Oracle® Health Sciences Pharmacovigilance Operational Analytics

Installation Guide

Release 1.0

E23555-01

September 2011

ORACLE®

Oracle Health Sciences Pharmacovigilance Operational Analytics Installation Guide, Release 1.0

E23555-01

Contents

Preface v

Audience v
Documentation Accessibility v
Finding Information and Patches on My Oracle Support vi
Related Documents viii
Known Installation and Configuration Issues ix
Conventions ix

1 OPVA Requirements

1.1 Requirements 1-1
1.1.1 Technology Stack and System Requirements 1-1
1.1.1.1 Server Components 1-1
1.1.1.2 Client Components 1-2
1.1.1.3 Supported Sources 1-3
1.1.1.4 Technology Stack Matrix 1-3
1.1.1.5 Typical Hardware Architecture 1-5
1.1.1.6 Installation Process Overview 1-6
1.1.2 Prerequisites 1-6
1.1.2.1 Client Tools 1-7

2 Installing Oracle Pharmacovigilance Operational Analytics

2.1 Preinstallation Configuration 2-1
2.2 Running the OPVA Installer 2-2
2.3 Preparing the DAC Repository 2-5
2.4 Configuring the OBIEE Repository and Webcatalog 2-8
2.4.1 Prerequisites 2-8
2.4.2 Deployment of OBIEE Repository and Catalog 2-8
2.4.2.1 Post-deployment of the OPVA RPD 2-13
2.5 Configuring the OBIEE Help files 2-13
2.5.1 Configuring the Help links in the Dashboards and Reports 2-13
2.6 Configuring SSO Using Oracle Access Manager 2-17
2.7 Creating Users and Groups in OPVA 2-33
2.7.1 Creating Groups for OPVA in WebLogic Server 2-33
2.7.2 Assigning OBIEE Application Roles for OPVA Groups 2-35
2.7.3 Creating Users for OPVA in WebLogic Server 2-36

2.7.4 Creating Users for DAC 2-37
2.8 Configuring SSL for OPVA in OBIEE 2-38
2.9 OBIEE Default Application Roles 2-40

Preface

Oracle Health Sciences Pharmacovigilance Operational Analytics (OPVA) is an analytical reporting application. OPVA extracts data from Oracle Argus Safety, providing a data warehouse containing key metrics across the pharmacovigilance business process. From this warehouse, OPVA provides key pre-defined reports, and enables the creation of additional custom reports. OPVA also includes reports that run against the source database, thereby providing an up to date data analysis.

In addition to Argus Safety, OPVA requires the presence of Informatica PowerCenter, Oracle Business Intelligence Data Warehouse Administration Console (DAC), Oracle Business Intelligence Enterprise Edition (OBIEE), and Oracle Database.

Audience

Installing OPVA requires a level of knowledge equivalent to having mastered the material in Oracle's DBA Architecture and Administration course. You must be able to read and edit SQL*Plus scripts. You must be able to run SQL scripts and review logs for Oracle errors.

Installing and maintaining Oracle Pharmacovigilance Analytics requires the following skill set across a variety of platforms including Linux, Unix, Solaris and Microsoft:

- Creating and managing user accounts, groups, and access
- Installation and maintenance of Oracle RDBMS
- Installation and maintenance of Informatica PowerCenter
- Installation and maintenance of Oracle Business Intelligence Enterprise Edition 11g
- Installation and maintenance of Oracle Datawarehouse Administration Console 11g
- Installation and maintenance of OAM
- Installation and maintenance of Oracle Weblogic 10.3.5
- Managing OS Environment, services, and network

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Finding Information and Patches on My Oracle Support

Your source for the latest information about Oracle Health Sciences Pharmacovigilance Operational Analytics is Oracle Support's self-service Web site, My Oracle Support (formerly MetaLink).

Always visit the My Oracle Support Web site for the latest information, including alerts, release notes, documentation, and patches.

Getting the OPVA Standard Configuration Media Pack

The OPVA media pack is available both as physical media and as a disk image from the Oracle E-Delivery Web site. The media pack contains the technology stack products and the OPVA application. To receive the physical media, order it from Oracle Store at https://oraclestore.oracle.com.

To download the OPVA media pack from eDelivery, do the following:

1. Navigate to http://edelivery.oracle.com and log in.
2. From the Select a Product Pack drop-down list, select Health Sciences.
3. From the Platform drop-down list, select the appropriate operating system.
4. Click Go.
5. Select Oracle Health Sciences Pharmacovigilance Operational Analytics Media Pack for Operating System and click Continue.
6. Download the software.

Creating a My Oracle Support Account

You must register at My Oracle Support to obtain a user name and password account before you can enter the Web site.

To register for My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click the **Register here** link to create a My Oracle Support account. The registration page opens.
3. Follow the instructions on the registration page.

Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to http://support.oracle.com.
2. Click **Sign In**.
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

Searching for Knowledge Articles by ID Number or Text String

The fastest way to search for product documentation, release notes, and white papers is by the article ID number.

To search by the article ID number:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Locate the Search box in the upper right corner of the My Oracle Support page.
3. Click the sources icon to the left of the search box, and then select Article ID from the list.
4. Enter the article ID number in the text box.
5. Click the magnifying glass icon to the right of the search box (or press the Enter key) to execute your search.

   The Knowledge page displays the results of your search. If the article is found, click the link to view the abstract, text, attachments, and related products.

In addition to searching by article ID, you can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page, you can drill into a product area through the Browse Knowledge menu on the left side of the page. In the Browse any Product, By Name field, type in part of the product name, and then select the product from the list. Alternatively, you can click the arrow icon to view the complete list of Oracle products and then select your product. This option lets you focus your browsing and searching on a specific product or set of products.
- Refine Search — Once you have results from a search, use the Refine Search options on the right side of the Knowledge page to narrow your search and make the results more relevant.
- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find knowledge articles and documentation.

Finding Patches on My Oracle Support

Be sure to check My Oracle Support for the latest patches, if any, for your product. You can search for patches by patch ID or number, or by product or family.

To locate and download a patch:

1. Sign in to My Oracle Support at http://support.oracle.com.
2. Click the **Patches & Updates** tab.

   The Patches & Updates page opens and displays the Patch Search region. You have the following options:

   - In the Patch ID or Number is field, enter the primary bug number of the patch you want. This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the Product or Family link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download**. Follow the instructions on the screen to download, save, and install the patch files.

Finding Certification Information

Certifications provide access to product certification information for Oracle and third party products. A product is certified for support on a specific release of an operating system on a particular hardware platform, for example, Oracle Database 10g Release 2 (10.2.0.1.0) on Sun Solaris 10 (SPARC). To find certification information:

1. Sign in to My Oracle Support at `http://support.oracle.com`.
2. Click the **Certifications** tab. The Certifications page opens and displays the Find Certifications region.
3. In Select Product, enter Oracle Health Sciences Pharmacovigilance Operational Analytics.
4. Click the Go to Certifications icon.

   The right pane displays the certification information.
5. Select a certification to view the certification details.

Related Documents

For more information, see the following documents:

The Oracle Business Intelligence Data Warehouse Administration Console (DAC) documentation set includes:

- *Data Warehouse Administration Console User's Guide (Part E12652)*
- *Oracle Business Intelligence Data Warehouse Administration Console Installation, Configuration, and Upgrade Guide (Part E12653)*

The *Oracle Fusion Middleware* documentation set includes:

- *Oracle Fusion Middleware Quick Installation Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E16518-02)
- *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10539-02)
- *Oracle Fusion Middleware Upgrade Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E16452-02)
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E15722-02)
- *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10544-02)
- *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10541-02)
- *Oracle Fusion Middleware Developer's Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10545-02)
- *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10543-03)
- *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence 11g Release 1 (11.1.1)* (E10540-02)

Known Installation and Configuration Issues

Oracle maintains a list of installation and configuration issues that you can download from My Oracle Support (MOS). For information about these issues, please see Note ID 1326918.1.

Conventions

The following text conventions are used in this document:

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

1

OPVA Requirements

1.1 Requirements

This section presents an overview of the Oracle Health Sciences Pharmacovigilance Operational Analytics (OPVA) architecture, required hardware and software, and dependencies across the components. Before you begin the installation, confirm that your environment meets hardware and software requirements described in this section.

1.1.1 Technology Stack and System Requirements

The requisite technology stack for OPVA is provided in the media pack, with the exception of Informatica products. It consists of the following products:

1.1.1.1 Server Components

1.1.1.1.1 OPVA Database Server OPVA is certified for Oracle Database Enterprise Edition 11.2.0.1. It supports Oracle Database Enterprise Edition 11.2.0.2 as well.

Supported Operating System

- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle Sun Solaris 10 (64 Bit)
- Microsoft Windows Server 2008 R1 with SP1 or above (32/64 bit)
- Microsoft Windows Server 2008 R2 (64 bit)
- Memory: RAM 4-16 GB (based on organization size), HDD – at least 500 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.2 OPVA Informatica Server OPVA is certified against Informatica PowerCenter 9.0.1 with Hotfix2. Refer Informatica PowerCenter installation guide for recommended hardware and supported platforms. OPVA has got certified the following:

- Operating System: Oracle Enterprise Linux 5 or above (32/64 bit)
- Memory: RAM at least 8 GB. HDD – at least 250 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.3 OPVA OBIEE Server OPVA is certified against Oracle Business Intelligence Enterprise Edition 11.1.1.5.0. Please refer the installation manual of OBIEE for further hardware and software requirements OPVA would recommend the following:

Operating System

- Microsoft Windows Server 2008 R1 with SP1 or above (32/64 bit)
- Microsoft Windows Server 2008 R2 (64 bit)
- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle Sun Solaris 10 (64 Bit)

> **Note:** If unix based OS is used for the OBIEE server, then the OBIEE Admin tool must be installed separately on a Windows box.

- Memory: RAM at least 8 GB, HDD – at least 250 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.4 OPVA Datawarehouse Administration Console Server OPVA requires Oracle Datawarehouse Administration Console Server 10.1.3.4 with patch 12381656.

Supported Operating System

- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle Sun Solaris 10 (64 Bit)
- Microsoft Windows Server 2008 R1 with SP1 or above (32/64 bit)
- Microsoft Windows Server 2008 R2 (64 bit)
- Memory: RAM 4-16 GB (based on organization size), HDD – at least 500 GB free space
- CPU: At least 2 Dual Core CPUs

1.1.1.2 Client Components

1.1.1.2.1 Oracle Database Client

- OPVA requires Oracle database client to connect to the database server. The supported client software version is 11.2.0.1.
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32 bit)

1.1.1.2.2 Oracle Datawarehouse Administration Console Client

- OPVA requires Oracle Datawarehouse Administration Console Client 10.1.3.4 with patch 12381656.
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32 bit)

1.1.1.2.3 Informatica PowerCenter Client

- An Informatica PowerCenter Client 9.0.1 with Hotfix 2 is required to connect to the Informatica Server.

- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32 bit)

1.1.1.2.4 OBIEE Admin Tool

- OBIEE Admin tool 11.1.1.5.0 must be installed for configuring the repository file (RPD).
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32/64 bit)

1.1.1.2.5 Optional Security Component You can also configure Single Sign on Support for your reports and dashboards using Oracle Access Manager 10.1.4. For more information regarding the Oracle Access Manager installation and supported platforms, please refer the *Oracle Access Manager Installation Guide*.

1.1.1.2.6 Miscellaneous Components

- For running the reports and dashboards, your machine should have the Adobe Flash Player 10 or above installed.
- Although OBIEE 11.1.1.5.0 reports are supported in Microsoft Internet Explorer, Firefox and Safari, OPVA is certified only for Microsoft Internet Explorer 7.0 and 8.0 only.

1.1.1.3 Supported Sources

OPVA, by default, supports only Oracle Argus Safety. It supports the following Oracle Argus Safety versions:

- Oracle Argus Safety 7.0
- Oracle Argus Safety 6.0.2

Customers can add customer data sources to the application by adding their own ETL. For more information about customizing OPVA, please refer to the Oracle Health Sciences Pharmacovigilance Operational Analytics Administrator and User Guide.

1.1.1.4 Technology Stack Matrix

The following table displays the technology stack matrix diagram of all the components of OPVA.

Specification	OBIEE Server	Database	Informatica Server	DAC Server *	Install / Admin Machine *	Client
Operating System	Windows Server 2008 with SP1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux 5 (32/64 Bit) Oracle Sun Solaris 10 (64 Bit)	Windows Server 2008 with SP 1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux 5 (32/64 Bit) Oracle Sun Solaris 10 (64 Bit)	Windows Server 2008 with SP1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux 5 (32/64 Bit) Oracle Sun Solaris 10 (64 Bit)	Windows Server 2008 with SP1 or above (32 Bit)	Windows 32 bit	Windows XP Pro SP3 Windows 7
Oracle Database		11.2.0.1.0 (Enterprise)-AL32UTF8 char set	11.2.0.1 Client		11.2.0.1 Client	
OBIEE Server	OBIEE 11.1.1.5.0					
OBIEE Admin Tool	OBIEE 11.1.1.5 Admin Tool*				OBIEE 11.1.1.5 Admin Tool	
Informatica			Informatica Server 9.0.1 + HF2	Informatica Client 9.0.1 + HF2	Informatica Client 9.0.1 + HF2	
DAC			DAC Server 10.1.3.4.1 + Patch 12381656	DAC Server & Client 10.1.3.4.1 + Patch 12381656	DAC Client 10.1.3.4.1 + Patch 12381656	
Browser						IE 7.0 (latest) or IE 8.0 (latest)
Adobe Flash Player						Flash Player 10 or above

* DAC
DAC Server needs to be installed on a machine where Informatica home is present. DAC Server can be installed on the same machine where Informatica Server is located; there is no need that it should be a stand-alone server.

* OBIEE
OBIEE Admin tool can be installed along with the OBIEE Server, provided the Operating System is Microsoft Windows.

Supported Security Configuration

OPVA supports the following optional security configurations:

- LDAP/LDAPS 3.0
- Single Sign On Solution through Oracle Access Manager 10.1.4

> **Note:** If OAM is used, then the OBIEE Server must have Oracle Enterprise WebGate 10.1.4.3 and Oracle Web Tier 11g installed.

1.1.1.5 Typical Hardware Architecture

A typical OPVA installation contains the following hardware architecture:

- Servers:
  - An Oracle Database server with Oracle Database 11.2.0.1
  - An Informatica PowerCenter 9.0.1 with Hotfix 2 Server + DAC Server 10.1.3.4 with patch 12381656
  - An OBIEE 11.1.1.5 Server

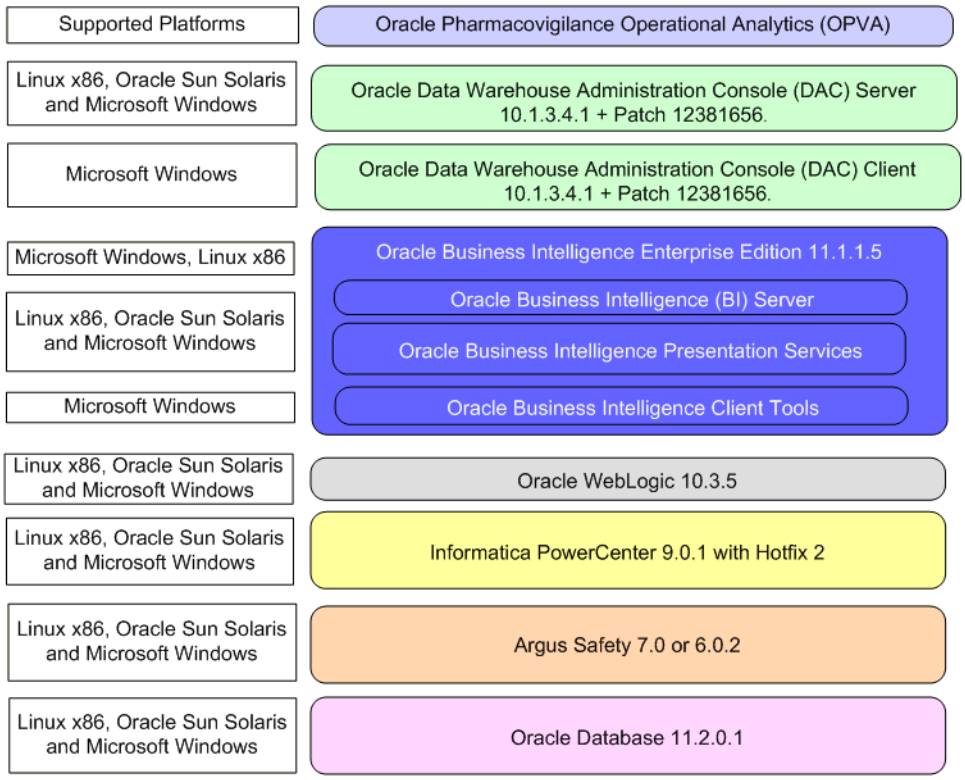
> **Note:** The above three boxes can run on any of the supported platforms: Linux/Solaris/Windows.

- Clients:
  - An Informatica PowerCenter Client 9.0.1 + Hotfix 2
  - Oracle Database Client 11.2.0.1
  - DAC Client 10.1.3.4 with patch 12381656
  - OBIEE Admin tool

> **Note:** All tools can be installed in a single Microsoft Windows 32 bit box.
>
> If the OBIEE server mentioned under the "Servers" section is a Windows 32 bit server, then all the clients can be installed in the same box itself.
>
> If the OBIEE Server is installed on a Windows 64 bit machine, then the OBIEE Admin tool can also be installed along with the server itself.
>
> Informatica PowerCenter and Oracle Database Client should be available in the same machine for OPVA installer to run.

> **Note:** It is important to get the technology stack products from the OPVA media pack because newer versions of the technology stack products may have become available but may not be compatible with OPVA.

Figure 1–1 Oracle Health Sciences Pharmacovigilance Operational Analytics Technology



1.1.1.6 Installation Process Overview

The following steps describes the overview of the installation process:

- Follow the steps described in Section 1.1.2, "Prerequisites".
- Execute the installer – to create the datamart and Informatica ETLs.
- Follow the post installation steps to configure DAC and OBIEE

For more information about certifications, refer to "Finding Certification Information".

1.1.2 Prerequisites

Before proceeding with the installation, ensure the following software is available.

- An Oracle Database Server – An Oracle 11.2.0.1 database server should be created before OPVA installation. Follow the platform specific Database Installation Guide for installing this server.

  Note: The database server should be configured with AL32UTF8 charset.

- An Informatica PowerCenter Server – An Informatica PowerCenter 9.0.1 + HF2 should be created before running the OPVA Installer. Follow platform specific Informatica PowerCenter Installation.

Note:

- Informatica Server needs a repository database. Customer can either use the database created in previous step or can create a new database for holding the repository. A PowerCenter repository should be created upon the installation of PowerCenter. This repository information along with the admin user credentials will be needed during OPVA installation.
- An Oracle 11.2.0.1 Client should be available in the Informatica server.

- A OBIEE Server - An Oracle Business Intelligence Enterprise Edition 11.1.1.5.0 Server must be installed before the OPVA Installation. Follow platform specific OBIEE Installation Guide for installation instructions.
- A DAC Server – An Oracle Datawarehouse Administration Console Server of version 10.1.3.4 with patch 12381656 needs to be installed on the same machine where Informatica client is loaded. Follow platform specific *ODAC Installation Guide* for installation instructions.

1.1.2.1 Client Tools

- An Informatica PowerCenter Client - An Informatica PowerCenter Client 9.0.1 with Hotfix 2 must be present. Supported only on a Microsoft Windows 32 bit machine.
- An Oracle Database client - An Oracle 11.2.0.1 database client should be present. This should be present in the same machine where the Informatica PowerCenter client is loaded.
- A DAC Client - A DAC Client 10.1.3.4.1 with patch 12381656 needs to be present. Supported only on a Microsoft Windows Server 2008 with SP1 or above (32 bit).

Note:

- Oracle recommends that you enable HTTPS on the middle-tier computer that is hosting the BIEE Web services, since otherwise the trusted user name and password that are passed can be intercepted.

2

Installing Oracle Pharmacovigilance Operational Analytics

Note: This installation assumes that assumes the typical hardware configuration with an Oracle database server, an Informatica PowerCenter server, and a Windows 2008 SP1 32 bit server with OBIEE Server & Admin Tool, DAC Server & Client, Informatica PowerCenter Client, and an Oracle Database Client.

All installation and configuration actions must be performed as an administrator or root user.

This section describes the detailed OPVA installation process. It also describes the pre and post OPVA installation tasks that you must complete for different environments. This section includes the following topics:

- Preinstallation Configuration
- Running the OPVA Installer
- Preparing the DAC Repository
- Configuring the OBIEE Repository and Webcatalog
- Configuring the OBIEE Help files
- Configuring SSO Using Oracle Access Manager
- Creating Users and Groups in OPVA
- Configuring SSL for OPVA in OBIEE
- OBIEE Default Application Roles

2.1 Preinstallation Configuration

Prior to running the OPVA Installer, the following tasks must be completed:

1. Configuring the Database server:

   The TNS Names entry for the Argus Safety Source Database should be available in the database server where datamart is configured.

2. The TNS entries for the Datawarehouse Schema should be present in the OBIEE 11g home in the path:

   <OracleBI Home>\Oracle_BI1\network\admin\tnsnames.ora

3. Configuring the Informatica client:

   The Informatica client should be configured to connect to the Informatica server. There should be an entry for the Informatica Domain in the domains.infa file.

4. Setting up the Informatica environmental parameters.

   - INFA_DOMAINS_FILE: Full filename with the path to the domains file present in the Informatica Client Home.
   - Path: Add the first entry in the path as the path to the PowerCenter Client Bin and then for the commandlineUtilities bin folder as shown in the following example:
     D:\Informatica\9.0.1\clients\PowerCenterClient\client\bin;;D:\Informatica\9.0.1\clients\PowerCenterClient\CommandLineUtilities\PC\server\bin;…

5. Configuring the oracle client:

   The TNS names entry for both datamart and the Argus Safety Source system should be configured here.

6. Setting up the DAC client:

   The DAC client should be configured to connect to the DAC server.

7. Setting up the Oracle client home in the PATH variable.

8. Setting up the SYSTEM user:

   The SYSTEM user to be given grants to create view over the V_$SESSION view in order to run the installer.

   Connect as “sys” on both the Argus Safety DB instance and the Datamart DB instance and execute this script:

   grant select on v_$session to system with grant option;

   Note: This grant can be revoked at a later time from the user system, once the installation is complete.

9. Setting up the tablespaces:

   The installer creates new schemas in the datamart and prompts for the tablespaces to be used. It is recommended to create one default tablespace and a temporary tablespace to be used for the new schemas.

2.2 Running the OPVA Installer

The basic OPVA components are installed using the Oracle Universal Installer. The installer gathers all the information about the database connectivity, datamart, Informatica repository by presenting a sequence of prompt screens and then installs the components accordingly. This installer needs to be executed in the OPVA server where Oracle client and Informatica client are installed.

Note: Make sure that PERL is present in the system path before running the installer.

Launch the Universal Installer

1. Extract the contents of the media pack into a temporary directory (For example, C:\opva_temp).
2. Navigate to the \install directory under the extracted temporary folder.
3. Double-click the setup.exe file to launch the Oracle Universal Installer with the Welcome screen.

Complete Running the OPVA Installer

The installer will take you through a series of prompts. Attend to the Installer's prompts. The following sections describe each Installer screen, and the required action.

OPVA Home Path

The OPVA Home path is the location where all the staged files from the Installer will get copied to the local machine. This is also the location from where Installer would execute the database and Informatica scripts.

Example Name: OPVAHome1

Path: C:\OPVA

Click Next

Argus Safety Database Details

This screen collects all information about the source Argus Safety database. Supply the values for Argus Safety database connect string, Argus Safety schema, password, Argus Safety database's system user password, VPD schema name, OPVA source schema and password.

> **Note:** OPVA Source schema is the new schema which would get created to store the views for all Argus Source tables that are needed for the ETL and reporting process.

Example:

AS Database Connect String: argus_src

AS Schema: argus_app

AS Password: <argus app user's password>

AS System Password: <system user's password>

VPD Schema: vpd_admin

OPVA Source Schema: opva_source

OPVA Source Password: <opva_source password>

Click Next

OPVA Datawarehouse Details

This screen collects all the information regarding the OPVA data warehouse details. Details of the data warehouse connect string, data warehouse system user password, the dw schema, password, rpd schema and rpd schema password, and the dw and temp table spaces.

Note: DW schema is the new schema that would be created by the installer to store the ETL data. OPVA RPD schema is the schema which would contain the synonyms of all the datamart tables and used by OBIEE reports.

Tablespaces that are going to be specified here should have got created during the pre-installation steps.

Example:

DW Database Connect String: opva_mart

DW System password: <system user's password of data warehouse database>

OPVA DW Schema: OPVA

OPVA DW Password: <password for OPVA schema>

OPVA RPD Schema: OPVA_RPD

OPVA Rpd Password: <password for RPD schema>

DW Default table space: DW_DFLT_TS

DW Temporary tablespace: DW_TEMP_TS

Click Next

Informatica PowerCenter Details

This screen collects all information to connect to the Informatica server.

Example:

PowerCenter Repository: OPVA_ PowerCenter_Reposiroty

PowerCenter Domain: Domain_opva

PowerCenter Admin user id: Administrator

PowerCenter Admin password: <administrator password>

OPVA Import folder: OPVA

Click Next

Informatica PowerCenter Client Home Details

The Informatica PowerCenter client home path is required for the installer to run successfully.

Example:

D:\Informatica\9.0.1\clients\PowerCenterClient\client

Click Next

Summary Screen

Verify setting => details provided in the summary screen and click Install.

The installer will stage the required components into the OPVA home and would create the datamart schemas, rpd schemas.

At the completion of the install, install log could be found at:

<opva home>\install\opva_install.log and pvadriverscript<timestamp>.log

2.3 Preparing the DAC Repository

> **Note:** This section assumes that the DAC client is present in the same machine where the OPVA installer is run. If not, copy the <opva_ home>\DAC\opva.zip file into the machine where the DAC client is installed.

Execute the following steps that must be implemented after logging into the machine where DAC client is present and after unzipping the contents of the <opva_ home>\DAC\opva.zip file to an appropriate folder:

1. Create a new DAC repository, or connect to an existing DAC repository, as Administrator.
2. Import the OPVA Warehouse Application metadata.
   a. Start the Data Warehouse Administration Console (DAC) client.
   b. From the **Tools** menu select **DAC Repository Management**, and then select **Import**.
   c. Click Change import/export folder to navigate to <DRIVE>:\OPVA_ HOME\DAC folder that holds the DAC Repository for OPVA ETL.
   d. Click **OK** to display the Import dialog box.
   e. Select the following categories of metadata you want to import: **Logical**, **Overwrite log file**, and **User Data**.
   f. Select **OPVA** application in the ApplicationList.
   g. Click **OK**.
   h. Click OK in the secondary window that is displayed after the import.
   i. You can inspect the import log in ${DAC_ INSTALL_DIR }\log\import.log to verify if import is successful.
3. Configure Informatica Repository Service in DAC.
   a. Navigate to the **Setup** view, then select the **Informatica Servers** tab.
   b. Click **New** to display the Edit tab below or select an existing Informatica server from the list.

      If you are configuring a new installation, the Informatica Servers tab will have some default values there for information. If you are upgrading an existing installation, the Informatica Servers tab might contain existing Informatica servers.
   c. Enter values in the following fields:

      Name — Enter the Logical name for the Informatica server (for example, INFO_REP_SERVER).

      Type — Select `Repository`.

      Server Hostname — Enter the host machine name where Informatica Server is installed.

      Server Port — Enter the port number Informatica Server or Informatica Repository Server use to listen to requests.

      Login — Enter the Informatica user login.

Password — Enter the Informatica Repository password.

Repository Name —Enter the Informatica Repository Name.

d. Test the connection to verify the settings.

e. Click **Save** to save the details.

4. Configure Informatica Integration Service in DAC.

Note: Make sure that you use the same Login and Password that you have used in setting up Informatica.

---

a. Click **New** to display the Edit tab below or select an existing Informatica server from the list.

If you are configuring a new installation, the Informatica Servers tab will have some default values there for information. If you are upgrading an existing installation, the Informatica Servers tab might contain existing Informatica servers.

b. Enter/edit values in the following fields:

Name — Enter the Logical name for the Informatica server (for example, INFO_SERVER).

Type — Select **Informatica**.

Domain — Enter the Informatica domain name.

Service — Enter the Informatica Service Name.

Login — Enter the Informatica Repository user login.

Password — Enter the Informatica Repository password.

Repository Name — Enter the Informatica Repository Name.

c. Test the connection to verify the settings.

d. Click **Save** to save the details.

5. In this step, you configure source databases (Argus Safety) and the target database (the OPVA warehouse). For each database with which DAC will interact for OPVA, perform the following steps:

a. Navigate to the **Setup** view, then select the **Physical Data Sources** tab.

b. Select the opva_dwh entry to display the Edit tab below.

c. Enter values in the following fields:

Name — Keep the Logical name as opva_dwh for the database connection.

Type — Select `Source` when you create the database connection for a transactional (OLTP) database. Select `Warehouse` when you create the database connection for a data warehouse (OLAP) database.

Connection Type — Select a connection type for the database connection.

Instance or TNS Name — Enter the Data Mart database instance name.

Table Owner — Enter the Data Mart schema name.

Table Owner Password — Enter the Data Mart schema password.

DB Host — Enter the Data Mart host name.

Port — Enter the Data Mart host port.

Data Sure Number – Enter the number 0.

d. Test the connection to verify the settings.

e. Click **Save** to save the details.

f. Repeat the same steps after selecting the opva_src database connection.

g. Enter values for the following fields:

Name — Keep the Logical name as opva_src for the database connection.

Type — Select Source as the Type.

Connection Type — Select a connection type for the database connection.

Instance or TNS Name — Enter the - Enter the Argus Safety database instance name.

Table Owner — Enter the Data Source schema name given when installing the OPVA schema in the Argus Safety DB Instance.

Table Owner Password — Enter the OPVA schema password.

DB Host — Enter the Argus Safety Database host name.

Port — Enter the Argus Safety Database host port.

Data Source Number – Enter the number 1.

6. Perform the following steps in the DAC to run the OPVA - DATAWAREHOUSE Execution Plan.

a. Navigate to the Execute view, then select the Execution Plans tab.

b. Select OPVA - Data Warehouse Load from the list.

c. Display the Parameters tab, and click Generate.

d. Enter 1 as value for number of copies of parameters, and click **Generate**.

e. On the Execution Plans tab, click Build.

f. On the Execution Plans tab, click Run Now to execute the ETLs.

DAC Configurable Parameters

Following is the list of DAC configurable parameters:

Table 2–1 DAC Configurable Parameters

Parameter	Description
$$p_last_extract_date	This is last refresh time of the source tables minus prune days.
$$p_config_days	Number of days offset to the Current Execution Plan's actual start time adjusted to source database timezone minus prune days.
$$p_datasource_num_id	The ID associated with every source system. The default ID is 1 for Argus Safety.
$$p_enterprise_id	The ID associated for every Enterprise. The default value is 0. Not in use in any of the ETLs at this time.

Table 2–1 (Cont.) DAC Configurable Parameters

Parameter	Description
$$p_rekey_fact	The default value is 0 and set it to 1, if match and merge changes requires a rerun of the Fact rekeying process.
$$p_etl_proc_id	The process ID for the execution plan run.

Note: If the version of Argus Safety Instance used with OPVA is version 6.0.2, then execute the following steps:

1. Open the PowerCenter Workflow Manager and connect to the repository where the OPVA Informatica folder is imported.

2. Navigate to the Connections -> Relational menu to open the Relational Connection Browser.

3. Click on opva_src and click on 'Edit'.

4. Remove the contents (call opvaUtilSecPkg.psetcontext();)in the Attribute - Connection Environment SQL.

5. Click OK to save the changes.

2.4 Configuring the OBIEE Repository and Webcatalog

2.4.1 Prerequisites

Ensure OBIEE 11g (11.1.1.1.5.0) is installed and the Administrator Console and the Enterprise Manager (Fusion Middleware Control) is running by checking the following URLs:

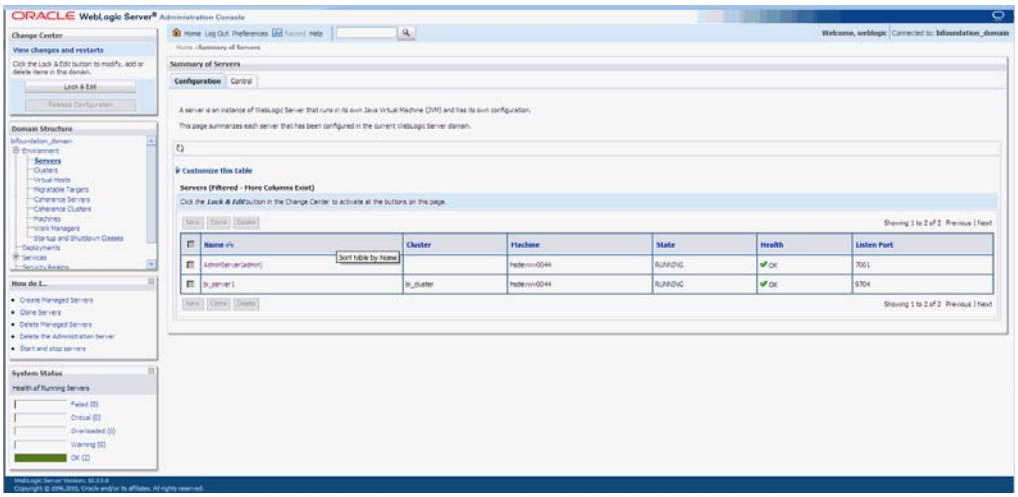
- http://<machinename>.<port>/console
- http://<machinename>.<port>/em

Note: Port 7001 is the default Weblogic port. It may change based upon the system configuration. Please check with your Oracle Weblogic administrator for the correct port number if the above port does not work as expected.

2.4.2 Deployment of OBIEE Repository and Catalog

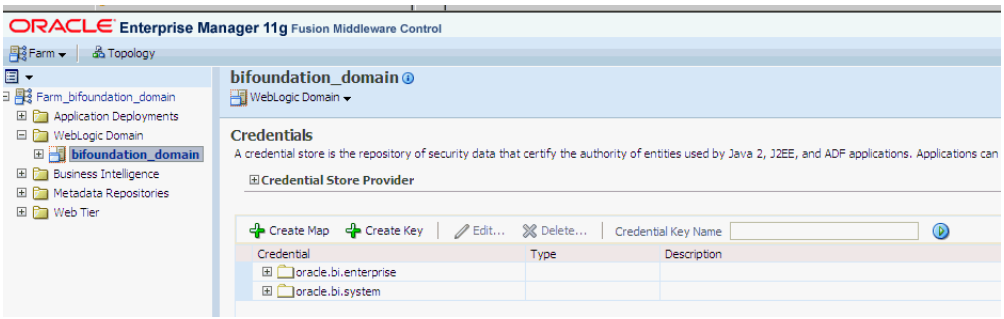
1. Log in to the Administrator Console (http://<machinename>.<port>/console) and navigate to Environment -> Servers. You can see the status of BI Server like below:

Figure 2–1 Oracle WebLogic Server Administration Console



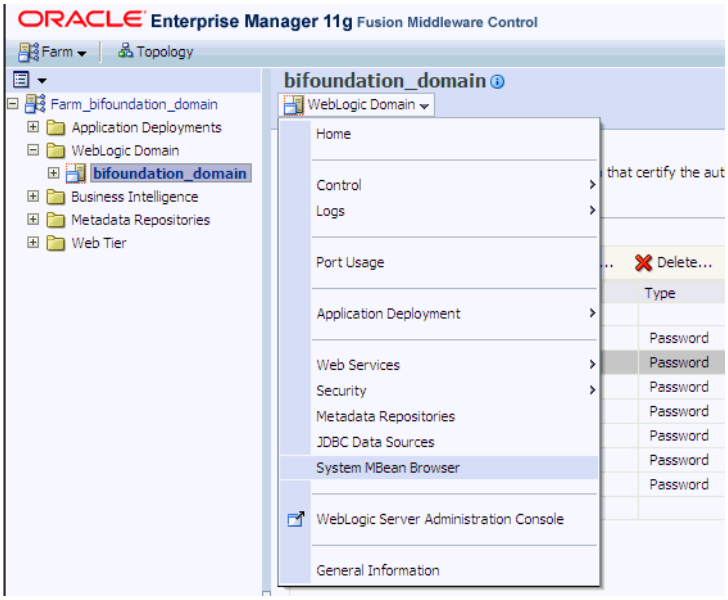
2. Now log in to EM URL `http://<machinename>.<port>/em` using the same username/password used for the Admin Console URL above.
3. Create an encrypted key entry in the EM for the OPVA RPD
   - Expand the tree node Weblogic Domain and click on the bifoundation_domain (the domain created for OBIEE) and invoke the menu Weblogic Domain -> Security -> Credentials to give the screen as shown here:

Figure 2–2 The bifoundation_domain Screen



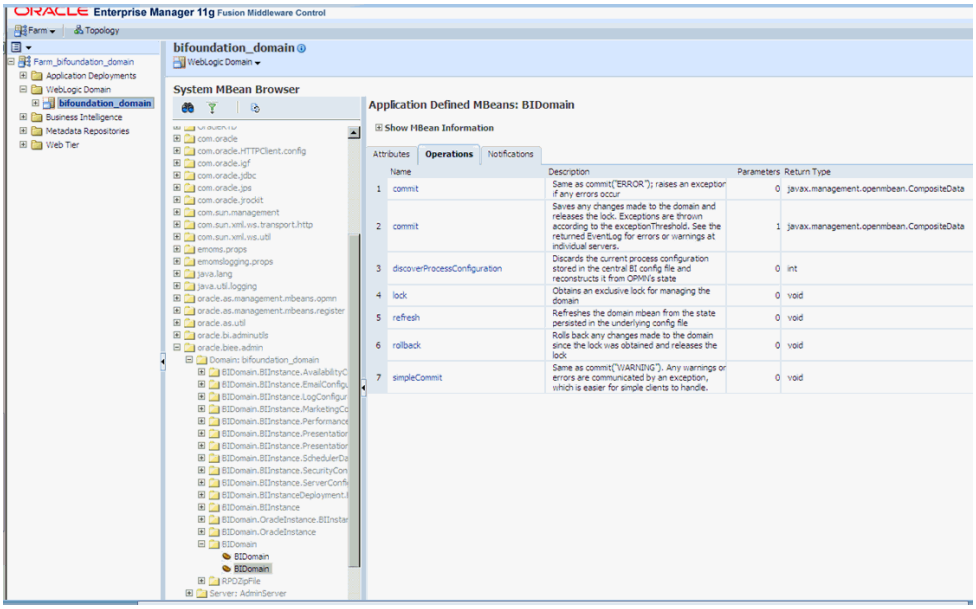
   - Click on Create Key and enter details as given here for the OPVA rpd file:
     - Select Map: oracle.bi.enterprise
     - Key: repository.opva
     - Type: password
     - User Name: Administrator
     - Password: password of choice
   - Click OK to create the security key
4. Invoke the System MBean Browser as shown here:

Figure 2–3 The WebLogic Domain Drop-down List



5. Navigate to the MBean Application Defined MBeans -> oracle.biee.admin -> Domain: bifoundation_domain -> BIDomain -> BIDomain as shown below

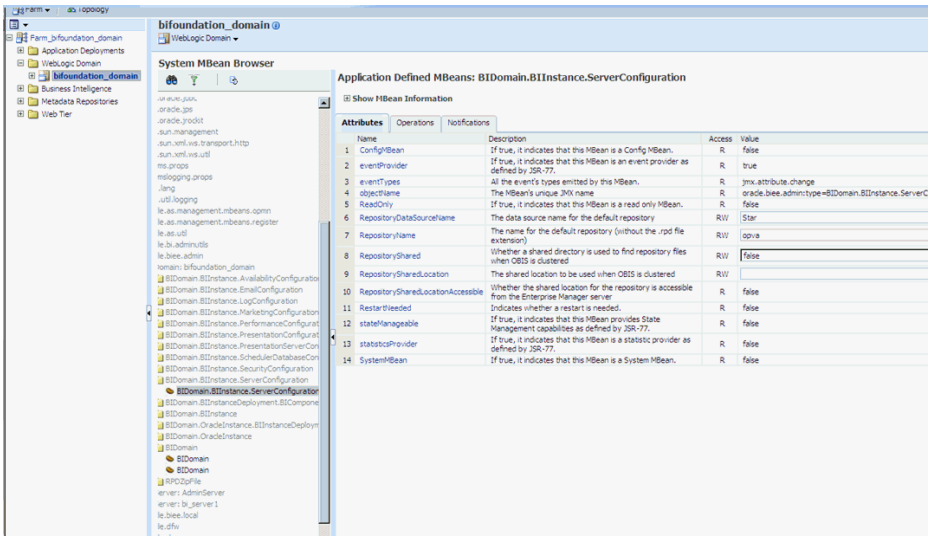
Figure 2–4 The Application Defined MBeans: Operations Screen



6. Navigate to the Operations Tab and click on lock, and then click on the Invoke button to lock the domain.

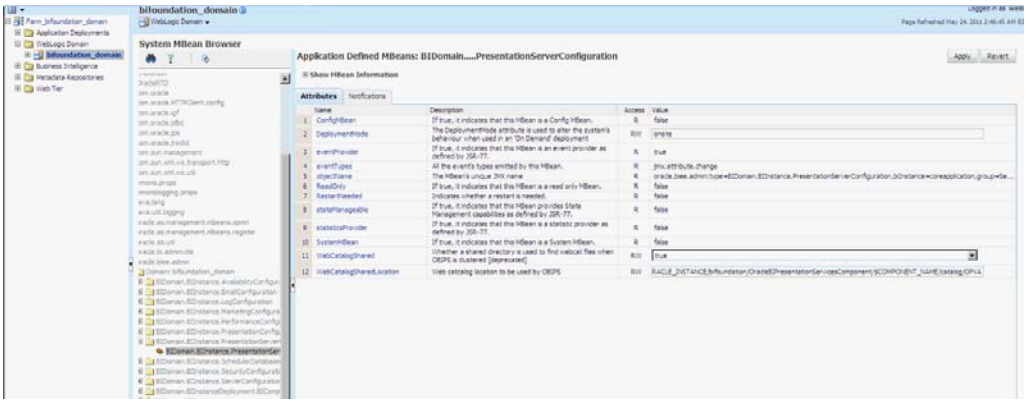
7. In the same window navigate to the Domain: bifoundation_domain -> BIDomain.BIInstance.ServerConfiguration - BIDomain.BIInstance.ServerConfiguration as shown below and in the Attributes tab change the attribute RepositoryName as "opva" as shown below and click on Apply.

Figure 2–5 The Application Defined MBeans: Attributes Screen



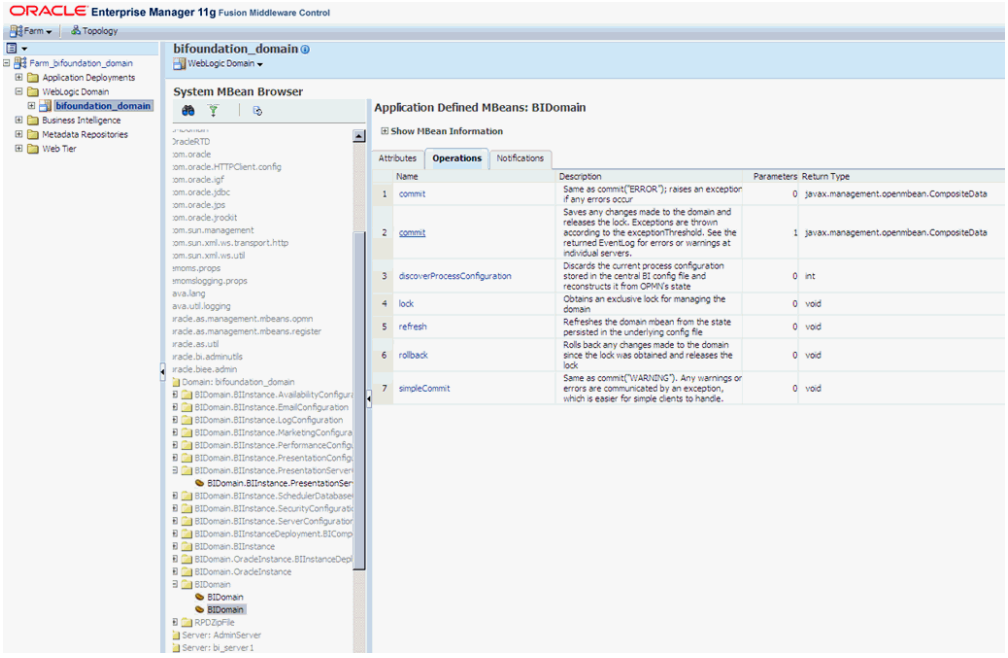
8. Next Navigate to Domain: bifoundation_domain -> BIDomain.BIInstance.PresentationServerConfiguration -> BIDomain.BIInstance.PresentationServerConfiguration and in the Attributes tab change the attribute WebCatalogSharedLocation as $ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/$COMPONENT_NAME/catalog/OPVA and click on Apply.

Figure 2–6 The Application Defined MBeans: BIDomain: Attributes Screen



9. Navigate back to the MBean Application Defined MBeans -> oracle.biee.admin -> Domain: bifoundation_domain -> BIDomain -> BIDomain and in the Operations tab invoke the commit operation pass the parameter as ERROR.

Figure 2–7 The Application Defined MBeans: BIDomain: Operations Screen



10. Navigate through the tree control (Business Intelligence -> coreapplication) to invoke the coreapplication screen for OBIEE and click on the Deployment tab.
11. Click on Lock and Edit Configuration and click on the Repository sub tab to invoke the screen as shown below. Add the information as given here:
    - Repository file: Upload the OPVA.rpd from <OPVA_Home>\report\opva.rpd of OPVA.
    - Repository Password: opva123

Note: If the OBIEE Server is not the same machine as the install machine, then copy the catalog file from <opva_home>\report\catalog\opva.zip into the machine where OBIEE server is installed.

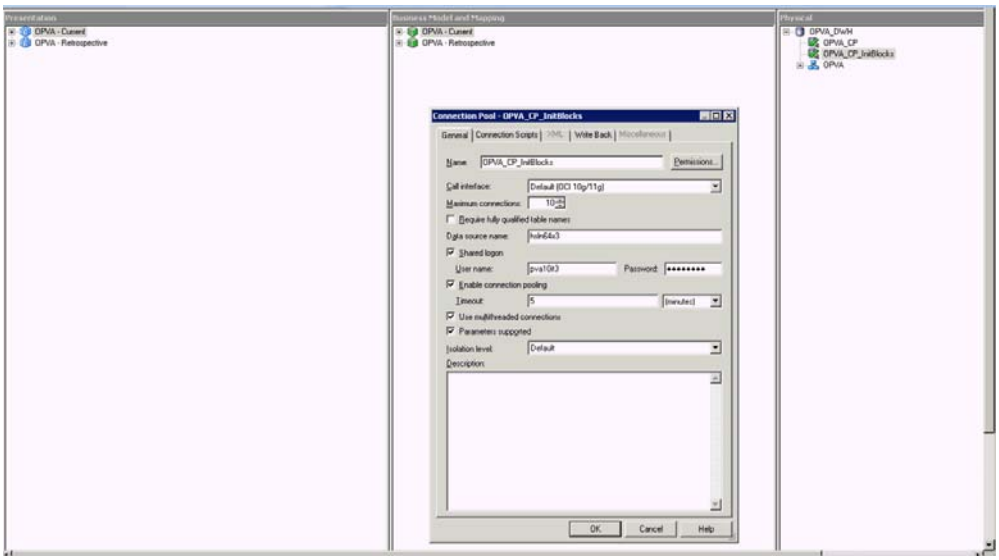
- Confirm the catalog location as $ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/$COMPONENT_NAME/catalog/opva
- Copy the Catalog from the opva installed directory to the location mentioned above in point c ex: installed location: d:\opva\report\catalog\opva.zip to the location in WLS: <MIDDLEWARE_HOME>\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\catalog and extract the zip file to the same location
- Click on Apply and then Activate Changes
- Restart the OBIEE Services

2.4.2.1 Post-deployment of the OPVA RPD

Open the OPVA RPD in the Administration Tool in online mode and change the connection pool settings for both OPVA_CP and OPVA_CP_InitBlocks to point to the DWH RPD Schema created during installation:

1. Repository Password: opva123
2. User: weblogic or BISystemUser
3. Password: Password for the user mentioned above

Figure 2–8 The OPVA RPD Screen



Note: If the version of the Argus Safety instance configured for OPVA application is 6.0.2, then navigate to the Connection Scripts tab in the Connection Pool settings of 'OPVA_CP' and remove the PLSQL call 'call opvaUtilSecPkg.pSetContext();' and save the changes.

2.5 Configuring the OBIEE Help files

Note: If the OBIEE Server is not the same machine where the installer is run, then copy the zip file <opva_home>\help\opva_help.zip into the machine where OBIEE server is installed.

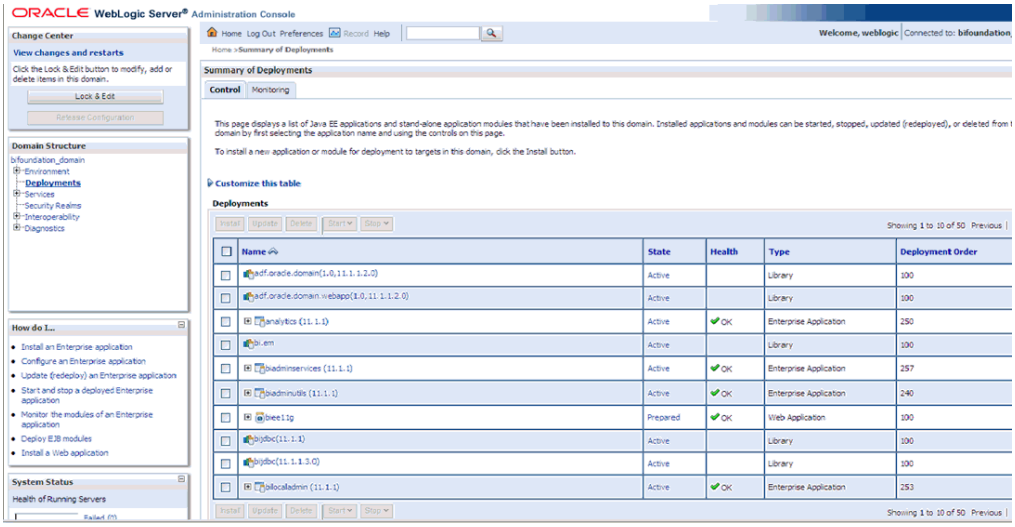
2.5.1 Configuring the Help links in the Dashboards and Reports

1. Navigate to the following path in your Weblogic Server:

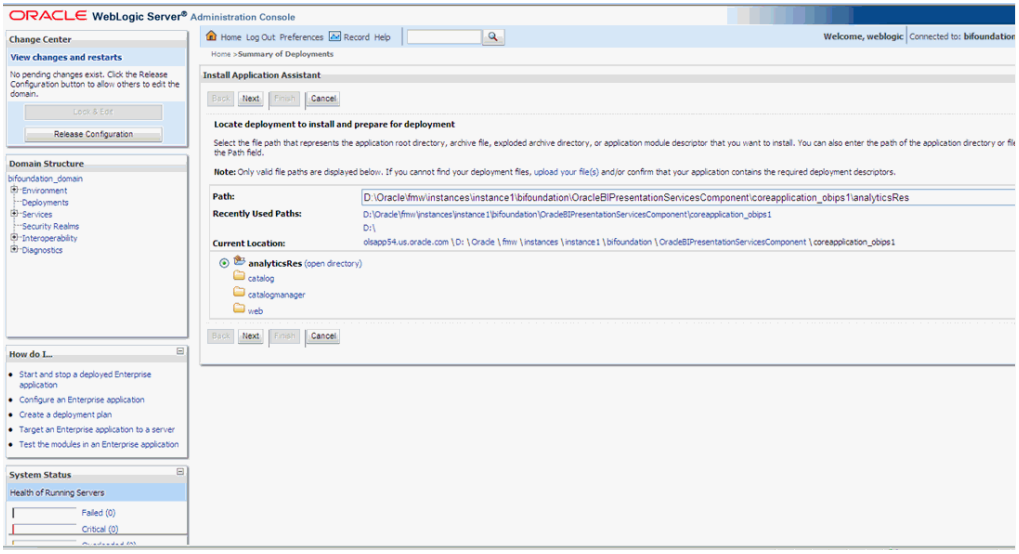
   <MIDDLEWARE_HOME>\fmw\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\analyticsRes\

2. Extract the contents of the help.zip file into the path listed above.
3. Log in to Console (Log in to the Weblogic Server).

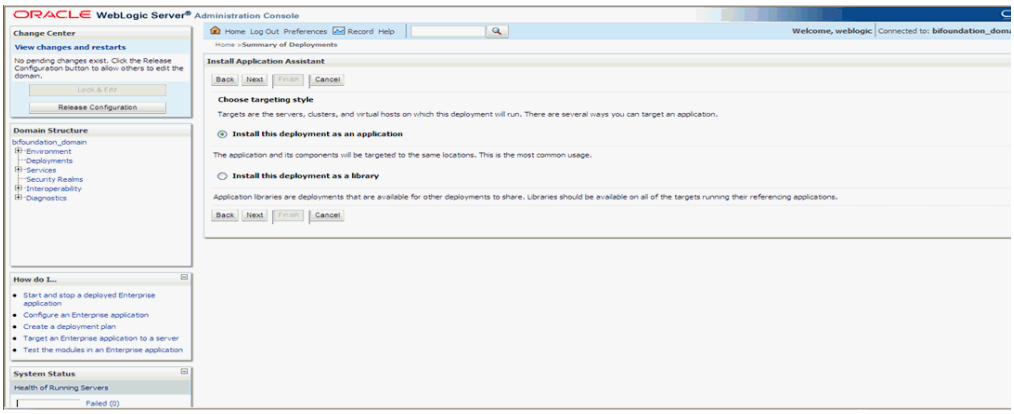
4. Navigate to Deployments.
5. Click on 'Lock & Edit' in the left pane to enable the 'Install' button.



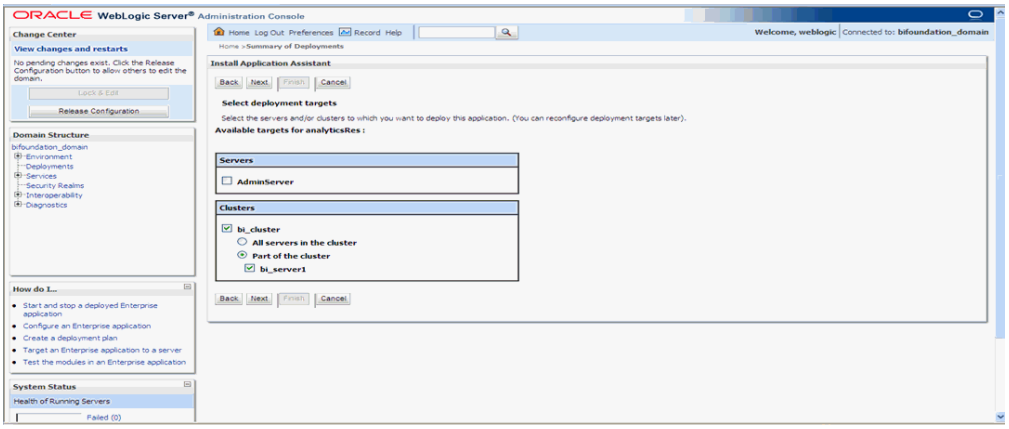
6. Click on Install and navigate to '<MIDDLEWARE_HOME>\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1'.
7. Select 'analyticsRes' and click 'Next'.



8. Select 'Install this deployment as an application' (default) and click 'Next'.



9. Select 'Deployment targets', choose 'bi_server1', and click 'Next'.

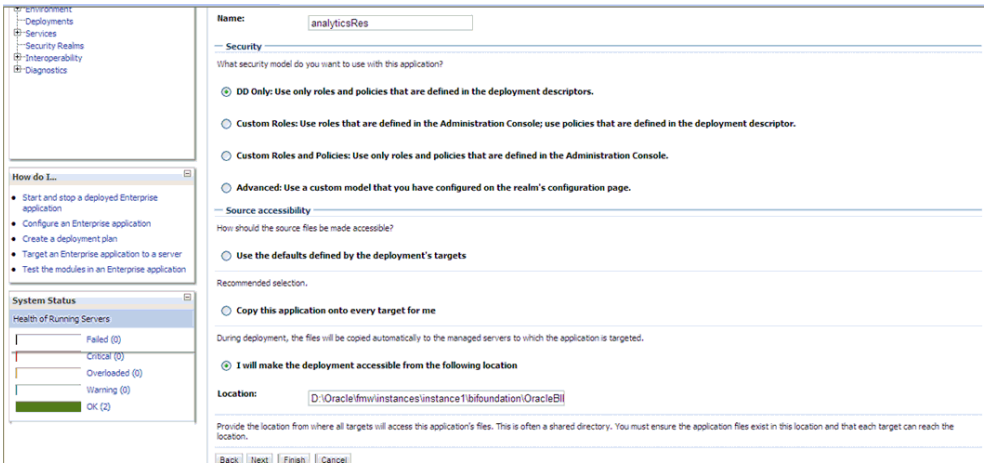


10. Under 'Source accessibility:'

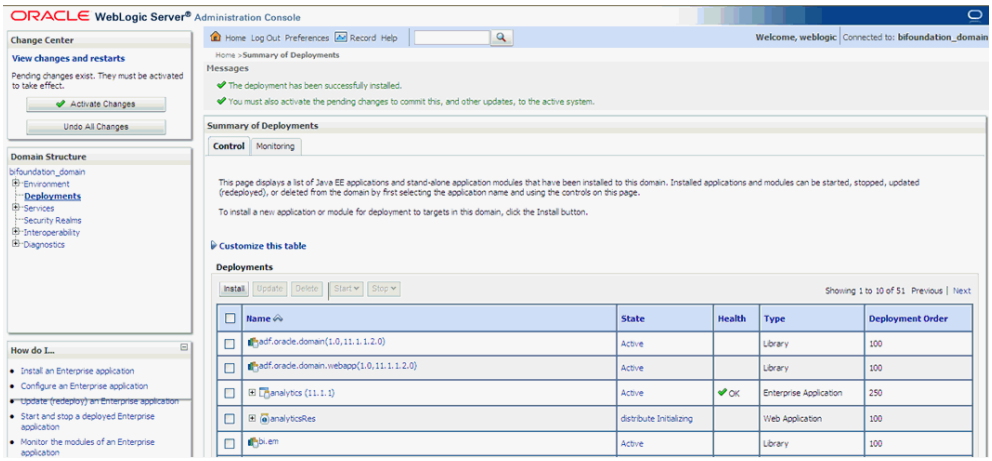
    Select 'I will make the deployment accessible from the following location'

    '<MIDDLEWARE_HOME>\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\analyticsRes'

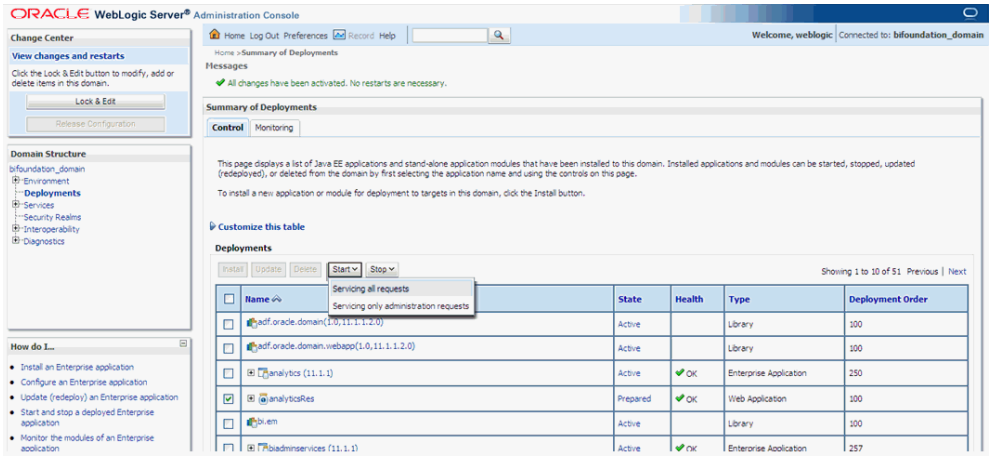
11. Click Finish.



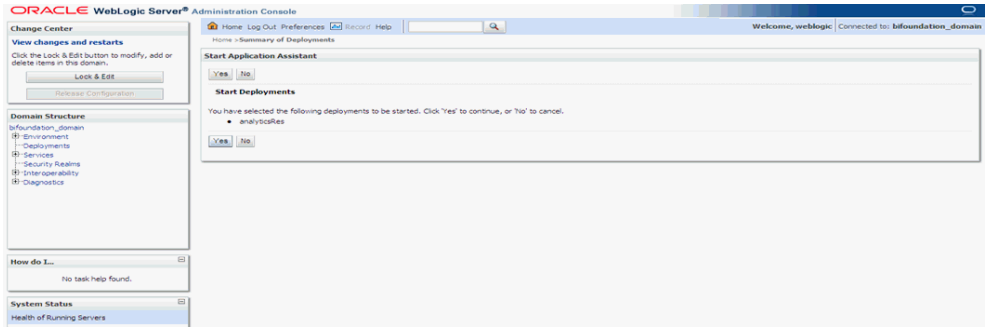
The 'analyticsRes' should appear under Deployments.



12. Click on Active Changes, select 'analyticsRes', and click the Start button on the screen.

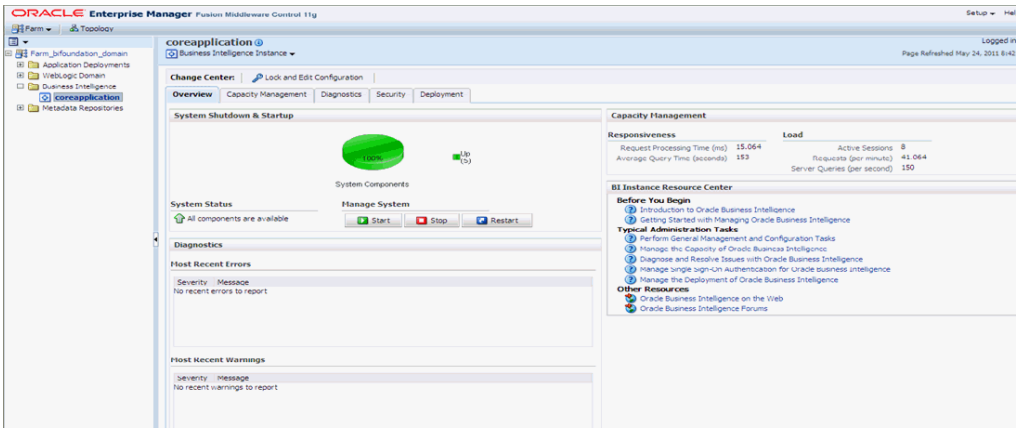


13. Start Application Assistant, and click Yes.



The 'analyticsRes State' should be active after starting the above. Logout from the Console.

14. Log in to EM (Enterprise Manager) and restart the BI Components.



Once the BI components have been restarted successfully, log in to Analytics, and check the Brand Name and help links provided in the Dashboards.

2.6 Configuring SSO Using Oracle Access Manager

Note: This section is only applicable if OAM is used.

This section describes how to configure SSO in the Oracle Access Manager (OAM).

The following are the pre-requisites for this configuration:

- There should be an OAM installation (Identity server, Access server, WebPass, Policy Manager).
- User profiles should exist in the LDAP server as well as in Argus Safety with the same credentials.
- Oracle Web Tier 11.1.1.3 should be installed on the same server where the OBIEE server is installed and configured with the Weblogic Server hosting OBIEE.

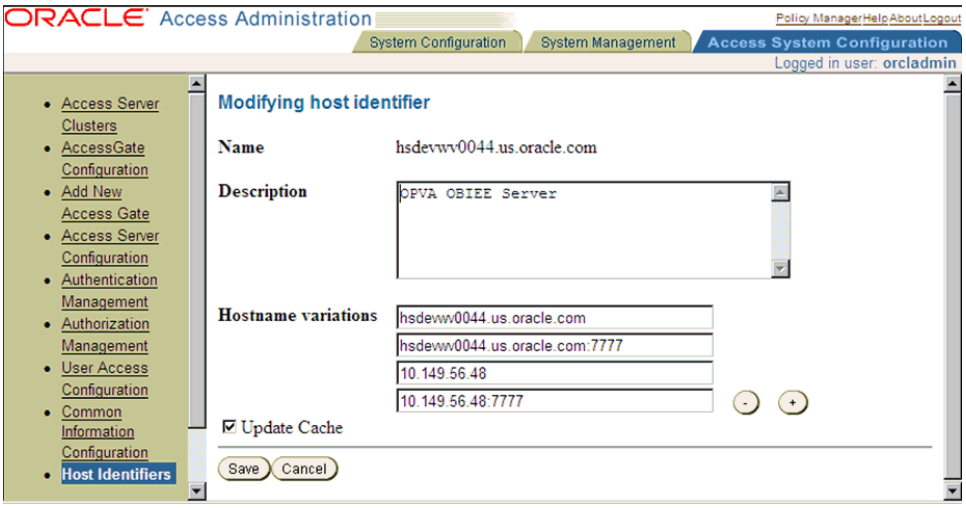
Perform the following steps to install SSO on the OAM:

1. Navigate to the Access System console of OAM and click the Access System Configuration tab. Click Host Identifiers on the left panel and provide the Fully Qualified Domain Name (FQDN), IP Address and both entries along with port numbers of the OPVA Web Tier machine. Click Save.

   For example:

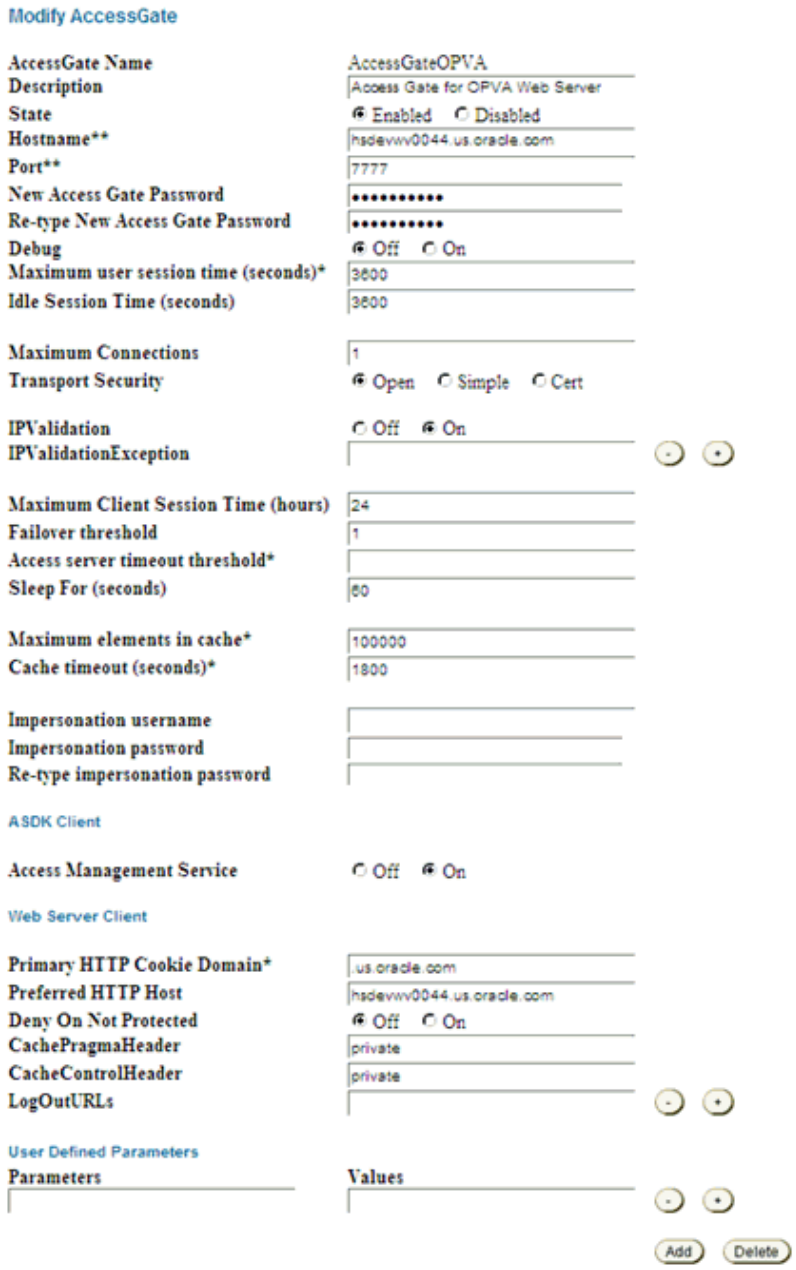
   - hsdevwv0044.us.oracle.com
   - hsdevwv0044.us.oracle.com:7777
   - 10.149.56.48
   - 10.149.56.48:7777

Figure 2–9 The Access System Administration: Host Identifiers Screen



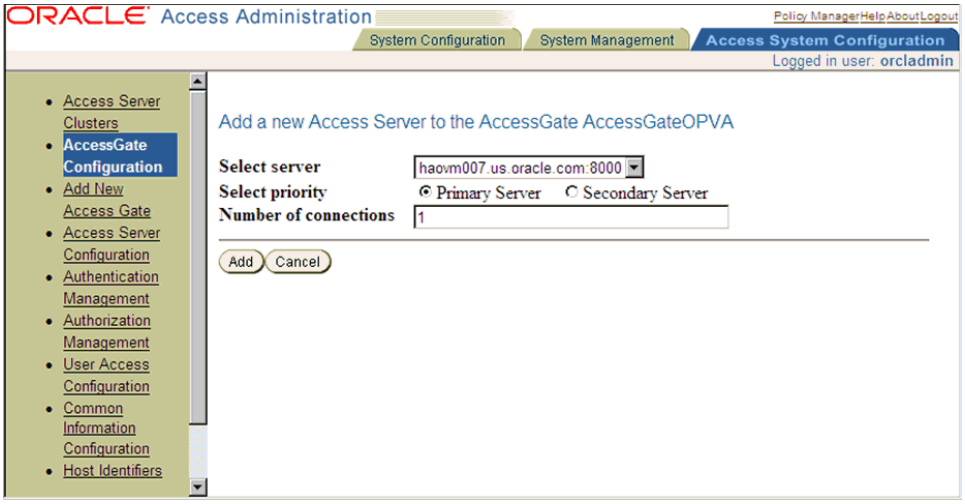
2. In the Access System console of OAM, click **Access System Configuration**.
3. Click **Add New Access Gate** link on the left panel.
4. Provide details like access gate name, port, and password. Also, enter the following details:
   - Hostname: Provide the FQDN of the OPVA Web Tier Server where you will install the webgate
   - Access Management Service: Set this radio button as 'On'
   - Primary HTTP Cookie Domain: Provide FQDN of the machine where you will install the webgate, prefixed by a period. For example, **.idc.oracle.com** and please ensure the '.' before the FQDN
   - Preferred HTTP Host: Provide the same value as the Hostname
   - CachePragmaHeader: Enter value as 'private'
   - CacheControlHeader: Enter value as 'private'
   - Once you have entered all the above details, click Save to add the webgate.

Figure 2–10 The Host Identifiers Screen with Entered Information



5. You will see the message "Please associate an Access Server or Access Server Cluster with this AccessGate."
6. Click List Access Servers.
7. In the following screen, click Add. Select an access server from the drop-down and click Add to associate the webgate with the access server.

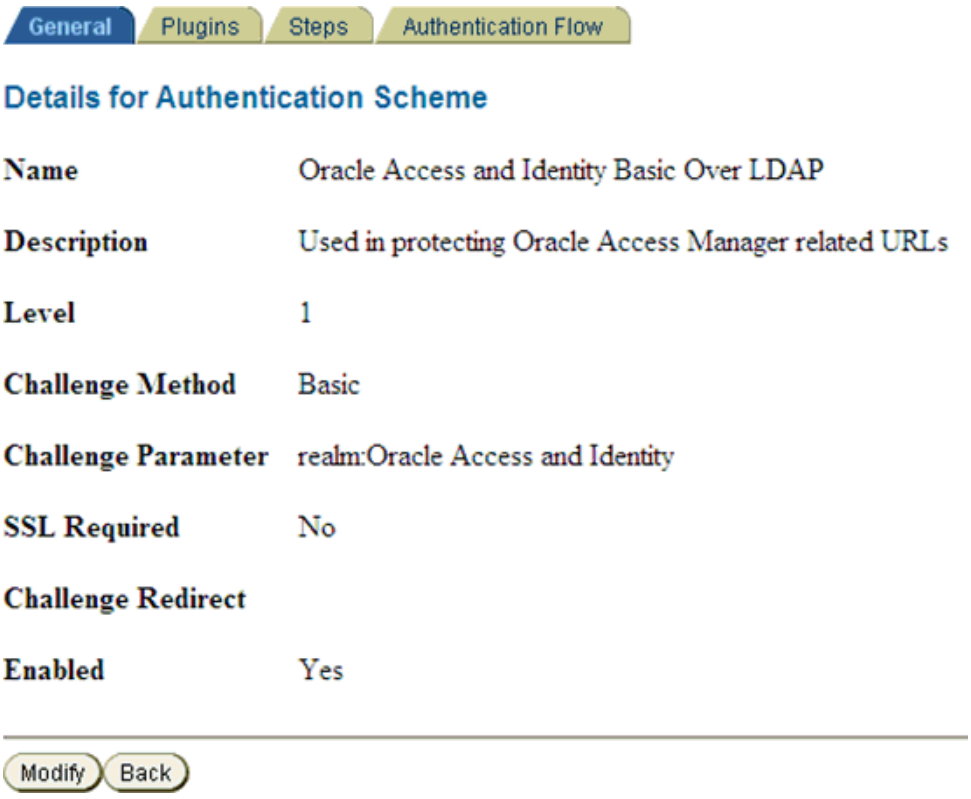
Figure 2–11 The Access System Configuration: Access Gate Configuration Screen



Note: The access servers in this list will appear based on the access servers installed in the OAM image or installation that you have. Do not attempt adding Access Servers from OAM Console.

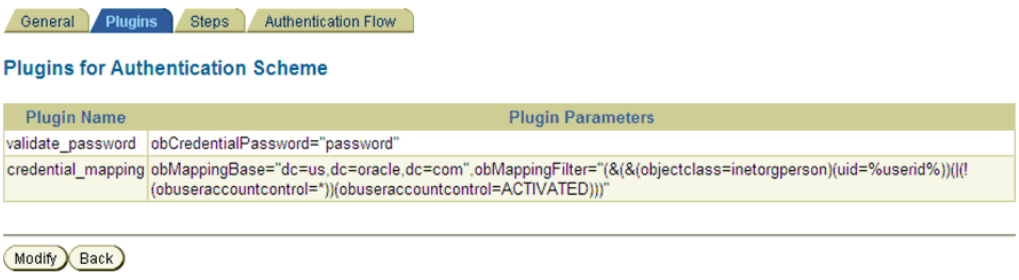
8. In the Access System Configuration Tab, click on Authentication Management and ensure that there is at least one schema for LDAP Authentication. If no schema exists, follow these steps:
   - Click on Add and enter the information as show here:

Figure 2–12 Authentication Management: General tab



- Click on Save, click the Plugins Tab, and add the following:
  - Plugin Name: validate_password
  - Plugin Parameters: obCredentialPassword="password"
  - Plugin Name: credential_mapping
  - Plugin Parameters: obMappingBase="dc=us,dc=oracle,dc=com",obMappingFilter="(&(&(objectclass=inetorgperson)(uid=%userid%))(|(!(obuseraccountcontrol=*))(obuseraccountcontrol=ACTIVATED)))"

Figure 2–13 Authentication Management: Plugins tab

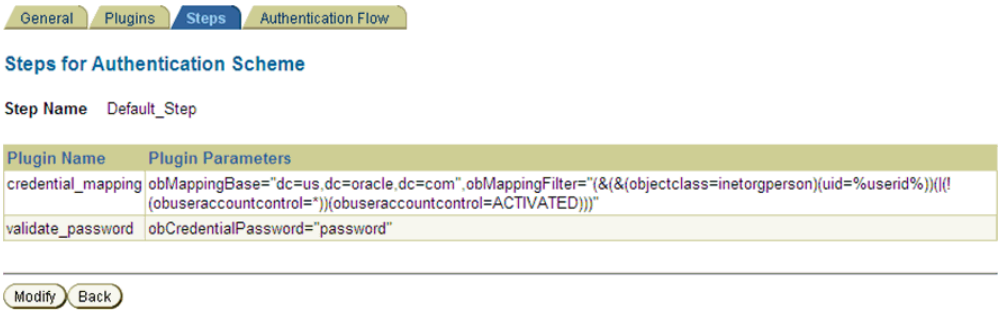


- Click on Save.
- Choose the Steps Tab next and add a new step 'Default_Step'. Add the 'Available Plugins' to the Active Plugins in the order:
  - credential_mapping

– validate_password

Note: The order of Plugins added is important.

Figure 2–14 Authentication Management: Steps tab

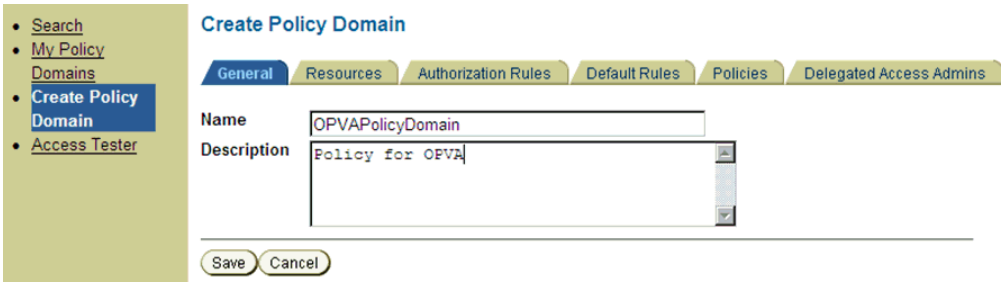


- Click on Save.
- Choose the Authentication Flow Tab and configure as shown below:

Figure 2–15 Authentication Management: Authentication Flow tab

9. Click on Policy Manager to setup the rules for protecting the OPVA Application URL as follows:
   - Click on Create Policy Domain.
   - Enter the details as given below:

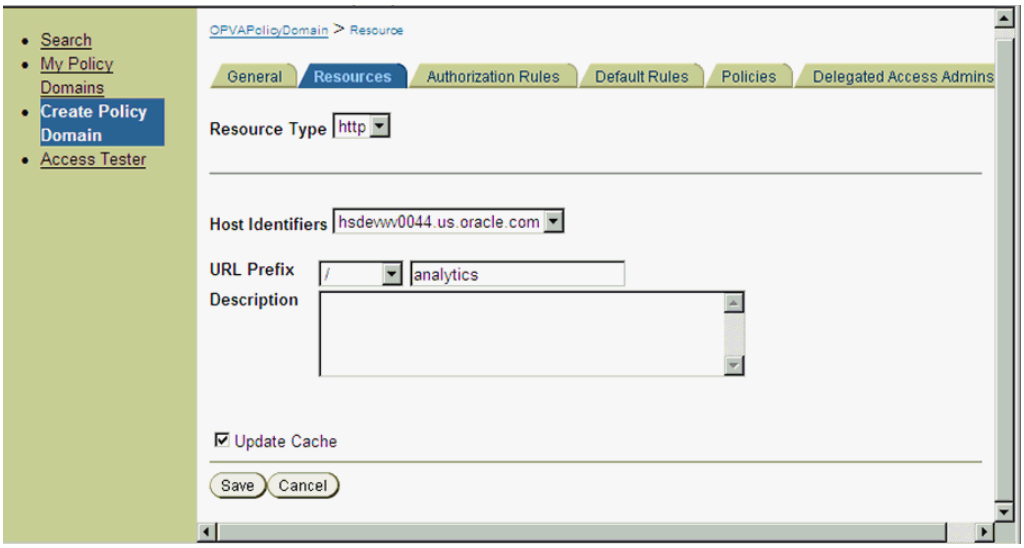
Figure 2–16 Create Policy Domain: General tab



- Click on Save, and then choose 'Modify' set enabled to Yes.

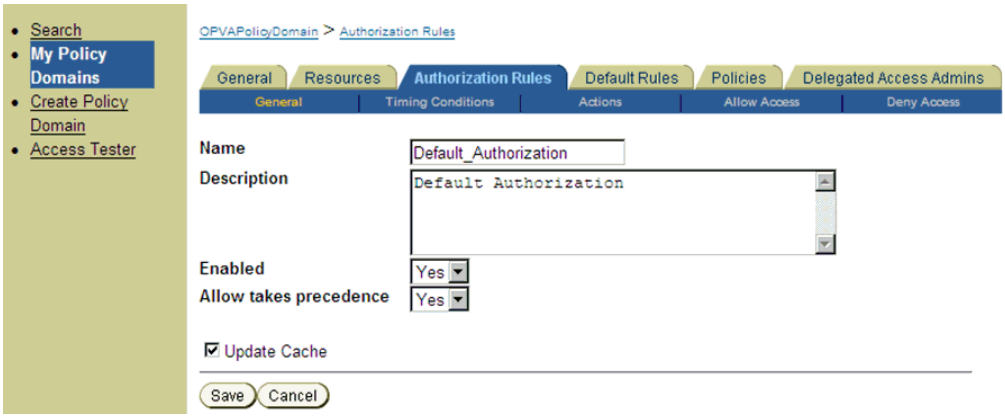
- Navigate to the 'Resources' tab and click on Add and enter details as shown here and click on Save:

Figure 2–17 Create Policy Domain: Resources tab



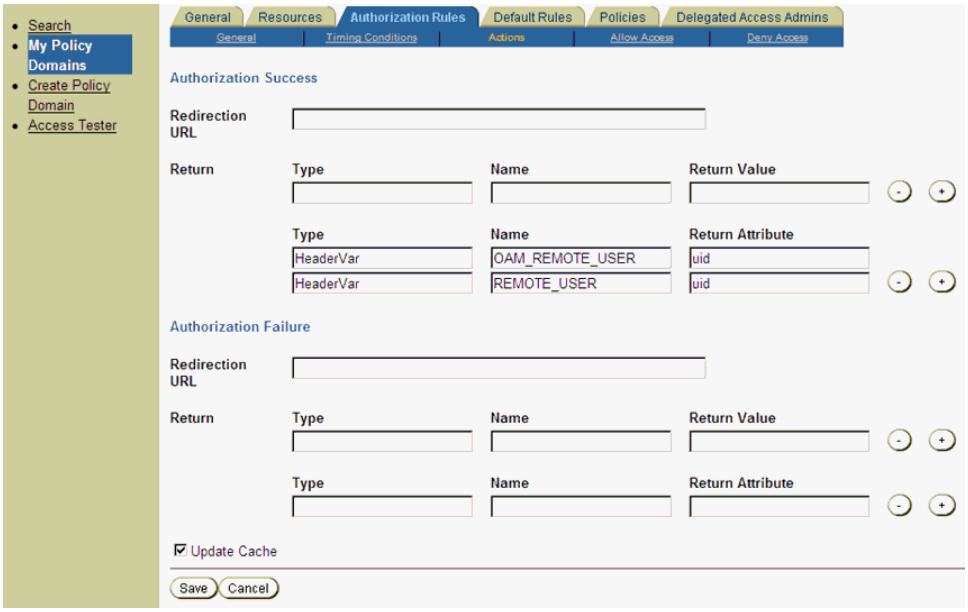
- Navigate to Authorization Rules and click on Add and enter details as given here and save the details:

Figure 2–18 My Policy Domains: Authorization Rules tab



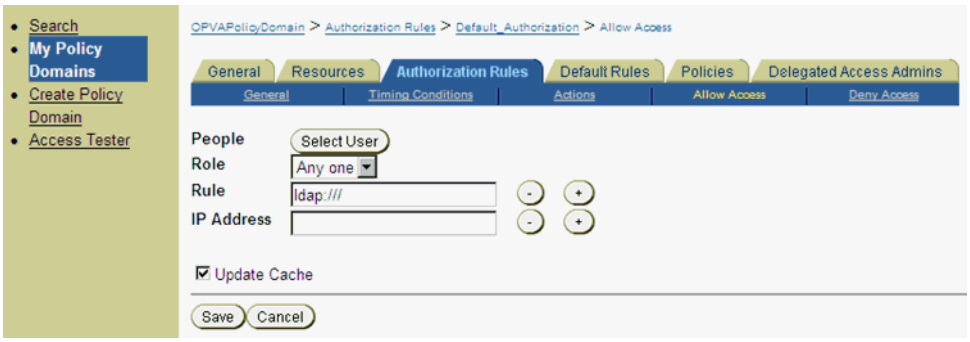
- Navigate to the Actions sub tab and click on add. Enter the details as shown here and click on Save:

Figure 2–19 My Policy Domains: Authorization Rules tab: Actions sub-tab



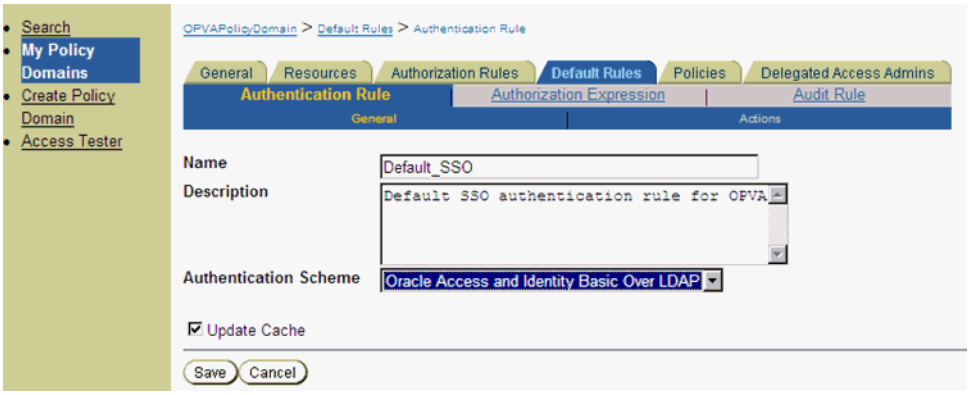
- After saving these details click on the Allow Access sub tab and click Add, enter the following details and click on Save:

Figure 2–20 My Policy Domains: Authorization Rules tab: Allow Access sub-tab



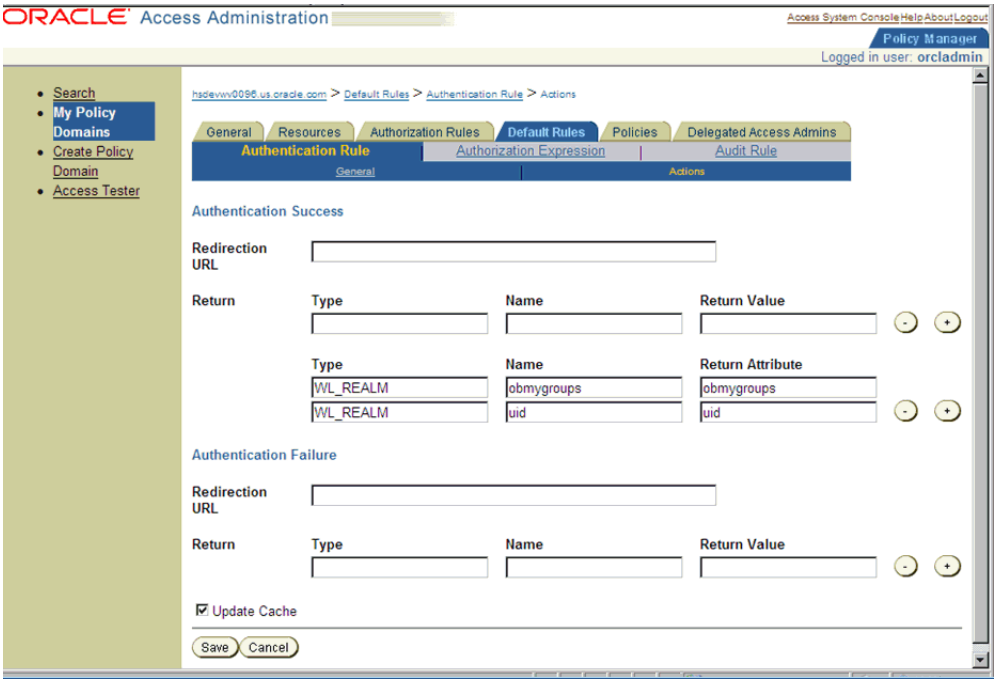
- Now click on Default Rules tab and add a new Authentication Rule by clicking on Add and entering information as given here in the General sub tab:

Figure 2–21 My Policy Domains: Default Rules tab: General sub-tab



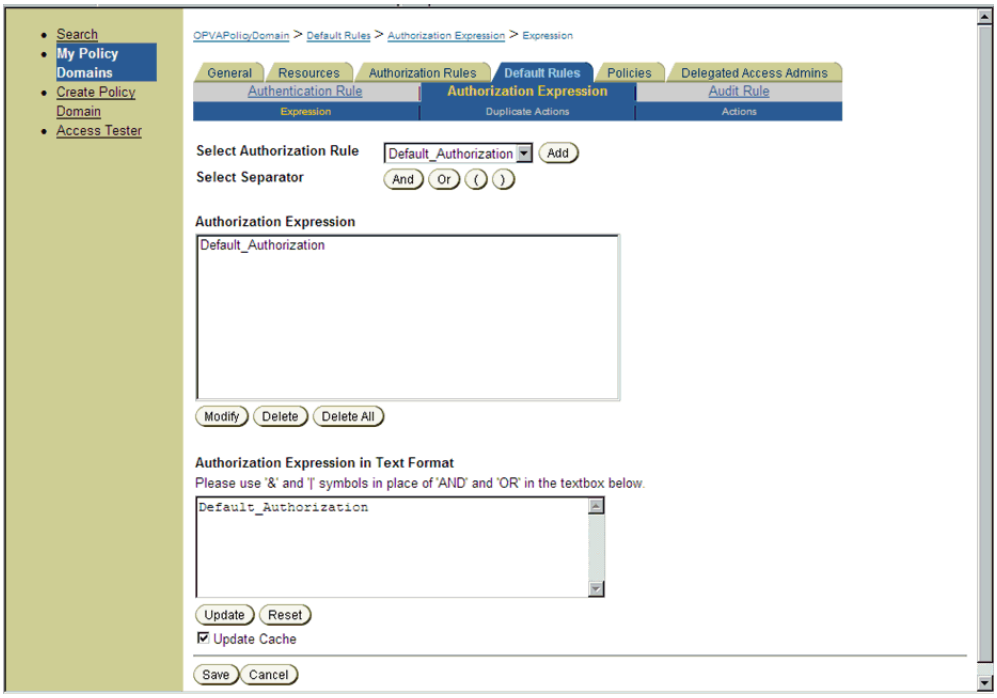
- Save the details in the General sub tab, and choose the Actions sub-tab.
- Click on Add and enter the details as shown here and save the details:

Figure 2–22 My Policy Domains: Default Rules tab: Actions sub-tab



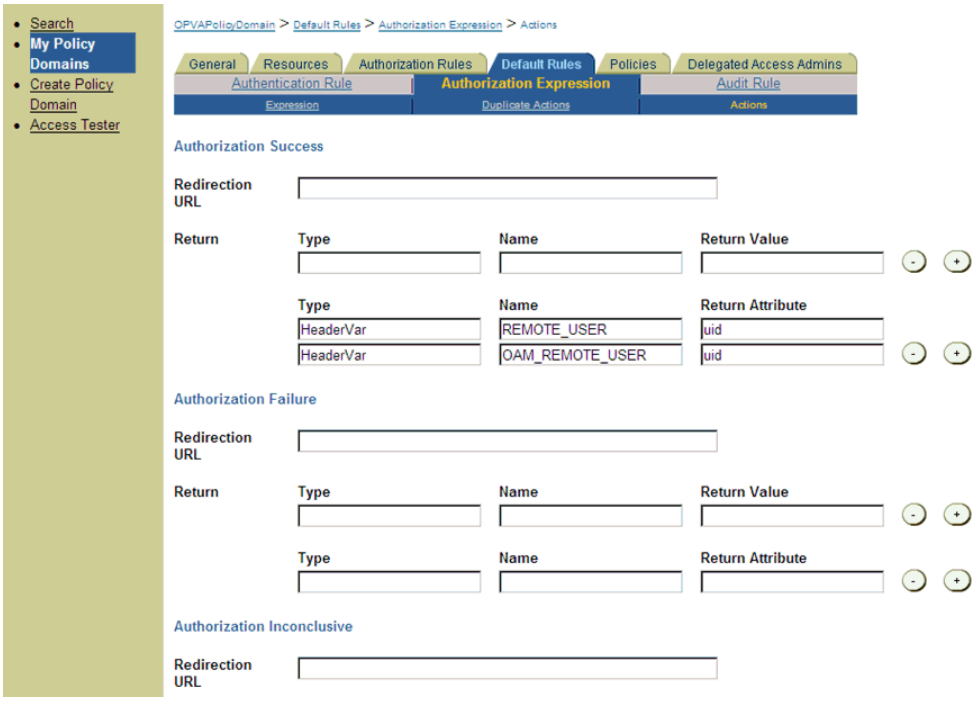
- Choose Authorization Expression tab and click on Add to add an entry per the details given here in the Expression sub tab:

Figure 2–23 My Policy Domains: Default Rules tab: Expression sub-tab



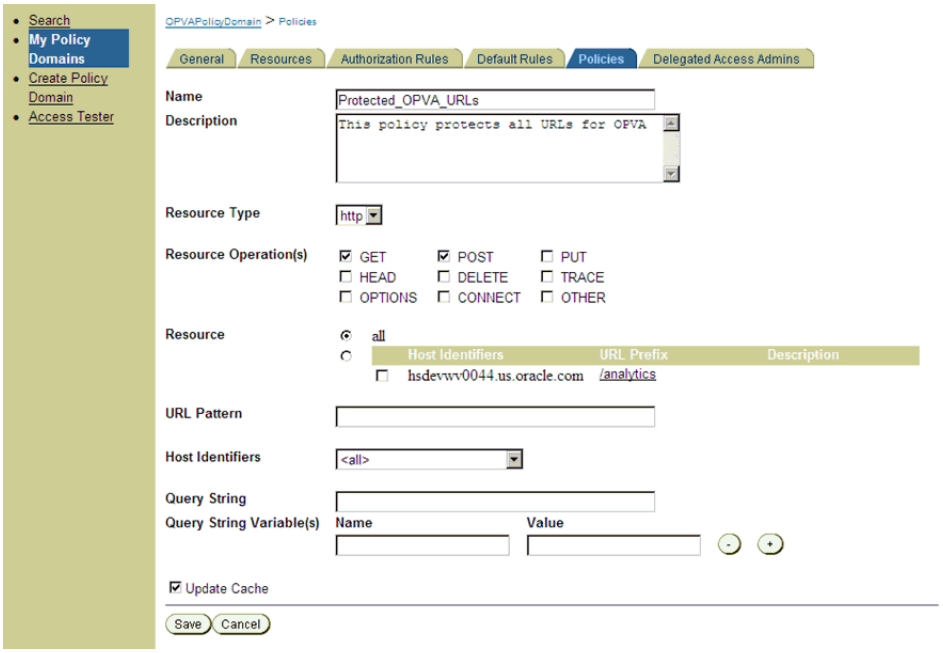
- Click on Save.
- Select the Actions sub tab and click on Add, enter the details as given here:

Figure 2–24 My Policy Domains: Default Rules tab: Actions sub-tab



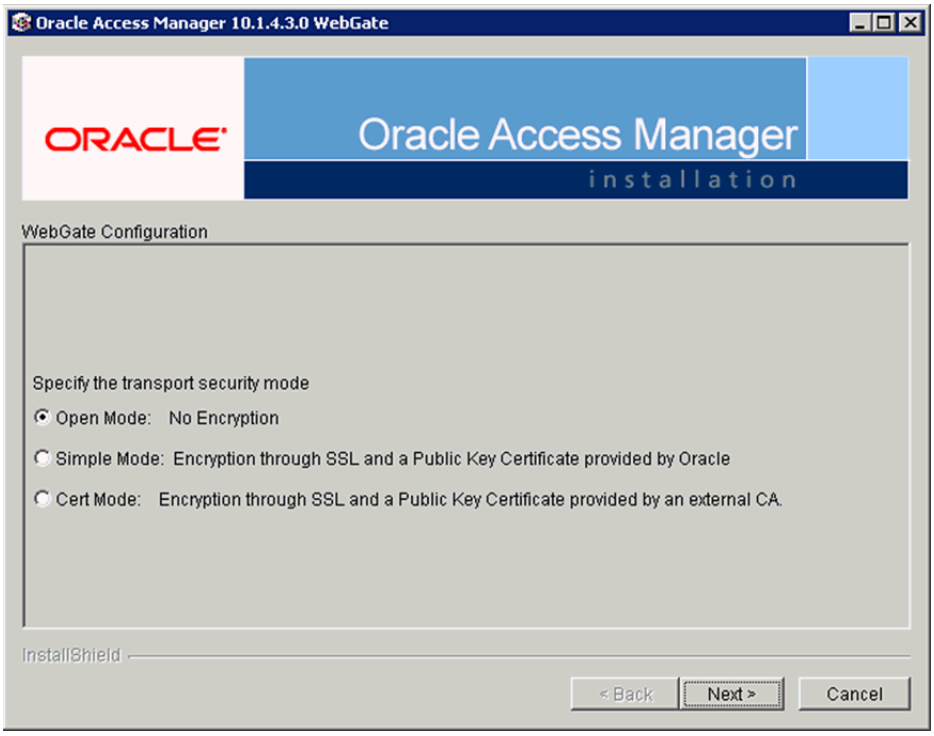
- Click on Save.
- Click on the Policies tab and choose the Add button, enter details as given here:

Figure 2–25 My Policy Domains: Policies tab



10. Navigate to the OPVA Web Tier Machine, which is the machine where you have installed OPVA OBIEE Server and run the installer for Webgate (OFM Webgate 11g for OAM 10.1.4.3.0).
    - Once the installer launches, click Next on the initial two information screens
    - Choose the install directory for the webgate and click Next for the information on the installation.
    - Click Next to begin the installation of webgate, once completed it starts the configuration, where in enter the details as given here below:

Figure 2–26 Oracle Access Manager Installation Screen



- Click Next to continue the configuration and enter details as shown here:
  - WebGate ID: AccessGateOPVA
  - Password: Password as given during creation of the access gate in OAM
  - Access Server ID: Access_svr_idm_vm
  - Hostname: Server name where OAM Access Server is installed
  - Port: 8000 (Port number on the which the Access Server is listening to)
- Click 'Next' and in the next screen choose the radio button 'Yes' and select 'Next' to continue configuring the httpd.conf file
- Select the location for the httpd.conf file, typically it will be at OracleWebTierHome/instances/instance2/config/OHS/ohs1/httpd.conf and then click OK to continue with configuration
- Restart the Web Server to complete the installation
- Verify the installation of the webgate by checking the URL:

  `http://<machinename>.<port>`
  `/access/oblix/apps/webgate/bin/webgate.cgi?progid=1`

11. Configure the HTTP Server as a reverse proxy for the WebLogic Server
    - Modify the file mod_wl_ohs.conf present in the location to reflect as shown below: Location: OracleWebTierHome\instances\instance2\config\OHS\ohs1

> **Note:** This is a template to configure mod_weblogic.

LoadModule weblogic_module "${ORACLE_HOME}/ohs/modules/mod_wl_ohs.so"

This empty block is needed to save mod_wl related configuration from EM to this file when changes are made at the Base Virtual Host Level

<IfModule weblogic_module>

WebLogicHost <WEBLOGIC_HOST>

WebLogicPort <WEBLOGIC_PORT>

Debug ON

WLLogFile /tmp/weblogic.log

MatchExpression *.jsp

WebLogicHost hsdevwv0044.us.oracle.com

WLTempDir <MIDDLEWARE_HOME>\Oracle_WT1\error_Logs

WLLogFile <MIDDLEWARE_HOME>\Oracle_WT1\error_Logs\ohs1_error.log

Debug ON

DynamicServerList Off

WebLogicPort 7001

<Location /analytics>

SetHandler weblogic-handler

WebLogicHost hsdevwv0044.us.oracle.com

WebLogicPort 9704

</Location>

</IfModule>

<Location /weblogic>

SetHandler weblogic-handler

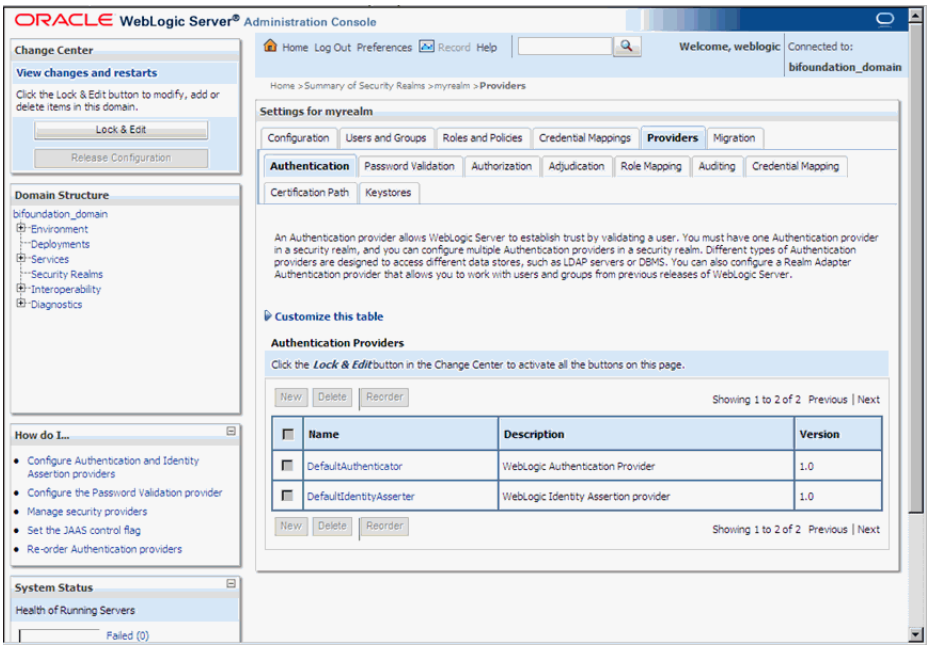
PathTrim /weblogic

ErrorPage http:/WEBLOGIC_HOME:WEBLOGIC_PORT/

</Location>

12. Restart the Web Tier Instance in WebLogic EM
    - Configure a new Authenticator for Oracle WebLogic Server
    - Log in to the WebLogic Server Administrator Console and navigate the Security Realms-> myrealm and click on the Providers tab

Figure 2–27 myrealm Settings: Providers tab



- Click on Lock & Edit in the right-hand corner of the web page, highlighted as Change Center
- Click New to create a new Authentication Provider and add the details as given here:
  - Name: OPVAOIDAuthenticator, or a name of your choosing
  - Type: OracleInternetDirectoryAuthenticator
  - After saving the details, click on the new Authenticator created and enter details as given here:
  - In the Common sub tab change the Control Flag as SUFFICIENT
  - Click on Save
  - Click the Provider Specific tab and enter the following required settings using values for your environment:

    Host: Your LDAP host.

    For example: hsdevlv0016.us.oracle.com

    Port: Your LDAP host listening port.

    For example: 389

    Principal: LDAP administrative user.

    For example: cn=orcladmin,cn=Users,dc=us,dc=oracle,dc=com

    Credential: LDAP administrative user password

    User Base DN: Same searchbase as in Oracle Access Manager.

    For example: cn=Users,dc=us,dc=oracle,dc=com

    All Users Filter:

    For example: (&(uid=*) (objectclass=person))

User Name Attribute: Set as the default attribute for username in the directory server.

For example: uid

Group Base DN: The group searchbase

For example: cn=Groups,dc=us,dc=oracle,dc=com

Leave the other defaults as is

GUID Attribute: the GUID attribute defined in the OID LDAP Server

For example: uid

Click Save.

13. Configuring a new Identity asserter for WebLogic Server
    - In Oracle WebLogic Server Administration Console, select Security Realms from the left pane and click the realm you are configuring. For example, myrealm. Select Providers.
    - Click New. Complete the fields as follows:
      - Name: OPVAOAMIdentityAsserter, or a name of your choosing
      - Type: OAMIdentityAsserter
      - Click OK
      - Click on the newly created Asserter and set the Control Flag to REQUIRED
      - Click Save
      - Navigate the Provider Specific tab and enter details as given here:

        Transport Security: open

        Application Domain: OPVAPolicyDOmain, as set in the OAM Policy Manager

        Access Gate Password: the password for the access gate

        Access Gate Name: AccessGateOPVA, as specified in the OAM Access Console

        Primary Access Server: hsdevlv0016.us.oracle.com:8000, OAM server with port

        Click on Save
    - In the Providers tab, perform the following steps to reorder Providers:
      - Click Reorder
      - On the Reorder Authentication Providers page, select a provider name and use the arrows beside the list to order the providers as follows:

        OPVAOAMIdentityAsserter

        OPVAOIDAuthenticator

        DefaultAuthenticator

        DefaultIdentityAsserter
      - Click OK to save your changes
    - Activate Changes: In the Change Center, click Activate Changes

- Restart Oracle WebLogic Server

14. The "BISystemUser" present in the default embedded LDAP should be deleted (via Security Realms in the Administration Console Link of the WebLogic Server) and the same/another user should be added in the newly added OID. This then needs to be added to the BI Application Roles as mentioned here:
    - Navigate to the Administration Console->Security Realms -> myrealm -> Users and Groups -> Users select the checkbox against BISystemUser (from Provider: Default Authenticator) and click on delete
    - Navigate to Security Realms -> myrealm -> Roles and Policies -> Realm Roles -> In the tree structure Expand Global Roles node and select the Roles link
    - In the subsequent screen Click on Admin role link
    - Click the button Add Conditions and in the next screen select the Predicate List as User and click Next
    - In the User Argument Name type in BISystemUser and click ADD and then click on the button Finish
    - In the Role Conditions screen ensure that the set operator is set to 'Or'
    - Save the configuration
    - Navigate to the Enterprise Manager of OBIEE or the Fusion Middleware Control page and navigate in the tree structure to the node Business Intelligence -> coreapplication and in the menu Business Intelligence Menu drop down select Security -> Application Roles
    - In the Roles displayed select BISystem and in the next screen remove the old BISystemUser (from the Default Provider) and add the newly created BISystemUser user in OID
    - Next add the trusted user's credentials to the oracle.bi.system credential map
    - From Fusion Middleware Control target navigation pane, expand the farm, then expand WebLogic Domain, and select bifoundation_domain
        - From the WebLogic Domain menu, select Security, then Credentials
        - Open the oracle.bi.system credential map, select system.user and click Edit
        - In the Edit Key dialog, enter BISystemUser (or name you selected) in the User Name field. In the Password field, enter the trusted user's password that is contained in Oracle Internet Directory
        - Click OK
    - Restart the Managed Servers
15. Enabling SSO Authentication in the Weblogic Server for OBIEE:
    - Log in to Fusion Middleware Control (EM) of the WebLogic Server.
    - Navigate to the Business Intelligence Overview page.
    - Navigate to the Security page.
    - Click Lock and Edit Configuration.
    - Check Enable SSO this makes the SSO provider list becomes active.
    - Select the configured SSO provider from the list.
    - Click Apply, then Activate Changes.

- Manually edit each instanceconfig.xml file for every Oracle BI Presentation Services process to configure the login and logout information. Inside the <Authentication> section, add the following:

  <SchemaExtensions>

  <Schema name="SSO" logonURL="{your SSO logon URL}" logoffURL="{your logoff

  URL}/>

  </SchemaExtensions>

  For e.g.-

  <SchemaExtensions>

  <Schema name="SSO" logonURL="http://<machinename>.<port>
  /analytics/saw.dll?bieehome&startPage=1"
  logoffURL="http://<machinename>.<port>
  /access/oblix/lang/en-us/logout.html"/>

  </SchemaExtensions>

- Restart the Oracle Business Intelligence components using Fusion Middleware Control

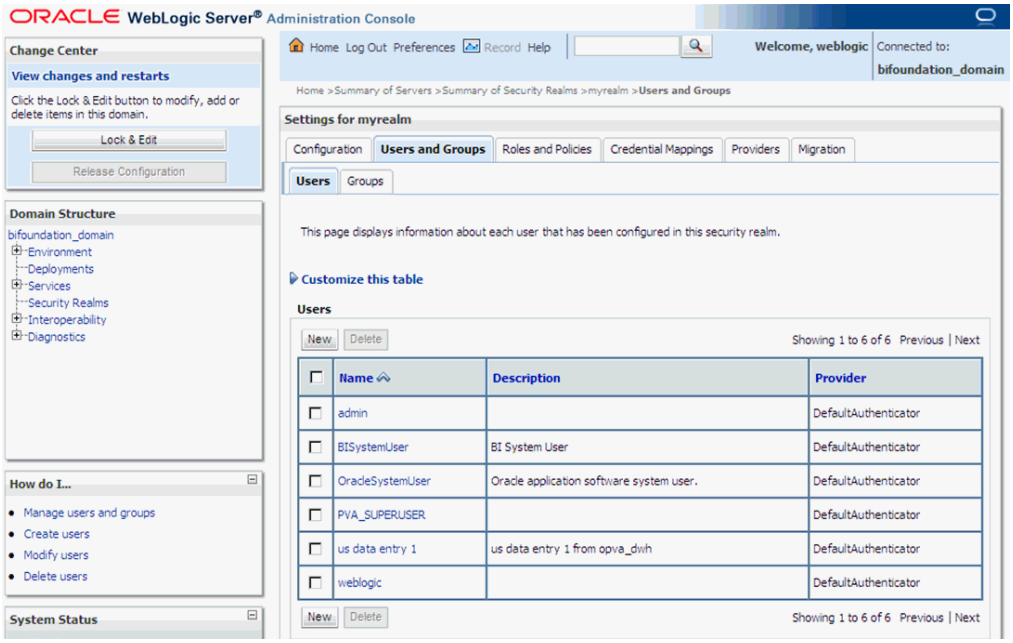
2.7 Creating Users and Groups in OPVA

2.7.1 Creating Groups for OPVA in WebLogic Server

Note: The following steps are applicable for creating users and groups if the embedded LDAP is used for maintaining the authentication for OPVA. If not using the embedded LDAP then these groups should be created in the external LDAP provider.

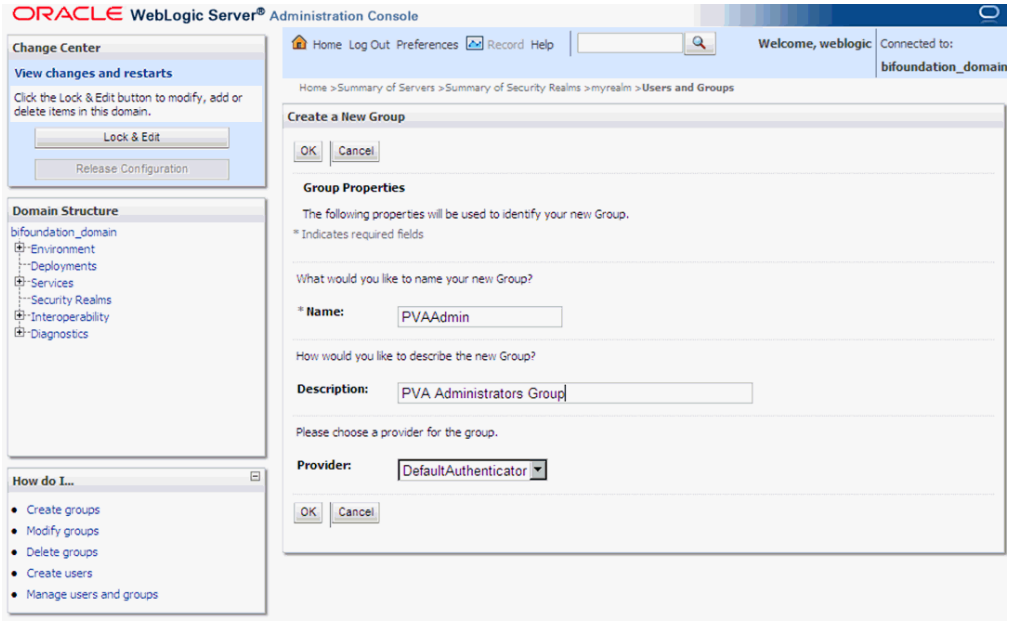
1. Open a new browser window for the WebLogic Administration Console.
2. Navigate to Security Realms -> myrealm -> Users and Groups tab.

Figure 2–28 myrealm Settings: Users and Groups tab



3. Select the Groups Tab and click on New.
4. Enter the group name as 'PVAAdmin' and click OK.

Figure 2–29 myrealm Settings: Groups tab: New Group



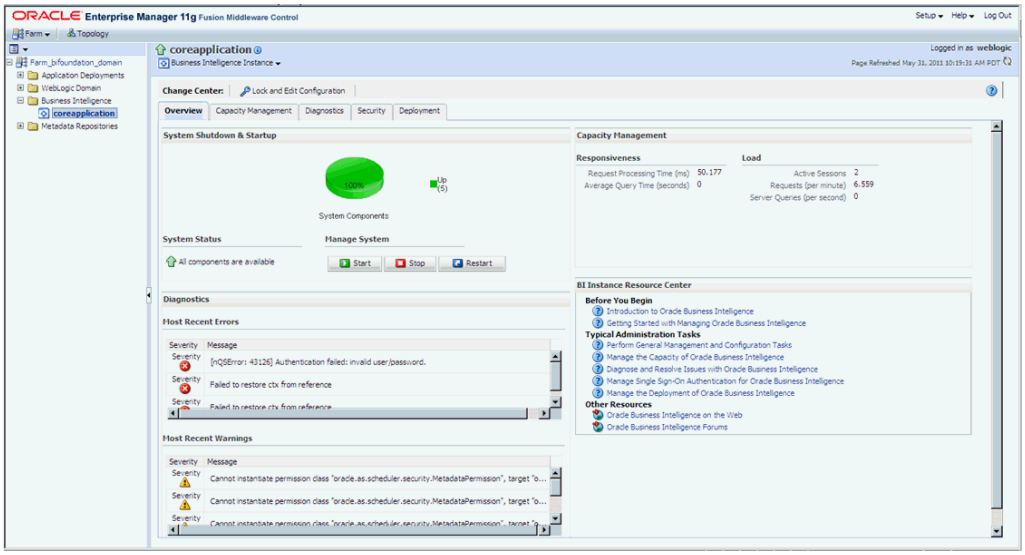
5. Follow the above process to create the groups 'PVASafetyGroup' and 'PVASafetyConsumersGroup'.

2.7.2 Assigning OBIEE Application Roles for OPVA Groups

Note: The below steps are applicable for the groups created in either the embedded LDAP or an external LDAP e.g. OID.

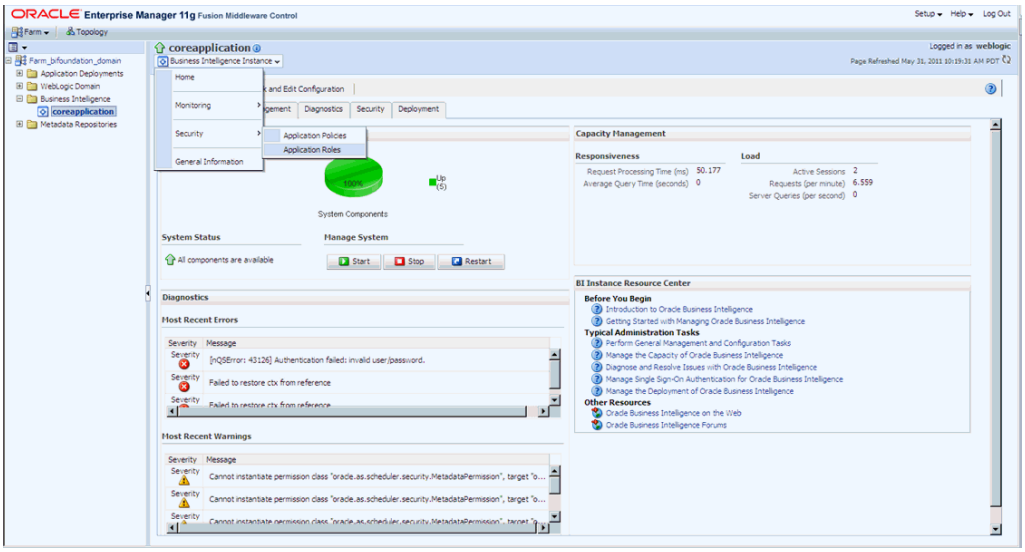
1. Start a new browser window for the Enterprise Manager for Fusion Middleware Control and navigate to the Business Intelligence -> coreapplication overview page as shown here:

Figure 2–30 coreapplication Screen



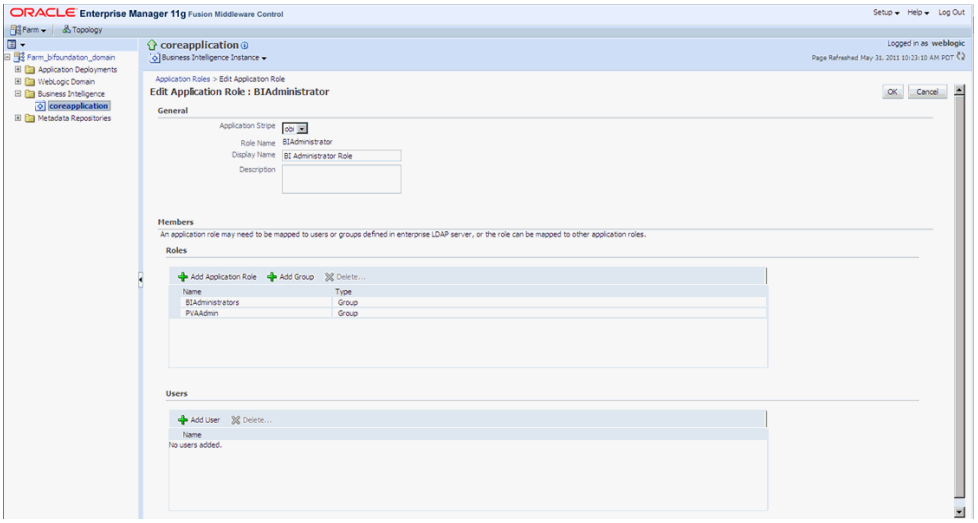
2. Invoke the Application Roles by choosing from the menu drop down at Business Intelligence Instance -> Security -> Application Roles

Figure 2–31 coreapplication: Application Roles Screen



3. Click on BIAdministrator application role and add the group PVAAdmin.

Figure 2–32 coreapplication: Add Group



4. Click OK.
5. Repeat the above steps to add the groups created as per the table given here:

Application Role	PVA Groups to be added
BIAdministrator	PVAAdmin
BIAuthor	PVAAdmin, PVASafetyGroup
BIConsumer	PVAAdmin, PVASafetyGroup, PVASafetyConsumersGroup

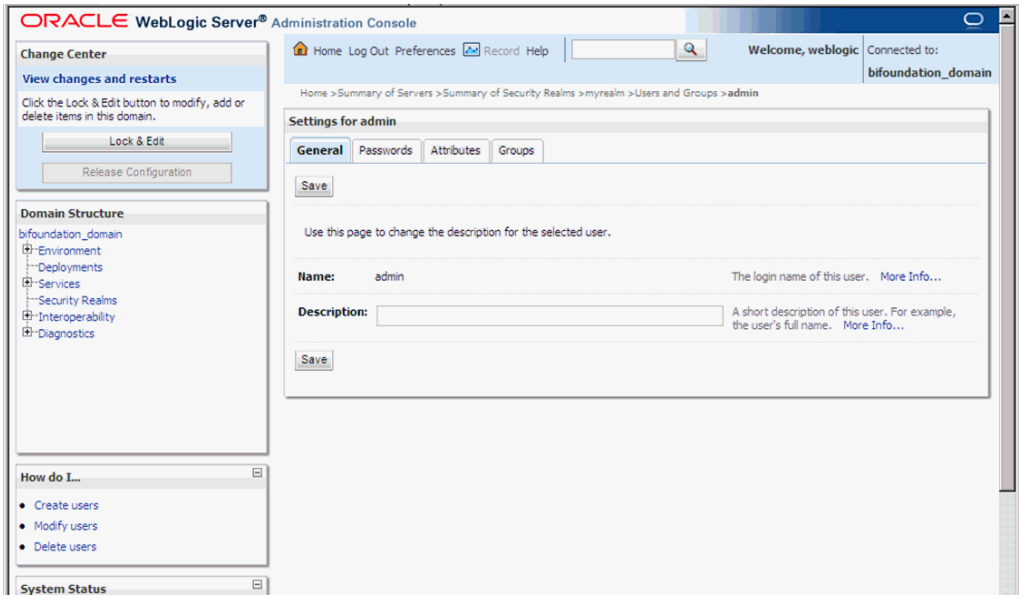
> **Note:** Refer to Appendix 2.9, OBIEE Default Application Roles for a list of privileges present as per the BIApplication Role specified above.

2.7.3 Creating Users for OPVA in WebLogic Server

> **Note:** The below steps are applicable for creating users and groups if the embedded LDAP is used for maintaining the authentication for OPVA. It is recommended to create at least one user to be added in the PVAAdmin group created above, to be used as a PVA Application administrator.

1. Start a new browser window for the WebLogic Administration Console.
2. Navigate to Security Realms -> myrealm -> Users and Groups tab.
3. Select the Users Tab and click on New.
4. Enter the User Name and Password details.
5. Click OK to save the User in the embedded LDAP.
6. This takes you back to the Users table display. Click on the User that you newly created to display the page as shown here:

Figure 2–33 Administration Console: General tab



7. Click on Groups tab and select the appropriate PVA Group you want the user to be added to and save the details.
8. Repeat the above steps to add users to the three groups (as created in the previous step).

2.7.4 Creating Users for DAC

1. Log in to the DAC Client as Administrator.
2. Click on the menu File -> User Management.
3. In the popped up window enter the following details.
   a. Name: Login Name for the user being created for DAC.
   b. Password: Password to authenticate the user being created.
   c. Roles: Select one of the these roles:
      - Administrator
      - Operator
      - Developer

      The following table lists the permissions available to each specific role.

Table 2–2 Creating Users for DAC

Role	Permissions
Administrator	Read and write permission on all DAC tabs and dialog boxes.

Table 2–2 (Cont.) Creating Users for DAC

Role	Permissions
Developer	Read and write permission on the following: -All Design view tabs -All Execute view tabs -Export dialog box -New Source System Container dialog box -Rename Source System Container dialog box -Delete Source System Container dialog box -Purge Run Details -All functionality in the Seed Data menu
Operator	Read and write permission on all Execute view tabs

d. Click on Save.

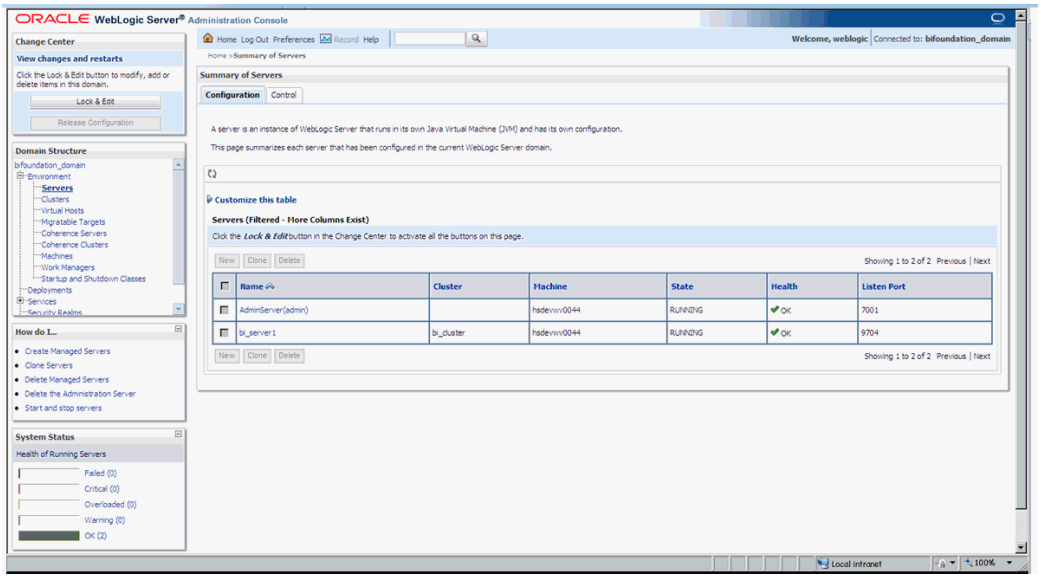
Note: It is recommended to create at least one user to be added with the Administrator Role in DAC to manage the DAC PVA metadata.

2.8 Configuring SSL for OPVA in OBIEE

To enable the default SSL configuration in OBIEE use the following steps:

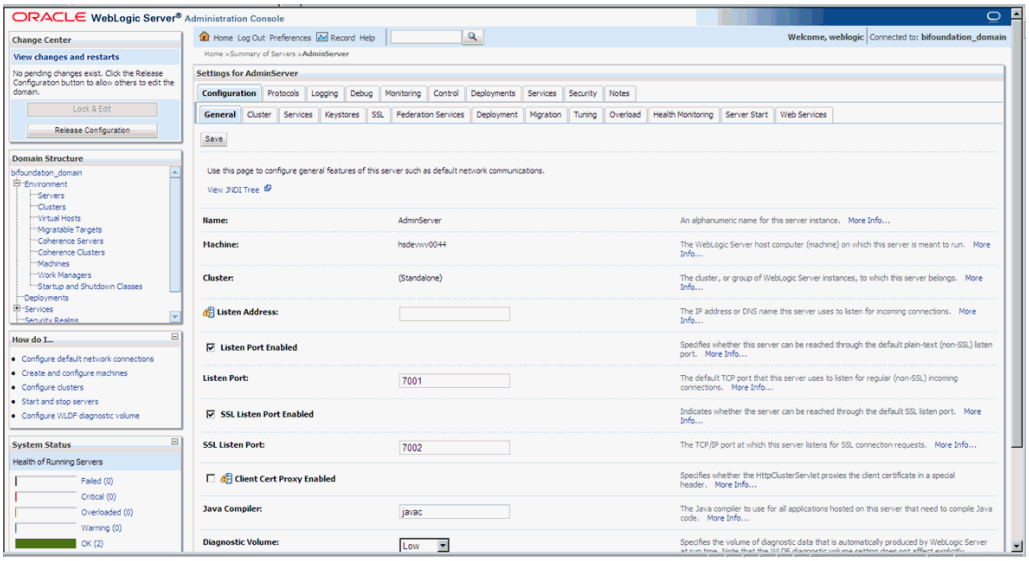
1. Open the WLS Administrator console for OBIEE.
2. Navigate to Environment -> Servers in the tree view displayed on the left side.

Figure 2–34 Servers: Configuration tab



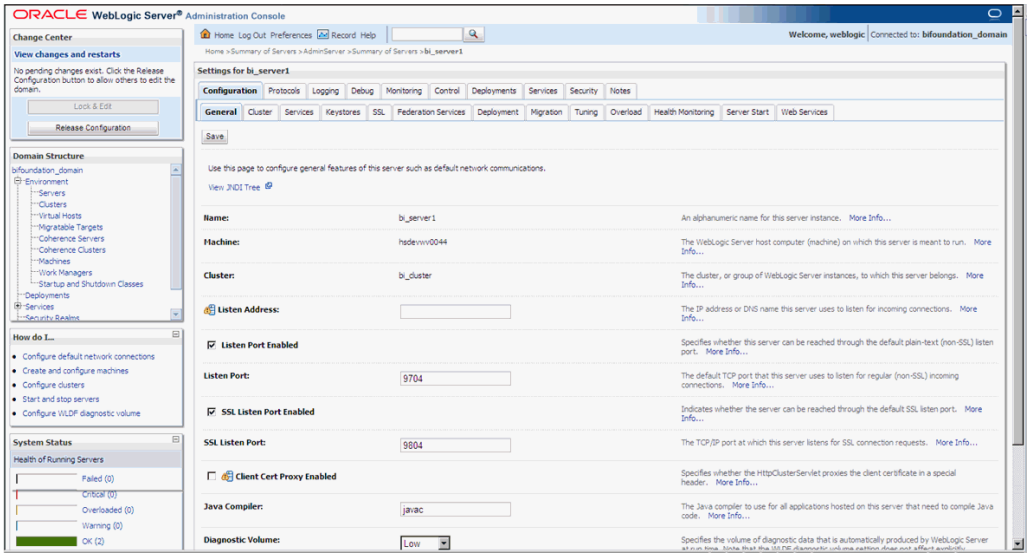
3. Click the Lock & Edit button to change the configuration.
4. Click the AdminServer(admin) link and in the General Tab, enable the SSL listen port, as displayed below:

Figure 2–35 Servers: Configuration tab: General sub-tab



5. Click Save.
6. In the Servers window, click bi_server1 (or the link for the OBIEE server configured).
7. Enable the SSL Listen Port for the OBIEE server as well.

Figure 2–36 General sub-tab: Enable the SSL Listen Port



8. Click on Save.
9. Edit the startWebLogic.cmd file present in the location

   <OracleBIHome>\user_projects\domains\bifoundation_domain\ and add the below entry to the file before the “call” statement.

   set JAVA_OPTIONS=%JAVA_OPTIONS%
   -Djavax.net.ssl.trustStore="D:/Oracle/Middleware/wlserver_
   10.3/server/lib/DemoTrust.jks" -Djavax.net.ssl.trustStorePassword=""

Note: Please edit the Path names according to your installation directories.

10. Restart all the Managed BI Servers.

Note: For more detailed information on configuring SSL certificates in OBIEE 11g, please refer to the guide - Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1) section - SSL Configuration in Oracle Business Intelligence.

2.9 OBIEE Default Application Roles

Component	Privilege	Description	Default Role Granted
Access	Access to Dashboards	Allows users to view dashboards.	BIConsumer
Access	Access to Answers	Allows users to access the basic features of the Analysis editor.	BIAuthor
Access	Access to Delivers	Allows users to create and edit agents.	BIAuthor
Access	Access to Briefing Books	Allows users to view and download briefing books.	BIConsumer
Access	Access to Administration	Allows users to access the Administration pages in Presentation Services,	BIAdministrator
Access	Access to Segments	Allows users to access segments in Oracle's Siebel Marketing.	BIConsumer
Access	Access to Segment Trees	Allows users to access segment trees in Oracle's Siebel Marketing.	BIAuthor
Access	Access to List Formats	Allows users to access list formats in Oracle's Siebel Marketing.	BIAuthor
Access	Access to Metadata Dictionary	Allows users to access the metadata dictionary information for subject areas, folders, columns, and levels.	BIAdministrator
Access	Access to Oracle BI for Microsoft Office	See Section C.2.3.3.2, "Access to Oracle BI for Microsoft Office Privilege."	BIConsumer
Access	Access to Conditions	Allows users to create conditions.	BIAuthor
Access	Access to KPI Builder	Allows users to create KPIs.	BIAuthor
Access	Access to Scorecard	Allows users access to Oracle BI Scorecard.	BIConsumer
Actions	Create Navigate Actions	See Section C.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions."	BIAuthor

Component	Privilege	Description	Default Role Granted
Actions	Create Invoke Actions	See Section C.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions."	BIAuthor
Actions	Save Actions Containing Embedded HTML	See Section C.2.3.3.1, "Access to Oracle BI Enterprise Edition Actions."	BIAdministrator
Admin: Catalog	Change Permissions	Allows users to modify permissions for catalog objects.	BIAuthor
Admin: Catalog	Toggle Maintenance Mode	Shows the Toggle Maintenance Mode link on the Presentation Services Administration page, which allows users to turn maintenance mode on and off. In maintenance mode, the catalog is read-only; no one can write to it.	BIAdministrator
Admin: General	Manage Sessions	Shows the Manage Sessions link on the Presentation Services Administration page, which displays the Manage Sessions page in which users manage sessions.	BIAdministrator
Admin: General	Manage Dashboards	Allows users to create and edit dashboards, including editing their properties.	BIAdministrator
Admin: General	See Session IDs	Allows users to see session IDs on the Manage Sessions page.	BIAdministrator
Admin: General	Issue SQL Directly	Shows the Issue SQL link on the Presentation Services Administration page, which displays the Issue SQL page in which users enter SQL statements.	BIAdministrator
Admin: General	View System Information	Allows users to view information about the system at the top of the Administration page in Presentation Services.	BIAdministrator
Admin: General	Performance Monitor	Allows users to monitor performance.	BIAdministrator
Admin: General	Manage Agent Sessions	Shows the Manage Agent Sessions link on the Presentation Services Administration page, which displays the Manage Agent Sessions page in which users manage agent sessions.	BIAdministrator
Admin: General	Manage Device Types	Shows the Manage Device Types link on the Presentation Services Administration page, which displays the Manage Device Types page in which users manage device types for agents.	BIAdministrator

Component	Privilege	Description	Default Role Granted
Admin: General	Manage Map Data	Shows the Manage Map Data link on the Presentation Services Administration page, which displays the Manage Map Data page in which users edit layers, background maps, and images for map views.	BIAdministrator
Admin: General	See Privileged Errors	Allows users to see privileged error messages. Users can see detailed error messages about database connections or other details when lower level components fail.	BIAdministrator
Admin: General	See SQL Issued in Errors	Allows users to see SQL statements that are returned by the BI Server in error messages.	BIConsumer
Admin: General	Manage Marketing Jobs	Shows the Manage Marketing Jobs link on the Presentation Services Administration page, which displays the Marketing Job Management page in which users manage marketing jobs.	BIAuthor
Admin: General	Manage Marketing Defaults	Shows the Manage Marketing Defaults link on the Presentation Services Administration page, which displays the Manage Marketing Defaults page in which users manage defaults for Oracle's Siebel Marketing application.	BIAdministrator
Admin: Security	Manage Catalog Groups	Shows the Manage Catalog Groups link on the Presentation Services Administration page, which displays the Manage Catalog Groups page in which users edit Catalog groups.	BIAdministrator
Admin: Security	Manage Privileges	Shows the Manage Privileges link on the Presentation Services Administration page, which displays the Manage Privileges page in which users manage the privileges that are described in this table.	BIAdministrator
Admin: Security	Set Ownership of Catalog Objects	Allows users to edit the ownership of objects in the catalog on the Catalog page.	BIAdministrator
Admin: Security	User Population - Can List Users	Allows users to see the list of users for which they can perform tasks such as assigning privileges and permissions.	BIConsumer, BISystem
Admin: Security	User Population - Can List Groups	Allows users to see the list of groups for which they can perform tasks such as assigning privileges and permissions.	BIConsumer, BISystem

Component	Privilege	Description	Default Role Granted
Briefing Book	Add To or Edit a Briefing Book	Allows users to see the Add to Briefing Book link on dashboard pages and analyses and the Edit link in briefing books.	BIAuthor
Briefing Book	Download Briefing Book	Allows users to download briefing books.	BIConsumer
Catalog	Personal Storage	Allows users to have write access to their own My Folders folders and can create content there. If users do not have this privilege, then they can receive email alerts but cannot receive dashboard alerts.	BIConsumer
Catalog	Reload Metadata	Allows users to click the **Reload Server Metadata** link from the Refresh menu in the toolbar of the Subject Areas pane.	BIAdministrator
Catalog	See Hidden Items	Allows users to see hidden items in catalog folders. Users can also select the **Show Hidden Items** box on the Catalog page.	BIAuthor
Catalog	Create Folders	Allows users to create folders in the catalog.	BIAuthor
Catalog	Archive Catalog	Allows users to archive the folders and objects in the catalog.	BIAdministrator
Catalog	Unarchive Catalog	Allows users to unarchive catalog objects that have been archived previously.	BIAdministrator
Catalog	Upload Files	Allows users to upload files into an existing catalog.	BIAdministrator
Conditions	Create Conditions	Allows users to create or edit named conditions.	BIAuthor
Dashboards	Save Customizations	See Section 19.5, "Controlling Access to Saved Customization Options in Dashboards."	BIConsumer
Dashboards	Assign Default Customizations	See Section 19.5, "Controlling Access to Saved Customization Options in Dashboards."	BIAuthor
Formatting	Save SystemWide Column Formats	Allows users to save systemwide defaults when specifying formats for columns.	BIAdministrator
My Account	Access to My Account	Allows users to access the My Account dialog.	BIConsumer
My Account	Change Preferences	Allows users to access the Preferences tab of the My Account dialog.	BIConsumer
My Account	Change Delivery Options	Allows users to access the Delivery Options tab of the My Account dialog.	BIConsumer
Answers	Create Views	Allows users to create views.	BIAuthor
Answers	Create Prompts	Allows users to create prompts.	BIAuthor

Component	Privilege	Description	Default Role Granted
Answers	Access Advanced Tab	Allows users to access the Advanced tab in the Analysis editor.	BIAuthor
Answers	Edit Column Formulas	Allows users to edit column formulas.	BIAuthor
Answers	Save Content with HTML Markup	Allows users to save objects such as views and actions that contain HTML code.	BIAdministrator
Answers	Enter XML and Logical SQL	Allows users to use the Advanced SQL tab.	BIAuthor
Answers	Edit Direct Database Analysis	Allows users to create and edit requests that are sent directly to the back-end data source.	BIAdministrator
Answers	Create Analysis from Simple SQL	Allows users to select the **Create Analysis from Simple SQL** option in the Select Subject Area list.	BIAdministrator
Answers	Create Advanced Filters and Set Operations	Allows users to click the **Combine results based on union, intersection, and difference operations** button from the Criteria tab in the Analysis editor.	BIAuthor
Answers	Save Filters	Allows users to save filters	BIAuthor
Answers	Execute Direct Database Analysis	Allows users to issue requests directly to the back-end data source.	BIAdministrator
Delivers	Create Agents	Allows users to create agents.	BIAuthor
Delivers	Publish Agents for Subscription	Allows users to publish agents for subscription.	BIAuthor
Delivers	Deliver Agents to Specific or Dynamically Determined Users	Allows users to deliver agents to other users.	BIAdministrator
Delivers	Chain Agents	Allows users to chain agents.	BIAuthor
Delivers	Modify Current Subscriptions for Agents	Allows users to modify the current subscriptions for agents, including unsubscribing users.	BIAdministrator
Proxy	Act As Proxy	Allows users to act as proxy users for other users, as described in Section C.5, "Enabling Users to Act for Others."	Denied: BIConsumer
RSS Feeds	Access to RSS Feeds	Allows users to subscribe to and receive RSS feeds with alerts and contents of folders. If Presentation Services uses the HTTPS protocol, then the RSS Reader that you use must also support the HTTPS protocol.	BIAuthor
Scorecard	Create/Edit Scorecards	Allows users to create and edit scorecards.	BIAuthor

Component	Privilege	Description	Default Role Granted
Scorecard	View Scorecards	Allows users to view scorecards.	BIConsumer
Scorecard	Create/Edit Objectives	Allows users to create and edit objectives.	BIAuthor
Scorecard	Create/Edit Initiatives	Allows users to create and edit initiatives.	BIAuthor
Scorecard	Create Views	Allows users to create and edit scorecard views, such as strategy trees.	BIAuthor
Scorecard	Create/Edit Causes and Effects Linkages	Allows users to create and edit cause and effect relationships.	BIAuthor
Scorecard	Create/Edit Perspectives	Allows users to create and edit perspectives.	BIAdministrator
Scorecard	Add Annotations	Allows users to add comments to KPIs and scorecard components.	BIConsumer
Scorecard	Override Status	Allows users to override statuses of KPIs and scorecard components.	BIConsumer
Scorecard	Create/Edit KPIs	Allows users to create and edit KPIs.	BIAuthor
Scorecard	Add Scorecard Views to Dashboards	Allows users to add scorecard views (such as strategy trees) to dashboards.	BIConsumer
List Formats	Create List Formats	Allows users to create list formats in Oracle's Siebel Marketing.	BIAuthor
List Formats	Create Headers and Footers	Allows users to create headers and footers for list formats in Oracle's Siebel Marketing.	BIAuthor
List Formats	Access Options Tab	Allows users to access the Options tab for list formats in Oracle's Siebel Marketing.	BIAuthor
List Formats	Add/Remove List Format Columns	Allows users to add and remove columns for list formats in Oracle's Siebel Marketing.	BIAdministrator
Segmentation	Create Segments	Allows users to create segments in Oracle's Siebel Marketing.	BIAuthor
Segmentation	Create Segment Trees	Allows users to create segment trees in Oracle's Siebel Marketing.	BIAuthor
Segmentation	Create/Purge Saved Result Sets	Allows users to create and purge saved result sets in Oracle's Siebel Marketing.	BIAdministrator
Segmentation	Access Segment Advanced Options Tab	Allows users to access the Segment Advanced Options tab in Oracle's Siebel Marketing.	BIAdministrator
Segmentation	Access Segment Tree Advanced Options Tab	Allows users to access the Segment Tree Advanced Options tab in Oracle's Siebel Marketing.	BIAdministrator

Component	Privilege	Description	Default Role Granted
Segmentation	Change Target Levels within Segment Designer	Allows users to change target levels within the Segment Designer in Oracle's Siebel Marketing.	BIAdministrator
SOAP	Access SOAP	Allows users to access various web services.	BIConsumer, BISystem
SOAP	Impersonate as System User	Allows users to impersonate a system user using a web service.	BISystem
SOAP	Access MetadataService	Allows users to access the MetadataService web service.	BIConsumer, BISystem
SOAP	Access AnalysisExportViews Service	Allows users to access the ReportingEditingService web service.	BIConsumer
SOAP	Access ReportingEditingService	Allows users to access the ReportingEditingService web service.	BIConsumer, BISystem
SOAP	Access ConditionEvaluation Service	Allows users to access the ConditionEvaluationService web service.	BIConsumer, BISystem
SOAP	Access ReplicationService	Allows users to access the ReplicationService web service to replicate the Oracle BI Presentation Catalog.	BISystem
SOAP	Access CatalogIndexingService	Allows users to access the CatalogIndexingService web service to index the Oracle BI Presentation Catalog for use with full-text search.	BISystem
SOAP	Access DashboardService	Allows users to access the DashboardService web service.	BIConsumer, BISystem
SOAP	Access SecurityService	Allows users to access the SecurityService web service.	BIConsumer, BISystem
SOAP	Access ScorecardMetadataService	Allows users to access the ScorecardMetadataService web service.	BIConsumer, BISystem
SOAP	Access ScorecardAssessment Service	Allows users to access the ScorecardAssessmentService web service.	BIConsumer, BISystem
SOAP	Access HtmlViewService	Allows users to access the HtmlViewServiceService web service.	BIConsumer, BISystem
SOAP	Access CatalogService	Allows users to access the CatalogService web service.	BIConsumer, BISystem
SOAP	Access IBotService	Allows users to access the IBotService web service.	BIConsumer, BISystem
SOAP	Access XmlGenerationService	Allows users to access the XmlGenerationService web service.	BIConsumer, BISystem
SOAP	Access JobManagementService Service	Allows users to access the JobManagementService web service.	BIConsumer, BISystem

Component	Privilege	Description	Default Role Granted
SOAP	Access KPIAssessmentServic e	Allows users to access the JKPIAssessmentService web service.	BIConsumer, BISystem
Subject Area (*by its name*)	Access within Oracle BI Answers	Allows users to access the specified subject area within the Answers editor.	BIAuthor
View Analyzer	Add/Edit AnalyzerView	Allows users to access the Analyzer view.	BIAdministrator
View Column Selector	Add/Edit Column SelectorView	Allows users to create and edit column selector views.	BIAuthor
View Compound	Add/Edit CompoundView	Allows users to create and edit compound layouts.	BIAuthor
View Graph	Add/Edit GraphView	Allows users to create and edit graph views.	BIAdministrator
View Funnel	Add/Edit FunnelView	Allows users to create and edit funnel graph views.	BIAuthor
View Gauge	Add/Edit GaugeView	Allows users to create and edit gauge views.	BIAuthor
View Filters	Add/Edit FiltersView	Allows users to create and edit filters.	BIAuthor
View Dashboard Prompt	Add/Edit Dashboard PromptView	Allows users to create and edit dashboard prompts.	BIAuthor
View Static Text	Add/Edit Static TextView	Allows users to create and edit static text views.	BIAuthor
View Legend	Add/Edit Legend View	Allows users to create and edit legend views.	BIAuthor
View Map	Add/Edit MapView	Allows users to create and edit map views.	BIAuthor
View Narrative	Add/Edit NarrativeView	Allows users to create and edit narrative views.	BIAuthor
View Nested Request	Add/Edit Nested RequestView	Allows users to create and edit nested analyses.	BIAuthor
View No Results	Add/Edit No ResultsView	Allows users to create and edit no result views.	BIAuthor
View Pivot Table	Add/Edit Pivot TableView	Allows users to create and edit pivot table views.	BIAuthor
View Report Prompt	Add/Edit Report PromptView	Allows users to create and edit prompts.	BIAuthor
View Create Segment	Add/Edit Create SegmentView	Allows users to create and edit segment views.	BIAuthor
View Logical SQL	Add/Edit Logical SQLView	Allows users to create and edit logical SQL views.	BIAuthor
View Table	Add/Edit TableView	Allows users to create and edit table views.	BIAuthor
View Create Target List	Add/Edit Create Target ListView	Allows users to create and edit target list views.	BIAuthor
View Ticker	Add/Edit TickerView	Allows users to create and edit ticker views.	BIAuthor

Component	Privilege	Description	Default Role Granted
View Title	Add/Edit TitleView	Allows users to create and edit title views.	BIAuthor
View View Selector	Add/Edit View SelectorView	Allows users to create and edit view selector views.	BIAuthor
Write Back	Write Back to Database	Grants the right to write data into the data source.	Denied: BIConsumer
Write Back	Manage Write Back	Grants the right to manage write back requests.	BIAdministrator