oas/set-data-sources.html#GUID-13359663-9030-4E6F-B5CC-2D63E43E456F

OAS: Quick Reference For In-Place Upgrade From Oracle Business Intelligence Enterprise 12c To OAS On Linux (Doc ID 2645014.1). (2020, March). Retrieved from https://support.oracle.com/epmos/faces/DocContentDisplay?id=2645014.1

Oracle Maximum Availability Architecture, MAA. (2021). *Oracle Maximum Availability Architecture (MAA)*. Retrieved from Oracle Maximum Availability Architecture (MAA): https://www.oracle.com/database/maximum-availability-architecture/

Oracle® Analytics Enterprise Deployment Guide for Oracle Analytics Server. (2020, September). *Oracle® Analytics Enterprise Deployment Guide for Oracle Analytics Server*. Retrieved from Oracle® Analytics Enterprise Deployment

Guide for Oracle Analytics Server: https://docs.oracle.com/en/middleware/bi/analytics-server/enterprise-deploy-oas/index.html

Oracle® Fusion Middleware. (2020, August). Retrieved from Installing and Configuring the Oracle Fusion Middleware Infrastructure 12c (12.2.1.4.0) - E95088-05: https://docs.oracle.com/en/middleware/fusion-middleware/12.2.1.4/infin/index.html

Oracle®Database JDBC Developer's Guide. (2021). *Oracle®Database JDBC Developer's Guide*. Retrieved from https://docs.oracle.com/en/database/oracle/oracle-database/19/jjdbc/index.html

Required and Recommended Patches and Patch Sets For Oracle Business Intelligence 12c and Oracle Analytics Server (Doc ID 2070465.1). (n.d.). Retrieved from https://support.oracle.com/epmos/faces/DocContentDisplay?id=2070465.1

index

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Installing and Configuring Oracle Analytics Server 24 (7.6) for use with Oracle Enterprise Manager 24ai Release 1 (24.1)
November 2424
Author: Abramson, Jerry (Oracle)