Oracle® Argus Analytics

Installation Guide

Release 1.1.1

E38197-01

February 2013

ORACLE®

Oracle Argus Analytics Installation Guide, Release 1.1.1

E38197-01

Contents

Preface v

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

Part I Installing Oracle Argus Analytics

1 Oracle Argus Analytics 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 1-3
1.1.1.3 Supported Sources 1-4
1.1.1.4 Technology Stack Matrix 1-4
1.1.1.5 Typical Hardware Architecture 1-5
1.1.1.6 Installation Process Overview 1-7
1.1.2 Pre-requisites 1-7
1.1.2.1 Client Tools 1-8

2 Installing Oracle Argus Analytics

2.1 Preinstallation Configuration 2-2
2.1.1 Configuring ETL Clients 2-3
2.1.1.1 Informatica 2-4
2.1.1.2 ODI Studio 2-4
2.2 Running the Oracle Argus Analytics Installer 2-7
2.3 Preparing the DAC Repository (Informatica Only) 2-13
2.4 ODI Smart Import and Topology Configuration (ODI only) 2-17
2.4.1 ODI Smart Import 2-17
2.4.2 Configuring the Topology in ODI Studio 2-19
2.4.3 Configuring the Standalone ODI Agent 2-20
2.4.4 Deploying and Configuring the ODI Java EE agent on the existing WebLogic Domain . 2-22

2.5 Configuring the OBIEE Repository and Webcatalog 2-26
2.5.1 Prerequisites 2-26
2.5.1.1 Upgrading the AN 1.1 RPD and Catalog (Upgrade Install Only) 2-26
2.5.2 Deployment of OBIEE Repository and Catalog 2-28
2.5.2.1 Post-deployment of the Oracle Argus Analytics RPD 2-33
2.5.3 Changing the OBIEE RPD Password 2-33
2.6 Configuring the OBIEE Help files 2-33
2.6.1 Configuring the Help links in the Dashboards and Reports 2-34
2.7 Configuring SSO Using Oracle Access Manager 10g 2-37
2.8 Configuring SSO Using Oracle Access Manager 11g 2-53
2.9 Configuring SSL for Oracle Argus Analytics in OBIEE 2-65
2.10 Configuring SSL for SSO in Oracle Argus Analytics with OAM 11g 2-67
2.11 Creating Users and Groups in Oracle Argus Analytics 2-69
2.11.1 Creating Groups for Oracle Argus Analytics in WebLogic Server 2-69
2.11.2 Assigning OBIEE Application Roles for Oracle Argus Analytics Groups 2-71
2.11.3 Creating Users for Oracle Argus Analytics in WebLogic Server 2-72
2.11.4 Creating Users for DAC 2-75
2.12 Configuring SSL for Oracle Argus Analytics in OBIEE 2-75
2.13 OBIEE Default Application Roles 2-77

Part II Appendix

A Managing Catalog Permissions and Privileges

A.1 Creating Users and Groups A-1
A.2 Creating Application Roles and Assigning User Groups to Roles A-1
A.3 Maintaining Catalog Privileges A-5
A.4 Managing Permissions for Catalog Folders and Requests A-8
A.4.1 Creating a New Catalog Folder under Shared Folders A-8
A.4.2 Managing Permissions for Catalog Folders or Saved Requests A-9

Preface

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

Oracle Argus Analytics was previously named Oracle Health Sciences Pharmacovigilance Operational Analytics (OPVA).

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

Audience

Installing Oracle Argus Analytics 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 Argus 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 Data Integrator
- Installation and maintenance of Oracle Business Intelligence Enterprise Edition 11g
- Installation and maintenance of Oracle Data Warehouse Administration Console 11g
- Installation and maintenance of Oracle Access Manager 10g/11g
- 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 Argus 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 Oracle Argus Analytics Standard Configuration Media Pack

The Oracle Argus Analytics 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 Oracle Argus Analytics application. To receive the physical media, order it from Oracle Store at https://oraclestore.oracle.com.

To download the Oracle Argus Analytics 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 Argus 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 Argus 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)
- *Oracle Fusion Middleware Installation Guide for Oracle Data Integrator 11g Release 1 (11.1.1)* (E16543-03)

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.

Part I

Installing Oracle Argus Analytics

This part of the Oracle Argus Analytics Installation Guide describes how to install Oracle Argus Analytics.

Part I contains the following chapters:

- Chapter 1, Oracle Argus Analytics Requirements
- Chapter 2, Installing Oracle Argus Analytics

1

Oracle Argus Analytics Requirements

1.1 Requirements

This section presents an overview of the Oracle Argus Analytics 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 Oracle Argus Analytics 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 Oracle Argus Analytics Database Server

Oracle Argus Analytics is certified for Oracle Database Enterprise Edition 11.2.0.3. It supports Oracle Database Enterprise Edition 11.2.0.1 as well.

Supported Operating System

- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle Solaris 10 (64 Bit)
- Oracle Solaris 11
- 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 Oracle Argus Analytics ETL Server

This section comprises the following sub-sections:

1.1.1.1.3 Oracle Argus Analytics Informatica Server

Oracle Argus Analytics is certified against Informatica PowerCenter 9.0.1 with Hotfix2. Refer to the Informatica PowerCenter Installation Guide for recommended hardware and supported platforms.

Oracle Argus Analytics has got certified with the following:

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

1.1.1.1.4 Oracle Data Integrator (ODI) Server

Oracle Argus Analytics is certified against Oracle Data Integrator 11.1.1.6.3. Refer to the ODI Installation Guide for recommended hardware and supported platforms.

Oracle Argus Analytics has got certified with the following:

- Operating System: Microsoft Windows (32 bit), Oracle Solaris 10 (64 Bit), Oracle Solaris 11
- Memory: At least 8 GB RAM. HDD – at least 250 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.5 Oracle Argus Analytics OBIEE Server Oracle Argus Analytics is certified against Oracle Business Intelligence Enterprise Edition 11.1.1.6.5. Refer to the installation manual of OBIEE for further hardware and software requirements Oracle Argus Analytics 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 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.

- Oracle Solaris 11
- Memory: RAM at least 8 GB, HDD – at least 250 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.6 Oracle Argus Analytics Data Warehouse Administration Console Server Oracle Argus Analytics requires Oracle Data Warehouse Administration Console Server 10.1.3.4 with patch 13551596.

Supported Operating System

- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle 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

- Oracle Argus Analytics requires Oracle database client to connect to the database server. The supported client software version is 11.2.0.1 and 11.2.0.3.
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32 bit)

1.1.1.2.2 Oracle Data Warehouse Administration Console Client

- Oracle Data Warehouse Administration Console Client is required only when Informatica PowerCenter is used as an ETL Tool
- Oracle Argus Analytics requires Oracle Data Warehouse Administration Console Client 10.1.3.4 with patch 13551596
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32 bit)

1.1.1.2.3 ETL Client

This section comprises the following sub-sections:

1.1.1.2.4 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)

1.1.1.2.5 ODI Studio

- An ODI Studio 11.1.1.6.3 is required to connect to the ODI Repository.
- Supported Operating System: Microsoft Windows Server 2008 R1 with P1 or above (32 bit). You can also refer to this link for supported platforms:

  http://www.oracle.com/technetwork/middleware/data-integrator/odi-11gr1certmatrix-163773.xls

1.1.1.2.6 OBIEE Admin Tool

- OBIEE Admin tool 11.1.1.6.5 must be installed for configuring the repository file (RPD).
- Supported Operating System: Microsoft Windows Server 2008 R1 with SP1 or above (32/64 bit)

1.1.1.2.7 Optional Security Component

You can also configure Single Sign On Support for your reports and dashboards using Oracle Access Manager 10.1.4 or 11g. For more information regarding the Oracle

Access Manager installation and supported platforms, please refer the *Oracle Access Manager Installation Guide*.

1.1.1.2.8 Miscellaneous Components

- For running the reports and dashboards, your machine should have the Adobe Flash Player 10 or above installed.
- Although OBIEE 11.1.1.6.5 reports are supported in Microsoft Internet Explorer, Firefox and Safari, Oracle Argus Analytics is certified only for Microsoft Internet Explorer 7.0, 8.0, and 9.0 only.

1.1.1.3 Supported Sources

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

- Oracle Argus Safety 7.0.2
- Oracle Argus Safety 6.0.5.2

Customers can add customer data sources to the application by adding their own ETL. For more information about customizing Oracle Argus Analytics, please refer to the Oracle Argus 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 Oracle Argus Analytics.

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
Operating System	Windows Server 2008 with SP1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux X86 Version 5 or above (32/64 Bit) Oracle Solaris 10 (64 Bit) Oracle Solaris 11	Windows Server 2008 with SP1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux X86 Version 5 or above (32/64 Bit) Oracle Enterprise Linux with UEK 6.1 (32/64 bit) Oracle Solaris 10 (64 Bit) Oracle Solaris 11	Windows Server 2008 with SP1 or above (32/64 Bit) Windows Server 2008 R2 (64 Bit) Oracle Enterprise Linux X86 Version 5 or above (32/64 Bit) Oracle Solaris 10 (64 Bit)	Windows Server 2008 with SP2+ (32/64 bit) Windows Server 2008 R2 (all SP levels included) Windows 7 (all SP levels included) Oracle Linux 5 (UL5+) or above (32/64 bit) Red Hat EL5 (UL5+) or above (32/64 bit) Oracle Solaris 10 (64 Bit) Oracle Solaris 11	Windows XP Pro SP3 Windows 7 Apple iOS (for Oracle BI Mobile App)
Oracle Database	11.2.0.3 Client 11.2.0.1 Client	11.2.0.3 (Enterprise) - AL32UTF8 character set 11.2.0.1 (Enterprise) - AL32UTF8 character set			

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
OBIEE	OBIEE 11.1.1.6.5				
Informatica	Informatica Server 9.0.1 HF2		Informatica Server 9.0.1 HF2		
DAC	DAC Server 10.1.3.4.1 + Patch 13551596		DAC Server 10.1.3.4.1 + Patch 13551596		
Browser	IE 7.0 or				IE 7.0 or
	IE 8.0 or				IE 8.0 or
	IE 9.0				IE 9.0
Adobe Reader	Reader 9.0.3, 10.0.1				Reader 9.0.3, 10.0.1
Single Sign On Solution (Optional)	Oracle Access Manager 10.1.4/11g				
Resolution					Minimal Resolution 1280x1024

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

1.1.1.4.1 Supported Security Configuration Oracle Argus Analytics supports the following optional security configurations:

- LDAP/LDAPS 3.0
- Single Sign On Solution through Oracle Access Manager 10.1.4/11g

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

1.1.1.5 Typical Hardware Architecture

A typical Oracle Argus Analytics installation contains the following hardware architecture:

- Servers:
  - An Oracle Database server with Oracle Database 11.2.0.3/11.2.0.1
  - ETL Server
    * Informatica: Informatica PowerCenter 9.0.1 with Hotfix 2 Server + DAC Server 10.1.3.4 with patch 13551596

    OR

    * ODI Studio 11.1.1.6.3

- An OBIEE 11.1.1.6.5 Server

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

- Clients:
  - ETL Clients
    * Informatica PowerCenter Client 9.0.1 + Hotfix 2

    OR

    * ODI Studio 11.1.1.6.3
  - Oracle Database Client 11.2.0.3/11.2.0.1
  - DAC Client 10.1.3.4 with patch 13551596
  - OBIEE 11.1.1.6.5 Admin tool

Note: All tools can be installed in a single Microsoft Windows 32 bit box.

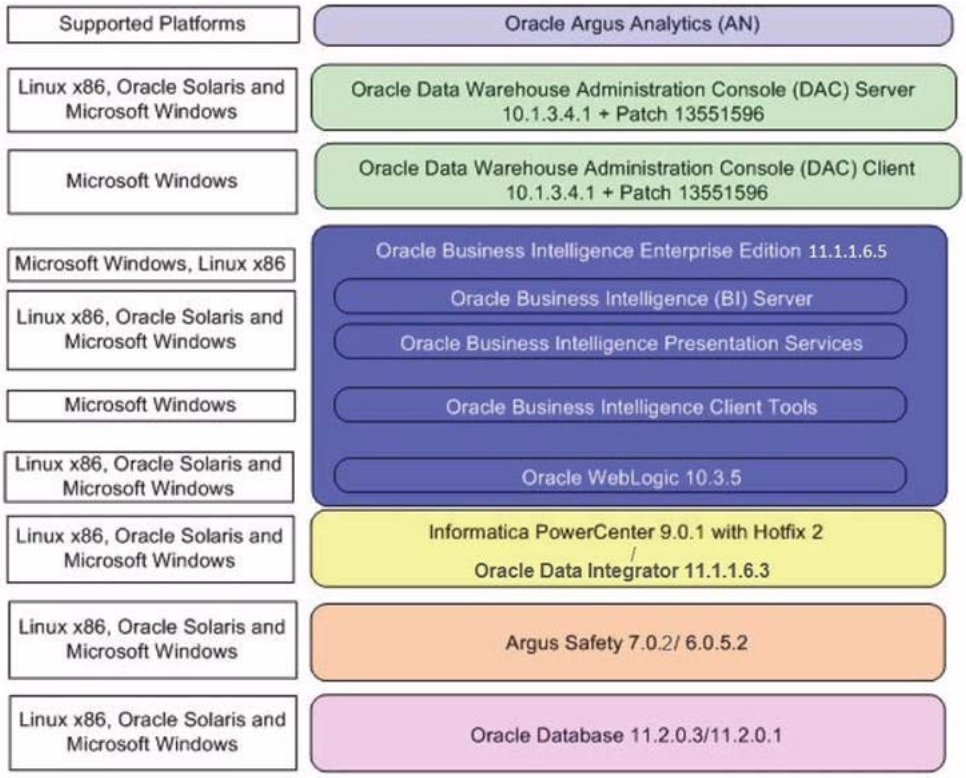
If the OBIEE server mentioned under the "Servers" section is a Windows 32 bit server, then all the clients can be installed in the same box itself.

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 Oracle Argus Analytics installer to run, if installation choice for ETL server is chosen as Informatica.

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

Figure 1–1 Oracle Argus 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, "Pre-requisites".
- Execute the installer – to create the data mart and Informatica ETLs.
- Follow the post-installation steps to configure DAC/ODI and OBIEE

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

1.1.2 Pre-requisites

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

- Oracle Database Server – An Oracle 11.2.0.3/11.2.0.1 database server should be created before Oracle Argus Analytics installation. Follow the platform-specific Database Installation Guide for installing this server.

  Note: The database server should be configured with AL32UTF8 character set.

- ETL Server Choice

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

Note:

- Informatica Server needs a repository database. Customers can either use the database created in the previous step or can create a new database for holding the repository.
  A **Versioned PowerCenter Repository** should be created upon the installation of PowerCenter. This versioned repository information will be needed during Oracle Argus Analytics installation along with the admin user credentials.
- An Oracle 11.2.0.3/11.2.0.1 Client should be available in the Informatica Server.

- DAC Server (Required only for Informatica ETL Server) – An Oracle Data Warehouse Administration Console Server of version 10.1.3.4 with patch 13551596 needs to be installed on the same machine where Informatica client is loaded. Follow platform-specific *ODAC Installation Guide* for installation instructions.

  OR

- Oracle Data Integrator - ODI Studio 11.1.1.6.3 should be installed on the server machine where ETLs have to be configured.

Note: ODI Server needs Master and Work Repository Database, which can be created on the same DWH DB Server created above.

- OBIEE Server - An Oracle Business Intelligence Enterprise Edition 11.1.1.6.5 Server must be installed before the Oracle Argus Analytics Installation. Follow platform-specific OBIEE Installation Guide for installation instructions.

1.1.2.1 Client Tools

- ETL Client Tools
- 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.
- DAC Client - A DAC Client 10.1.3.4.1 with patch 13551596 needs to be present. Supported only on a Microsoft Windows Server 2008 with SP1 or above (32 bit).

  OR

- ODI Studio installation mentioned in the sever section above can be used as an ETL client to administer/manage ETL metadata.
- Oracle Database Client - An Oracle 11.2.0.3/11.2.0.1 database client should be present. This should be present in the same machine where the Informatica PowerCenter client is loaded.

Note:

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

2

Installing Oracle Argus Analytics

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

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

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

- Preinstallation Configuration
- Running the Oracle Argus Analytics Installer
- Preparing the DAC Repository (Informatica Only)
- ODI Smart Import and Topology Configuration (ODI only)
- Configuring the OBIEE Repository and Webcatalog
- Configuring the OBIEE Help files
- Configuring SSO Using Oracle Access Manager 10g
- Configuring SSO Using Oracle Access Manager 11g
- Configuring SSL for Oracle Argus Analytics in OBIEE
- Configuring SSL for SSO in Oracle Argus Analytics with OAM 11g
- Creating Users and Groups in Oracle Argus Analytics
- Configuring SSL for Oracle Argus Analytics in OBIEE
- OBIEE Default Application Roles

Note: To connect to SQLPLUS, execute the following steps:

1. Open a command window in Windows. Alternatively, in Unix, type at the shell prompt.
2. Enter the sqlplus <dbuser>@<tnsnames_entry> command and press Enter.
3. Enter the password when prompted by the SQLPLUS program.

   You must not enter the password in the same command line that is used while calling the SQLPLUS program.

2.1 Preinstallation Configuration

Prior to running the Oracle Argus Analytics Installer, the following tasks must be completed:

1. The TNS entries for both the Data Mart Schema and the Argus Safety Database Schema should be present in the OBIEE 11g home in the path:

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

2. Configuring the TNS for Oracle Client:

   The TNS names entry for both Argus Analytics data mart and the Argus Safety Source system should be configured here:

   <Oracle Client Home>\network\admin\tnsnames.ora

3. Configuring the TNS for Oracle DB Servers:

   The TNS names entry for both Argus Analytics data mart and the Argus Safety Source system should be configured here:

   Argus Safety DB Server:

   <Oracle Client Home>\network\admin\tnsnames.ora

   This should contain the TNS entry for AN Data DB Server.

   Argus Safety DB Server:

   <Oracle DB Home>\network\admin\tnsnames.ora

   This should contain the TNS entry for Argus Safety DB Server.

4. Set up the Oracle Client Home in the PATH variable.
5. Setting up the SYSTEM user:

   The System user should be given grants to create view over the V_$SESSION view and execute privilege with grant option on DBMS_RLS in case of a multi-tenant system, in order to run the installer.

   Connect as SYS on both the Argus Safety DB instance and the Argus Analytics Data Mart DB instance and execute this script:

   GRANT SELECT ON V_$SESSION TO SYSTEM WITH GRANT OPTION;

   GRANT EXECUTE ON DBMS_RLS TO SYSTEM WITH GRANT OPTION;

Note: Once the installation is complete, this grant can be revoked from the user system.

The **NLS_LENGTH_SEMANTICS** DB parameter must be in CHAR mode. To verify this, connect as the **sys** user and execute the following statement in SQLPLUS on the Argus Analytics DB Instance only:

SHOW PARAMETER NLS_LENGTH_SEMANTICS

The value should show as CHAR, else execute the following statements in the same SQLPLUS window followed by a restart of the Argus Analytics DB Instance:

ALTER SYSTEM SET NLS_LENGTH_SEMANTICS=CHAR SCOPE=BOTH;

SHUTDOWN IMMEDIATE;

STARTUP;

Once the Argus Analytics DB Instance has been restarted, verify this parameter again to check if the value of CHAR has been set accordingly.

6. Setting up the TABLESPACES:

   The installer creates new schemas in the data mart 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 that get created in both the Argus Analytics DB Instance and the Argus Safety DB Instance.

   Example:

   Default TABLESPACE [one each needed at the AN DWH DB Server and Argus Safety DB Server]:

   CREATE TABLESPACE AN_DATA_TS

   DATAFILE ' AN_DATA_TS_01.dbf'

   SIZE 100M

   NEXT 1M

   LOGGING

   AUTO EXTEND ON;

   Example:

   Temporary TABLESPACE [one each needed at the AN DWH DB Server and Argus Safety DB Server]:

   CREATE TEMPORARY TABLESPACE AN_TEMP_TS

   TEMPFILE 'AN_TEMP_TS_01.dbf'

   SIZE 100M

   NEXT 1M

   AUTO EXTEND ON;

7. Follow the steps mentioned in the Configuring ETL Clients section below, and configure ETL Clients.

2.1.1 Configuring ETL Clients

This section lists steps to configure ETL Client on Informatica and ODI.

You need to configure ETL Client on either on of the two, as required.

2.1.1.1 Informatica

Follow the steps given below to configure ETL Client on Informatica:

1. The TNS entries for both the Data Mart Schema and the Argus Safety database Schema should be present in the Informatica Server as well so that the ETLs can pick data from the Argus Safety Database and populate the same in the PVA Warehouse.
2. 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.

   One can create the entry in the domains.infa file by configuring the Informatica Domain used for Argus Analytics in the Informatica Powercenter Repository Manager by navigating through the Repository > Configure Domains menu.
3. 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;...
4. Setting up the DAC Client:

   The DAC Client should be set configured to connect to the DAC Server.

Alternately, you may have to configure ETL Client on ODI.

2.1.1.2 ODI Studio

Follow the steps given below to configure ETL Client on ODI:

Creating DB Schemas for ODI Master and Work Repositories:

1. Connect to the DB Instance via "SQLPLUS" where you want to create the schemas (the AN DWH Data server can be used as well).
2. Create a schema to host the Master Repository and a schema to host the Work Repository for Argus Analytics as mentioned below:

ODI Master Repository:

CREATE USER **<AN_ODI_MASTER>** IDENTIFIED BY **<AN_ODI_MASTER_PASS>**

DEFAULT TABLESPACE **<MY_TBS>**

TEMPORARY TABLESPACE **<MY_TEMP>;**

GRANT CONNECT, RESOURCE TO **<AN_ODI_MASTER>**;

ODI Work Repository:

CREATE USER **<AN_ODI_WORK>** IDENTIFIED BY **<AN_ODI_WORK_PASS>**

DEFAULT TABLESPACE **<MY_TBS>**

TEMPORARY TABLESPACE **<MY_TEMP>;**

GRANT CONNECT, RESOURCE TO **<AN_ODI_WORK>**;

GRANT EXECUTE ON DBMS_LOCK TO **<AN_ODI_WORK>**;

ODI DBA User:

CREATE USER **<AN_ODI_DBA>** IDENTIFIED BY **<AN_ODI_DBA_PASS>**

DEFAULT TABLESPACE **<MY_TBS>**

TEMPORARY TABLESPACE **<MY_TEMP>;**

GRANT CONNECT, RESOURCE, DBA TO **<AN_ODI_DBA>**;

> **Note:** The Work Repository database user requires the grant execute privilege on DBMS_LOCK. Otherwise, Load Plans in ODI will not execute.

Legend:

<AN_ODI_MASTER>: ODI Master Repository Schema User name

<AN_ODI_MASTER_PASS>: ODI Master Repository Schema password

<AN_ODI_WORK>: ODI Work Repository Schema User name

<AN_ODI_WORK_PASS>: ODI Work Repository Schema password

<AN_ODI_DBA>: ODI DBA User name

<AN_ODI_DBA_PASS>: ODI DBA password

<MY_TBS>: Default tablespace

<MY_TEMP>: Temporary tablespace

Creating a Master Repository:

Follow the steps given below to create a master repository:

1. Start ODI Studio console and Open the New Gallery by choosing File > New. In the New Gallery, in the Categories tree, select ODI. Select from the Items list the Master Repository Creation Wizard. Click OK. The Master Repository Creation Wizard appears.
2. In the Master Repository Creation Wizard, select the browse icon of the JDBC Driver and then select Oracle JDBC Driver. Click OK.
3. Edit the JDBC URL to read as follows:

   jdbc:oracle:thin:<dwh_db_server>:<dwh_db_listener_port>:<dwh_db_sid>

   where:

   <*dwh_db_server*> is the DB Server where the ODI Master repository is created as mentioned in the above steps

   <*dwh_db_listener_port*> is the DB Servers listener port, such as 1521.

   <*dwh_db_sid*> is the DB server instance SID.
4. Enter the User as **<AN_ODI_MASTER>** and the Password as **<AN_ODI_MASTER_PASS>**.
5. For the repository configuration ID, use a number other than 100,101, 488, and 489.

6. For **DBA user** and **password** fields, provide the details as **<AN_ODI_DBA>** and **<AN_ODI_DBA_PASS>**, respectively.
7. Click **Test Connection** and verify successful connection. Click **OK**.
8. Click **Next**.
9. In the **Authentication** window, enter **Supervisor Password**. Enter password again to confirm and Click **Next**.
10. In the **Password Storage** window, select internal password **Storage**, and then click **Finish**.
11. When Master Repository is successfully created, you will see the Oracle Data Integrator Information message. Click **OK**. The ODI Master repository is now created.

Connecting to the ODI Master Repository:

Follow the steps given below to connect to the ODI Master Repository:

1. In ODI Studio, open the New Gallery by choosing File > New. In the New Gallery, in the Categories tree, select ODI. From the Items list select Create a New ODI Repository login.
2. Configure Repository Connections with the parameters from the tables provided below. To enter the JDBC URL, click the button next to JDBC URL field and select jdbc:oracle:thin:@<host>:<port>:<sid>, then edit the URL. Select **Master Repository Only** button. Click **Test**. Verify successful connection and click **OK**.
3. Finally, click **OK** and save the connection.

Oracle Data Integrator Connection	
Parameter	**Value**
Login Name	AN Master Repository
User	SUPERVISOR
Password	Supervisor Password

Database Connection (Master Repository)	
Parameter	**Value**
User	<AN_ODI_MASTER>
Password	<AN_ODI_MASTER_PASS>
Driver List	Oracle JDBC Driver
Driver Name	oracle.jdbc.OracleDriver
URL	jdbc:oracle:thin: <dwh_db_server>:<dwh_db_ listener_port>:<dwh_db_sid>

Note: Do not copy and paste in the JDBC URL field. This may cause problems with entering a valid URL string. Instead, open the drop-down menu and select the correct driver from the list. And then type the correct URL in the URL field.

4. Click **Connect to Repository**. Select the newly created repository connection Master Repository from the drop-down list. Click **OK**. The ODI studio starts.

   You are now successfully connected to the master repository in ODI Studio.

Creating Work Repository:

Follow the steps given below to create a work repository:

1. Start ODI Studio and connect to the AN Master Repository created in the step above.
2. Click the **Topology Navigator** tab and select the **Repositories** panel.
3. Right-click the **Work Repositories** node and select **New Work Repository**. This displays the **Create Work Repository Wizard**.
4. In the screen that follows, enter the following values for the parameters:

Parameter	Value
Technology	Oracle
Driver Name	oracle.jdbc.driver.OracleDriver
JDBC URL	jdbc:oracle:thin: <dwh_db_server>:<dwh_db_ listener_port>:<dwh_db_sid>
User	<AN_ODI_WORK>
Password	<AN_ODI_WORK_PASS>

5. Click **Test**. Verify successful connection and click **OK**.
6. Specify the properties of the **Oracle Data Integrator Work Repository**:

   ID: A specific ID for the new repository other than 100, 101, 488, and 489.

   Name: Give a unique name to the work repository such as <AN_WORKREP1>.

   Password: Enter the password, if required.

   Work Repository Table: Let this remain as Deployment.

   Click **Finish** to save the details.
7. In the **Create Work Repository Login** dialog, click **Yes** to create a connection for Work Repository in ODI.
8. Enter the Login name as **AN Work Repository** and click **OK**.
9. Disconnect from the **Master repository** and connect to the Work repository.
10. Click the **ODI** menu and select **Disconnect AN Master Repository**.
11. Click **Connect to Repository**. Select **AN Work Repository** from the **Login Name** drop-down list.
12. Enter the password and click **OK**.

    We have now successfully created and connected to the ODI Work repository.

2.2 Running the Oracle Argus Analytics Installer

The basic Oracle Argus Analytics components are installed using the Oracle Universal Installer. The installer gathers all the information about the database connectivity, data

mart, Informatica repository by presenting a sequence of prompt screens and then installs the components accordingly. This installer needs to be executed in the Oracle Argus Analytics 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:\argus_analytics_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 Oracle Argus Analytics 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.

Choice of New Install / Upgrade from AN 1.1

Please choose appropriately in the installation process if Argus Analytics is a fresh installation or an upgrade installation which is supported from Argus Analytics 1.1 to 1.1.1.

> **Note:**
>
> - For Exadata Hardware, you cannot upgrade the existing installation of Argus Analytics. You need to install Argus Analytics (fresh Installation) again.
> - The upgrade path installation needs information to be provided on the previous Argus Analytics 1.1 installation details.

Oracle Argus Analytics Home Path

The Oracle Argus Analytics 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 the Installer would execute the database and Informatica scripts.

Home Name: ANHome1

Path: C:\argus_analytics

Click **Next**.

> **Note:** In case of Installation choice as upgrade path, provide the previously installed AN Home details.

Select the Choice of New Install / Upgrade from AN 1.1

For new or upgrade install, corresponding details will be asked. These details are explained in the respective sections below.

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
- ESM Schema Owner
- ESM Schema Password
- Oracle Argus Analytics Source Schema and Password
- Oracle Argus Analytics Source RPD Schema and Password
- Oracle Argus Analytics Source Work Schema and Password
- Oracle Argus Analytics Source Default Tablespace [AN_DATA_TS]
- Oracle Argus Analytics Source Temp Tablespace [AN_TEMP_TS]

Note: Oracle Argus Analytics Source schema, Argus Analytics Source RPD schema, and Argus Analytics Source Work schema are the new schemas which would get created by the installer to store the views for all Argus Source tables that are needed for the ETL and reporting process. You must ensure that these are not pre-existing schemas before running the Oracle Argus Analytics Installer.

If **Upgrade Install** is chosen, provide the existing details of AN Schemas for the following:

Oracle Argus Analytics Source Schema and Password

Oracle Argus Analytics Source RPD Schema and Password

Oracle Argus Analytics Source Default Tablespace [AN_DATA_TS]

Oracle Argus Analytics Source Default Tablespace [AN_TEMP_TS]

Apart from this, the AN Source Work Schema that is provided, is used during the ETL process for ETL Management tasks, which are executed during ETL runs.

Example:

- AS Database Connect String: AS70X_SID
- AS Schema: ARGUS_APP
- AS Password: <ARGUS_APP user's password>
- AS System Password: <SYSTEM user's password>
- VPD Schema: VPD_ADMIN
- ESM Schema Owner: ESM_OWNER
- ESM Schema Password: < ESM_OWNER's password>

Click **Next**

- Oracle Argus Analytics Source Schema: AN_SRC

- Oracle Argus Analytics Source Password: <AN_SRC password>
- Oracle Argus Analytics Source RPD Schema: AN_SRC_RPD
- Oracle Argus Analytics Source RPD Password: <AN_SRC_RPD password>
- Oracle Argus Analytics Source Work Schema: AN_SRC_WRK
- Oracle Argus Analytics Source Work Password: <AN_SRC_WRK password>
- Oracle Argus Analytics Source Default Tablespace: AN_DATA_TS
- Oracle Argus Analytics Source Temp Tablespace: AN_TEMP_TS

Oracle Argus Analytics Data Mart Details

This screen collects all the information regarding the Oracle Argus Analytics data mart details.

The following are the details of the data mart:

- DWH Data Mart DB Connect String
- DWH Data Mart System User Password
- DWH Schema and Password
- DWH RPD Schema and Password
- DWH Work Schema and Password
- DWH Default Tablespace
- DWH Temporary Tablespace

Note: DW Schema, DWH RPD Schema, and DWH Work Schema are the new schemas that will be created by the installer to store the ETL data. Oracle Argus Analytics RPD schema is the schema which would contain the synonyms of all the data mart tables and is used by OBIEE reports.

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

If **Upgrade Install** is chosen, provide the existing details of AN Schemas for the following:

DWH Data Mart DB Connect String

DWH Data Mart System User Password

DWH Schema and Password

DWH RPD Schema and Password

DWH Default Tablespace

DWH Temporary Tablespace

If the Argus Safety System is a multi-tenant application, the VPD policy and additional contexts are created during installation with names predefined as:

- VPD Policy Names:

  <AN_SRC>_src_vpd

  <AN_DWH>_dwh_vp
- Contexts:

  <AN_SRC>_src_ctx

  <AN_DWH>_dwh_ctx
- Exadata Context:

  <AN_DWH>_exa_ctx

Example:

- DW Database Connect String: ANDWH_SID
- DW System Password: <system user's password of data mart database>
- Oracle Argus Analytics DW Schema: AN_DWH
- Oracle Argus Analytics DW Password: <password for AN_DWH schema>
- Oracle Argus Analytics RPD Schema: AN_DWH_RPD
- Oracle Argus Analytics RPD Password: <password for AN_DWH_RPD schema>
- Oracle Argus Analytics Work Schema: AN_DWH_WRK
- Oracle Argus Analytics Work Password: <password for AN_DWH_WRK schema>
- DW Default table space: AN_DATA_TS
- DW Temporary tablespace: AN_TEMP_TS

Click **Next**.

Exadata Database

If the Datawarehouse DB Server is Exadata, select **Yes**, else select the **No** radio button.

ETL Choice

Informatica or ODI Radio Buttons

Informatica and ODI technologies are available as ETL choices during installation. As per the choice respective details should be entered. Information required with respect to each tool is explained below.

Informatica PowerCenter Details

This screen is shown only when the choice of ETL during installation is selected as Informatica. It collects all the information to connect to the Informatica server.

> **Note:** The Informatica Repository should be a Versioned Repository. If it is not a versioned repository, the installation will fail.

Example:

- PowerCenter Repository: AN_ PowerCenter_Repository
- PowerCenter Domain: Domain_AN
- PowerCenter Admin user id: Administrator
- PowerCenter Admin password: <administrator password>
- Oracle Argus Analytics Import folder: OPVA

Click **Next**.

> **Note:** In case of an **Upgrade Install**, provide information as per the existing installation details for AN 1.1.
>
> Apart from this, if **Upgrade Install** is chosen then the installer will delete and recreate the relational connections 'opva_src' and 'opva_dwh' in the provided Informatica Repository.

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 Oracle Argus Analytics home and will create the Data Mart schemas, RPD & WORK schemas. In addition, it will also create contexts and VPD policy if the Argus Safety installation is a multitenant application.

After the installation has been completed, the install log can be found at:

<Argus Analytics home>\install\opva_install.log and pvadriverscript<timestamp>.log

This log file must be verified to ensure that the installer has completed successfully.

2.3 Preparing the DAC Repository (Informatica Only)

Note: This section assumes that the DAC client is present in the same machine where the Oracle Argus Analytics installer is run. If not, copy the <Argus Analytics 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 <Argus Analytics 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 Oracle Argus Analytics data mart 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 the **Change import/export** folder to navigate to <DRIVE>:\Argus Analytics home\DAC folder, that holds the DAC Repository for the Oracle Argus Analytics 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 Application List.
   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 Oracle Argus Analytics Data Mart). For each database with which DAC will interact for Oracle Argus Analytics, 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 mart (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 Oracle Argus Analytics schema in the Argus Safety DB Instance.

Table Owner Password — Enter the Oracle Argus Analytics 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 Mart 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

Parameters	Description	Allowed Values
$$p_config_days	Reduces the incremental extract window by the specified number of days. E.g.: Extract all changed rows between LAST_EXTRACT_DATE and (SYSDATE - $$p_config_days)	Integers Recommended Value: 0

Table 2–1 (Cont.) DAC Configurable Parameters

Parameters	Description	Allowed Values
$$p_enterprise_id	The specific Enterprise ID to run the ETL for.	-1: Runs the Incremental ETL for the entire Warehouse 0: Runs the Incremental ETL for all the enterprises the user ($$p_user_name) has access to. Integer Value [1,2,3, etc]: Runs the Incremental ETL for the specified Enterprise only.
$$p_etl_proc_id	The unique Identifier for the ETL Process that is run and it takes its value by default from DAC or from ODI	Do not change or specify any other value. Please leave it unmodified.
$$p_include_pseudo_state_flag	The parameter defines whether to include the workflow states present between the Locking record and the Unlocking record of a case in the Case Workflow State Fact table.	Default value is 1 1: Include the Workflow States between Locking and Unlocking records of the case. 0: Exclude the Workflow States between Locking and Unlocking records of the case.
$$p_last_extract_date	System defined value for defining the start date of the extract window for Incremental Data or the last time the ETL ran successfully for the enterprise specified	Do Not Change. It is taken by default from DAC metadata.
$$p_override_last_extract_date	Specify a Date value in the format MM/DD/RRRR in case you want to override the last extract date for the Incremental Data	Date values in the format: 01/01/1999 or 12/23/2007
$$p_rekey_fact	To rekey fact tables in case data in the W_HS_MAPPING_S defined for match and merge has changed	0: Will not rekey the Fact tables 1: Will rekey the Fact tables
$$p_user_name	The user name for which the Incremental ETL shall use to set the VPD Context for the specified enterprise in the parameter: $$p_enterprise_id	Default value: 'admin'
$$START_DATE	The start date of the days to populate from in the W_DAY_D/PVA_DAY table. It should be in the format: MM/DD/RRRR	Default value: 01/01/1980
$$END_DATE	The end date of the days to populate till in the W_DAY_D/PVA_DAY table. It should be in the format: MM/DD/RRRR	Default value: 01/01/2020

Note: If you are upgrading from Argus Analytics 1.1 to 1.1.1, it is not necessary to run/force a Full Load ETL again in DAC for Argus Analytics. Instead, provide a valid value for the **$$p_override_last_extract_date** parameter before executing the ETL **OPVA Data Warehouse Load**.

This ensures that DAC runs the new ETL of Argus Analytics 1.1.1 to get only the changed data in Argus Safety from the specified override date onwards. This is an important step to be considered in an upgrade. If this parameter is not set, the incremental ETL will run with a default Override Extract Date as the **01/01/1900** for the first time and will refresh the entire warehouse again unnecessarily. It will also run for a much longer duration than expected.

Use the **Run History** tab in DAC for Argus Analytics to find the last successful run date for the ETL **OPVA Data Warehouse Load** of the Argus Analytics 1.1 release. This value or an earlier date can be specified for the **$$p_override_last_extract_date** parameter.

For example, if the last successful run in Argus Analytics 1.1 release for the ETL **OPVA Data Warehouse Load** in Incremental mode was 01/15/2013, set the **$$p_override_last_extract_date** parameter to 01/15/2013 prior to executing the ETL.

Once this incremental load has been executed successfully, set the **$$p_override_last_extract_date** DAC parameter back to Null, so that the subsequent executions of the ETL will take the new extract window, as per the data in the control tables per enterprise which is set at the end of every successful ETL run.

2.4 ODI Smart Import and Topology Configuration (ODI only)

This section comprises the following sub-sections:

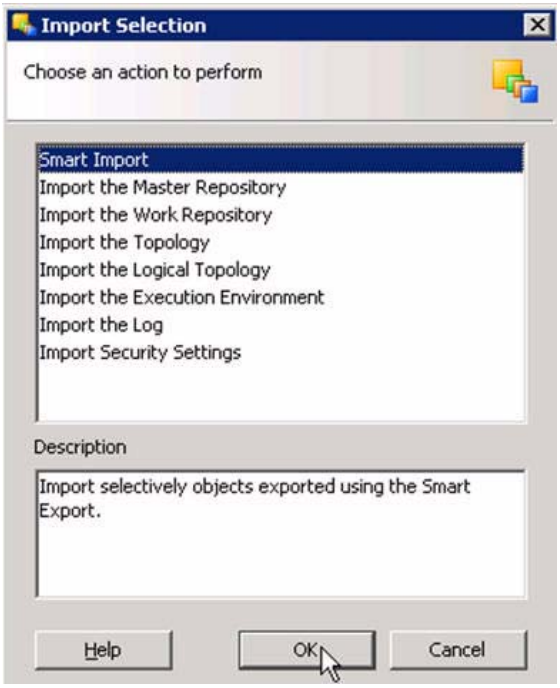
- ODI Smart Import
- Configuring the Topology in ODI Studio
- Configuring the Standalone ODI Agent
- Deploying and Configuring the ODI Java EE agent on the existing WebLogic Domain

2.4.1 ODI Smart Import

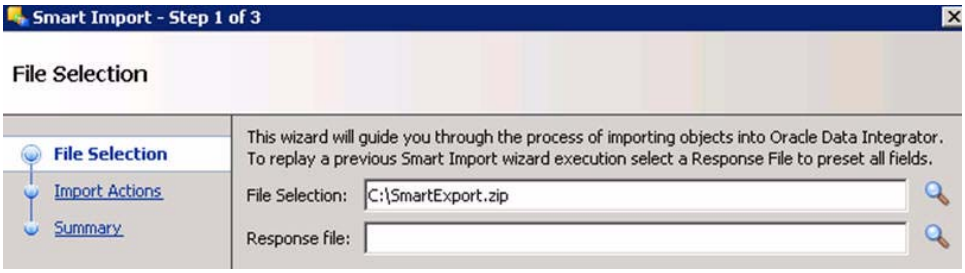
Follow the steps listed below to execute ODI Smart Import:

1. Log in to the work repository in ODI Studio by selecting the **AN Work Repository** connection.
2. Select the **Connect Navigator** drop-down list from the top right on the **Designer** tab and click **Import**.

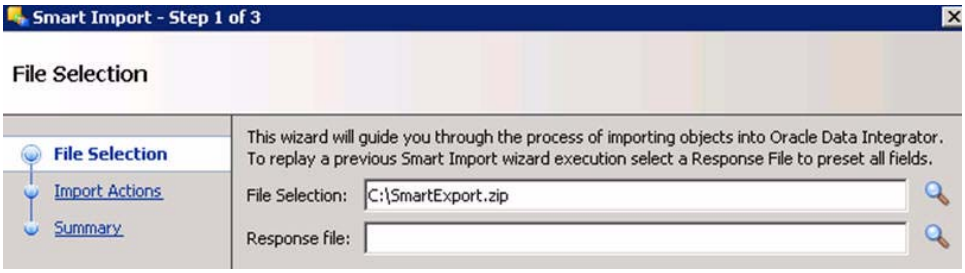
3. Select **Smart Import** from the **Import Selection** menu and click **OK**. The **Smart Import Wizard** is displayed.



4. Select the zip file called an.zip from the <AN_INSTALL_HOME>\odi directory in the File Selection textbox and click next. The files can also be browsed by clicking on the symbol available with the textbox.



5. ODI imports the file and checks for any issues that can occur while importing ODI objects. If issues are found, then the same will be displayed in import actions window. Click **Next** if no issues are found.



6. Click **Finish**.

   This imports all the AN objects in ODI repository and makes them visible in the ODI Studio Console.

2.4.2 Configuring the Topology in ODI Studio

Follow the steps listed below to configure Topology in ODI Studio:

1. Open the ODI Studio and connect as AN Work Repository.
2. Navigate to Topology.
3. Select the Physical Architecture tab.
4. Expand the tree structure to expose the following:

   Technologies > Oracle >
5. Edit the node DS_AN_ArgusAnalytics.
6. Edit the following fields in the Definition window:
   - Instance/dblink (Data Server):

     The complete TNS entry of the DWH server should be pasted here in a single line:

     (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = <DWH_DB_SERVER>)(PORT = <DWH_DB_LISTENER_PORT>)) (CONNECT_DATA =(SID=<DWH_DB_SID>)))

   - Connection:
     - User: <AN_DWH_WRK> [the DWH work schema user created during installation]
     - Password: <AN_DWH_WRK_PASS> [The password for the DWH Work schema]
7. In the JDBC window, edit the following fields:
   - JDBC URL: jdbc:oracle:thin: <DWH_DB_SERVER>:<DWH_DB_LISTENER_PORT>:<DWH_DB_SID>
8. Save the details and click **Test Connection** to validate it.
9. Expand the tree below DS_AN_ArgusAnalytics to expose the tree node DS_AN_ArgusAnalytics.AN_DWH.
10. Edit the node DS_AN_ArgusAnalytics.AN_DWH.
11. Change the Schema by selecting from the drop-down list for the following fields:
    - Schema (Schema): <AN_DWH>
    - Schema (Work Schema): <AN_DWH_WRK>
12. Save the changes.
13. Similarly, edit the node DS_AN_ARGUS_SAFETY to provide information on the Argus Safety DB Server.
14. Edit the following fields in the Definition window:
    - Instance/dblink (Data Server):

      The complete TNS entry of the DWH server should be pasted here in a single line:

      (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = <AS_DB_SERVER>)(PORT = <AS_DB_LISTENER_PORT>)) (CONNECT_DATA =(SID=<AS_DB_SID>)))

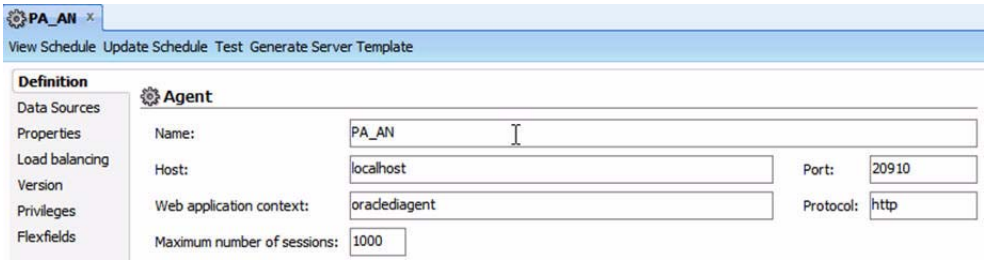
- Connection:
  - User: <AN_SRC_WRK> [the AN Source Work Schema user created during installation]
  - Password: <AN_SRC_WRK_PASS> [The password for the AN Source Work Schema]

15. In the JDBC window, edit the following fields:
    - JDBC URL: jdbc:oracle:thin:<AS_DB_SERVER>:<AS_DB_LISTENER_PORT>:<AS_DB_SID>
16. Save the details and click **Test Connection** to validate it.
17. Expand the tree below DS_AN_ArgusSafety to expose the tree node DS_AN_ArgusSafety.AN_SRC.
18. Edit the node DS_AN_ArgusSafety.AN_SRC.
19. Change the Schema by selecting from the drop-down list for the following fields:
    - Schema (Schema): <AN_SRC>
    - Schema (Work Schema): <AN_SRC_WRK>
20. Save the changes.

2.4.3 Configuring the Standalone ODI Agent

Follow the steps listed below to configure the Standalone ODI Agent:

1. Use the ODI Studio Topology Manager to edit the standalone agent PA_AN definition. And save the information as per the installation done for ODI.



Note: The Host field contains the Host name where the standalone Agent will be running. In this example, the host is on the same server, and the default port number used is 20910.

Change the Port Number to any value other than the default to avoid conflicts with other installations (for example, 20920).

2. Go to the <ODI_HOME>/oracledi/agent/bin/ directory and edit odiparams.bat file and set the following properties per the installation done:

   set ODI_MASTER_URL=jdbc:oracle:thin:@<DB_SERVER>:<DB_LISTENER_PORT>:<DB_SID>

   set ODI_MASTER_USER=AN_ODI_MASTER

   set ODI_MASTER_ENCODED_PASS=eyfHauaP43Z1nj4JIml4ziQZmp

set ODI_SUPERVISOR=SUPERVISOR

set ODI_SUPERVISOR_ENCODED_PASS=<encoded password from encode.bat, as explained below>

set ODI_SECU_WORK_REP=AN_ODI_WORK

set ODI_JAVA_HOME=<ODI_HOME>/jrockit

Note: The encoded password can be generated using the encode.bat file present in <ODI_HOME>/oracledi/agent/bin/.

1. Open a new command window [cmd].
2. Change the directory to <ODI_HOME>/oracledi/agent/bin/.
3. Execute the following command: Encode.bat<password>
4. The resulting string can be used as the encoded password in the above statements.

---

3. Create a new batch file agent_PA_AN.bat at the following location:

   <ODI_HOME>/oracledi/agent/bin/

4. Edit the agent_PA_AN.bat file and enter the agent details:

   Example: <ODI_HOME>/oracledi/agent/bin/agent.bat "-NAME=PA_AN" "-PORT=20910"

   Change the Port Number from 20910 to the value specified in Step 1.

5. Test the Agent in ODI Topology Manager.

Note: Refer to the **Executing the ETL Load Plans in ODI** section in the Oracle Argus Analytics User Guide to run the ETLs in ODI and for more information on ODI Configurable Parameters.

Note: If you are upgrading from Argus Analytics 1.1 to 1.1.1, it is not necessary to run the Full Load ETL (LP_FL_AN) again in ODI for Argus Analytics. Instead, the load plan LP_IL_AN can be directly executed, along with providing a valid value for the **VAR_INT_OVERRIDE_LAST_EXTRACT_DATE** parameter. Apart from this, the load plan requires another list of parameters.

This ensures that ODI runs the new ETL of Argus Analytics 1.1.1 to get only the changed data in Argus Safety from the specified override date onwards. This is an important step to be considered in an upgrade. If this parameter is not set, the incremental ETL will run with the default Override Extract Date as the **01/01/1900** for the first time and will refresh the entire warehouse again unnecessarily. It will also run for a much longer duration than expected.

Use the **Run History** tab in DAC for Argus Analytics to find the last successful run date for the ETL **OPVA Data Warehouse Load** of the Argus Analytics 1.1 release. This value or an earlier date can be specified for the **VAR_INT_OVERRIDE_LAST_EXTRACT_DATE** parameter.

Once this incremental load has been executed successfully, you need not specify a value for the **VAR_INT_OVERRIDE_LAST_EXTRACT_DATE** parameter for the subsequent executions of the Load Plan - LP_IL_AN. This parameter automatically takes the new extract window as per the data in the control tables per enterprise, which is set at the end of every successful run of this load plan.

2.4.4 Deploying and Configuring the ODI Java EE agent on the existing WebLogic Domain

Pre-requisites

1. Weblogic Server is installed and domain is configured <OBIEE-DOMAIN> (for example, BIFOUNDATION_DOMAIN or a new domain created specifically for ODI).
2. Oracle Data Integrator 11gR1 is installed.
3. ODI Master and Work Repositories are already configured, as described in section 2.1.1.2, ODI Studio.

Note: Install the ODI Agent as Java EE application by extending the existing Weblogic domain <OBIEE-DOMAIN> (for example, BIFOUNDATION_DOMAIN).

Installation and Configuration

1. Execute the following steps to install ODI Java EE Agent and ODI Console:
   a. Double-click **Setup.exe** for the ODI Installer. This displays the installer Welcome screen. Click **Next**.
   b. The Installer displays the **Install Software Updates** screen. Select the appropriate radio button and click **Next**.
   c. In the **Select Installation Type** screen, check only **Java EE Agent** and **ODI Console** under **Java EE Installation** node. Click **Next**.

d. In the **Prerequisite Checks** screen, verify that all the checks are fine and click **Next**.

e. Enter the appropriate details in the **Specify Installation Location** screen:

Oracle Middleware Home: <MIDDLEWARE_HOME>. For example, C:\Oracle\Middleware.

Oracle Home Directory: Specify the ODI Home directory Name. For example, Oracle_ODI1

f. Click **Next**.

g. The Installer displays the **Installation Summary** screen. Click **Next**.

h. This installs the **Java EE Agent** and **ODI Console**. Once the Installation progress is **100%**, click **Next**.

i. The Installer displays the **Installation Completed** screen. Click **Finish**.

2. Execute the following steps to create Agent in ODI Studio:

a. Start ODI Studio and connect to ODI Work repository.

b. Navigate to **Topology Navigator** > **Physical architecture** and create a new ODI Agent:

Name: OracleDIAgent (The agent name is case-sensitive. Use the exact name **OracleDIAgent**)

Port: <OracleDIAgent_Port>. For example, 8001

Host: FQDN of the Weblogic server where ODI Java EE Agent is installed. For example, obiee_server.us.oracle.com

Web application context: oracledIagent

c. Save the changes.

Note: Configure the **CTX_AN** Context appropriately or create a new context to be used with execution plan in ODI.

---

3. Execute the following steps to configure ODI Java EE Agent:

a. Open the Command Prompt, change directory to: <WLS-HOME>\common\bin (e.g. D:\Oracle\fmw\wlserver_10.3\common\bin). Execute config command. The **Configuration Wizard** starts.

b. In the **Welcome** screen, select **Extend an existing Weblogic domain** radio button and click **Next**.

c. Select the already installed Weblogic domain <OBIEE-DOMAIN> (for example, BIFOUNDATION_DOMAIN) in the **Select a Weblogic Domain Directory** screen and click **Next**.

d. In the **Select Extension Source** screen, select the following source and click **Next**:

Select **Oracle Data Integrator - Console 11.1.1.0 (Oracle Data Integrator SDK Shared Library Template - 11.1.1.0** will then also be selected; leave this option selected)

Select **Oracle Data Integrator - Agent - 11.1.1.1 (Oracle Data Integrator - Agent Libraries - 11.1.1.0** will then also be selected; leave this option selected)

e. Click **Next** on **Configure JDBC Data Sources** screen.

f. Click **Next** on **Test JDBC Data Sources** screen.

g. In the **Configure JDBC Component Schema** screen:

Select the ODI Master Schema and enter the following details.

DBMS/Service: Database Service Name where ODI Master Repository is created as in step 2.1.1.2. For example, odi_db.us.oracle.com

Port: Listener Port Number for Database where ODI Master Repository is created. For example, 1521

Schema Owner: <AN_ODI_MASTER> ODI Master Repository Schema name.

Schema Password: <AN_ODI_MASTER_PASS> ODI Master Repository Schema password.

Select the **ODI Work Schema** and enter the following details.

DBMS/Service: Database Service Name where ODI Work Repository is created as in step 2.1.1.2. For example, odi_db.us.oracle.com

Host Name: Database Server Name where ODI Work Repository is created as in step 2.1.1.2. For example, odi_db_server.us.oracle.com

Port: Listener Port number for Database where ODI Work Repository is created. For example, 1521

Schema Owner: <AN_ODI_WORK> ODI Work Repository Schema Name.

Schema Password: <AN_ODI_WORK_PASS> ODI Work Repository Schema Password.

Click **Next**.

h. In the **Test JDBC Component Schema** screen, verify that the test for both Master and Work Repository Schemas are successful and click **Next**.

i. In the **Select Optional Configuration** screen, select the following options and click **Next**.

Managed Servers, Clusters and Machines

Deployments and services

j. Click **Next** in the **Configure Managed Servers** screen.

k. Click **Next** in the **Configure Clusters** screen.

l. Click **Next** in the **Assign Servers to Clusters** screen.

m. Click **Next** in the **Create HTTP Proxy Applications** screen.

n. Click **Next** in the **Configure Machines** screen.

o. Click **Next** in the **Assign Servers to Machines** screen.

p. In the **Target Deployments to Clusters or Servers** screen, verify that **oraclediagent** and **odiconsole** are checked under **Deployments** for **AdminServer** and **<ODI_SERVER>** (for example, odi_server1) and click **Next**.

q. In the **Target Services to Clusters or Servers** screen, verify that **odiMasterRepository** and **odiWorkRepository** are checked under **JDBC -**

JDBC System Resources for **<ODI_SERVER>** (for example, odi_server1) and click **Next**.

r. On the **Configuration Summary** screen, click **Extend**. This extends the existing domain.

s. Click **Exit**, when the configuration is complete.

4. Execute the following steps to connect to the WebLogic server and Managed server <ODI_SERVER> (for example, odi_server1)

   Now that the WebLogic domain has been extended with the ODI JEE agent, you need to connect to WebLogic server and Managed server <ODI_SERVER> (for example, odi_server1).

   a. In the command prompt, change directory to the directory of the domain home (for example, C:\Oracle\Middleware\user_projects\domains\<OBIEE -DOMAIN>\bin) and execute the **startweblogic** command.

   b. Security must be set up for the JAVA EE application to have access to the ODI repository. The entry will be created within the credential store, which will allow the JAVA EE Agent to authenticate itself to be able to use the required resources. This user must be already set up in the ODI Security (for example, SUPERVISOR). To do so, execute the following steps.

      Start WLST: In the new command window, change directory to the WLS_HOME common bin (e.g. C:\Oracle\Middleware\oracle_common\common\bin), and execute the **wlst** command. This will open the Weblogic Server Administration Scripting Shell.

      Execute the following command to connect to the running Admin server: (Use the appropriate Weblogic username and password)

      connect('<WEBLOGIC_USERNAME>','<WEBLOGIC_PASSWORD>','t3://localhost:7001')

      Execute the following command to add the correct credential store for ODI Supervisor :

      createCred (map="oracle.odi.credmap", key="SUPERVISOR", user="<SUPERVISOR>", password="<PASSWORD>", desc="ODI SUPERVISOR Credential")

      Note: All commands are case-sensitive.

      ---

   c. To start the Managed server <ODI_SERVER> (for example, odi_server1), change directory to WLS Home (for example, C:\Oracle\Middleware\user_projects\domains\OBIEE-DOMAIN\bin), and execute the following command:

      StartManagedWeblogic <ODI_SERVER> (e.g. StartManagedWeblogic odi_server1)

      Enter the Weblogic user name (for example, weblogic) for the Username. Enter the appropriate password. Verify that your managed server is started in RUNNING mode.

Note: To stop Managed WebLogic server odi_server1, change directory to WLS Home (e.g. C:\Oracle\Middleware\user_projects\domains\OBIEE-DOMAIN\bin), and execute the following command:

stopManagedWebLogic <ODI_SERVER> (e.g. stopManagedWebLogic odi_server1)

Enter the Weblogic user name (for example, weblogic) for the Username. Enter the appropriate password.

5. Execute the following steps to test the ODI Java EE Agent:
   a. Login to ODI Studio Work Repository and navigate to **Topology**.
   b. Open the **OracleDIAgent**.
   c. Click the Test icon to test connectivity of your configured ODI Java EE agent.
   d. Click **OK** and close the **OracleDIAgent** tab.

2.5 Configuring the OBIEE Repository and Webcatalog

2.5.1 Prerequisites

Ensure OBIEE 11g (11.1.1.6.5) 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.

2.5.1.1 Upgrading the AN 1.1 RPD and Catalog (Upgrade Install Only)

Note: Ensure that you take a backup of the AN 1.1 RPD and Catalog before proceeding with the upgrade.

2.5.1.1.1 Upgrading the AN 1.1 RPD

The following steps will let you upgrade the AN 1.1 RPD to the latest code in AN 1.1.1. Note that `if there have been no customizations to the AN 1.1 RPD, you can skip this section`, because the latest RPD is already present at <AN_INSTALL_HOME>/repository/opva.rpd.

Steps to upgrade the AN 1.1 RPD (if required):

1. Open the AN 1.1 RPD file that you wish to upgrade to AN 1.1.1 in the OBIEE Admin Tool in offline mode.

2. Provide the repository password.
3. From the menu, select File > Merge.
4. Select the Full Repository Merge radio button.
5. Select the button to choose the Original Master Repository, and click Repository. This opens the file dialog window to choose a repository file.
6. Select the AN 1.1 RPD file.
7. Enter the repository password as 'opva123'.
8. Similarly, select the button to choose the Modified Repository and click the Repository. This opens the file dialog window to choose a repository file.
9. Select the AN 1.1 RPD file present at <AN_INSTALL_HOME>/repository/opva.rpd.
10. Enter the repository password as opva123.
11. Provide a file name for the merged repository file to be saved.
12. Provide the merged repository password as opva1234.
13. Click Next. This generates the merged RPD, which is upgraded to the AN 1.1.1 release.
14. Copy this file to another location and rename it back to opva.rpd, which will later be used to deploy on the OBIEE Server.

2.5.1.1.2 Upgrading the AN 1.1 Catalog

The following steps will let you upgrade the AN 1.1 catalog to the latest code in AN 1.1.1. Note that `if there have been no customizations to the AN 1.1 catalog, you can skip this section`, because the latest catalog is already present at <AN_INSTALL_HOME>/catalog/opva.zip.

Steps to upgrade the AN 1.1 Catalog from OBIEE 11.1.1.5 to 11.1.1.6.5:

The steps given below assume that the AN 1.1 RPD and Catalog is already deployed on the OBIEE 11.1.1.6.5 server. And that the same server would have now been upgraded to OBIEE 11.1.1.6.5.

Otherwise, if it is a freshly installed OBIEE 11.1.1.6.5 server, then deploy the AN 1.1 OBIEE RPD and Catalog (before deploying the AN 1.1 opva.rpd file, open and save it once in OBIEE Admin Tool 11.1.1.6.5 before deployment).

1. Log in to EM for OBIEE 11.1.1.6.5 and shutdown all the OBIEE services.
2. Locate and edit the following file: <OracleBIHome>/instances/instance1/config/oracleBIPresentationServicesComponent/coreapplication_obipsn/instanceconfig.xml
3. Find the element: <catalog> in this file and edit/paste the following line if not already present to set it to "true" <UpgradeAndExit>true</UpgradeAndExit>
4. Restart the OBIEE Services in EM.
5. The OBIEE Presentation Services component should start and shut down on its own.
6. Once this is completed, the catalog file gets upgraded to OBIEE v11.1.1.6.5.
7. Revert the changes in the instanceconfig.xml back to <UpgradeAndExit>false</UpgradeAndExit>

8. Restart the OBIEE services in EM.

Steps to upgrade the AN 1.1 Catalog from OBIEE 11.1.1.5 to 11.1.1.6.5:

The steps given below assume that the AN 1.1 RPD and Catalog is already deployed on the OBIEE 11.1.1.6.5 server. And that the same server would have now been upgraded to OBIEE 11.1.1.6.5.

Otherwise, if it is a freshly installed OBIEE 11.1.1.6.5 server, then deploy the AN 1.1 OBIEE RPD and Catalog (before deploying the AN 1.1 opva.rpd file, open and save it once in OBIEE Admin Tool 11.1.1.6.5 before deployment).

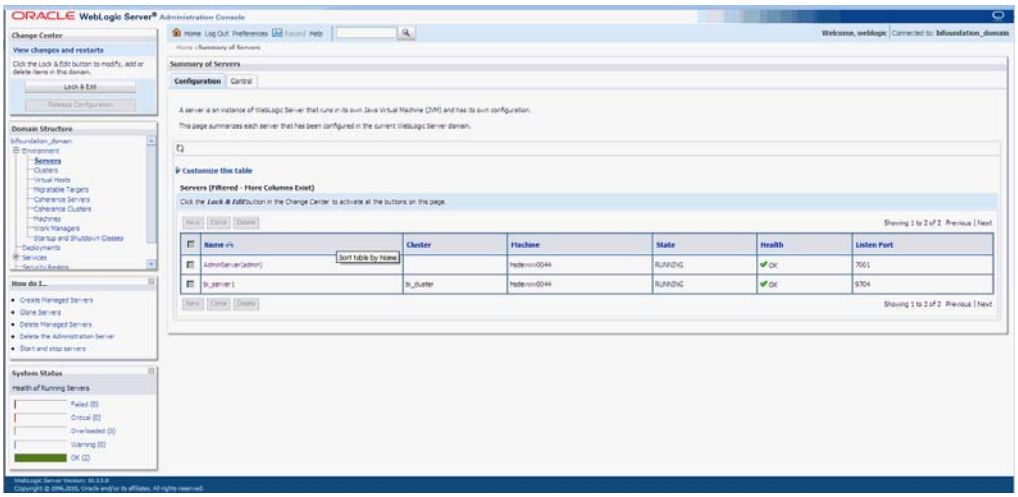
1. Open the AN 1.1 Catalog file that you wish to upgrade to AN 1.1.1 in the Catalog Manager in offline mode.
2. Expand the *root* directory in the tree structure.
3. Select the *shared* directory.
4. Go to File > Unarchive.
5. In the resulting window, choose the Archive File Path as: <AN_INSTALL_HOME>/catalog/opva_upg_11_to_111_archive.txt
6. Click OK.
   This will upgrade the catalog to the latest version of AN 1.1.1.
7. Copy this file to another location and will later be used to deploy on the OBIEE server.

2.5.2 Deployment of OBIEE Repository and Catalog

> **Note:** The default password for the **opva.rpd** repository file is **opva123**. You can change this password, as per your requirement prior to deployment in OBIEE, using the OBIEE Administrator Tool. You must remember to use this password in the steps mentioned below.

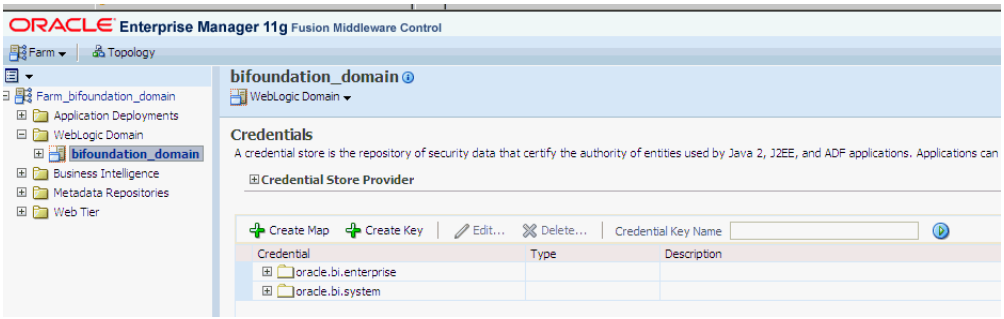
1. Log in to the Administrator Console (`http://<machinename>.<port>/console`) and navigate to Environment -> Servers. You can see the status of BI Server like below:

Figure 2–1 Oracle WebLogic Server Administration Console



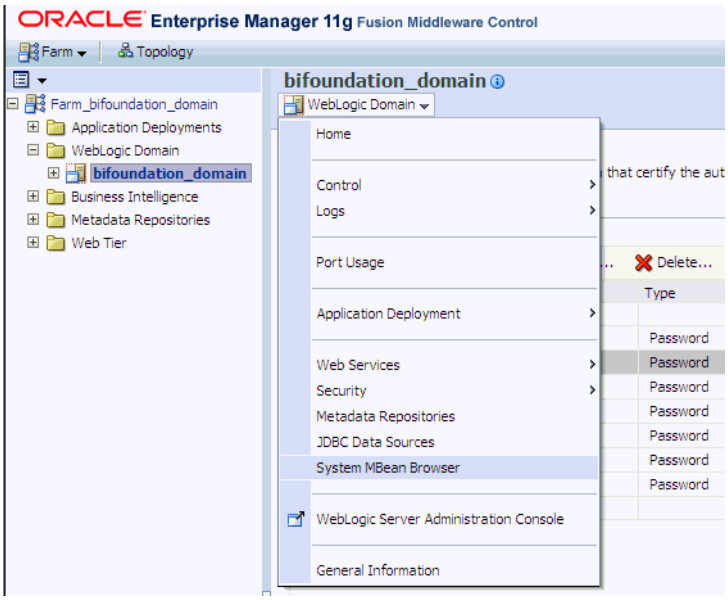
2. Now log in to EM URL `http://<machinename>.<port>/em` using the same username/password used for the Admin Console URL above.
3. Create an encrypted key entry in the EM for the Oracle Argus Analytics RPD
   - Expand the tree node Weblogic Domain and click on the bifoundation_domain (the domain created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

Figure 2–2 The bifoundation_domain Screen



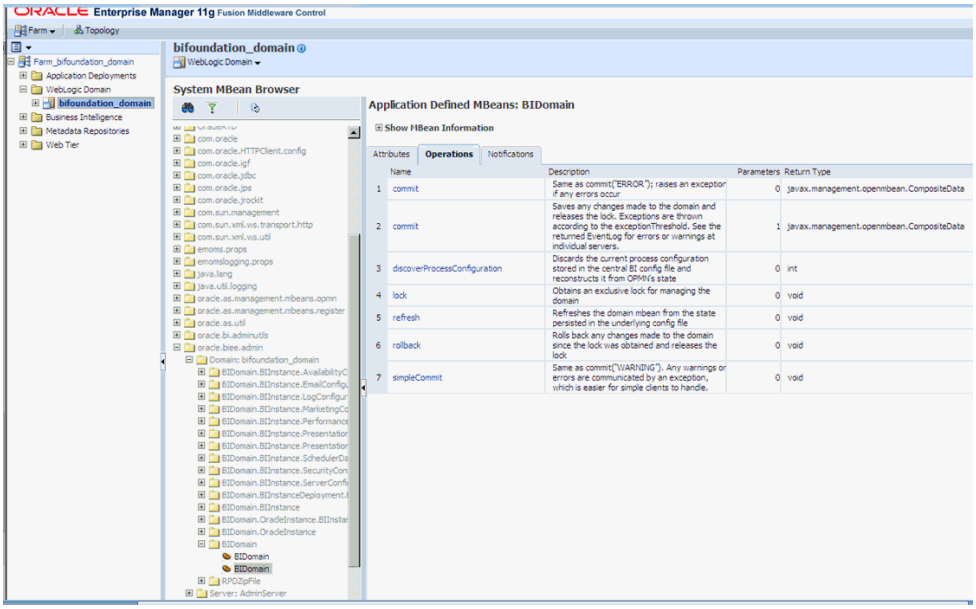
   - Click on Create Key and enter details as given here for the OPVA rpd file:
     - Select Map: oracle.bi.enterprise
     - Key: repository.opva
     - Type: password
     - User Name: Administrator
     - Password: password of choice
   - Click OK to create the security key
4. Invoke the System MBean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

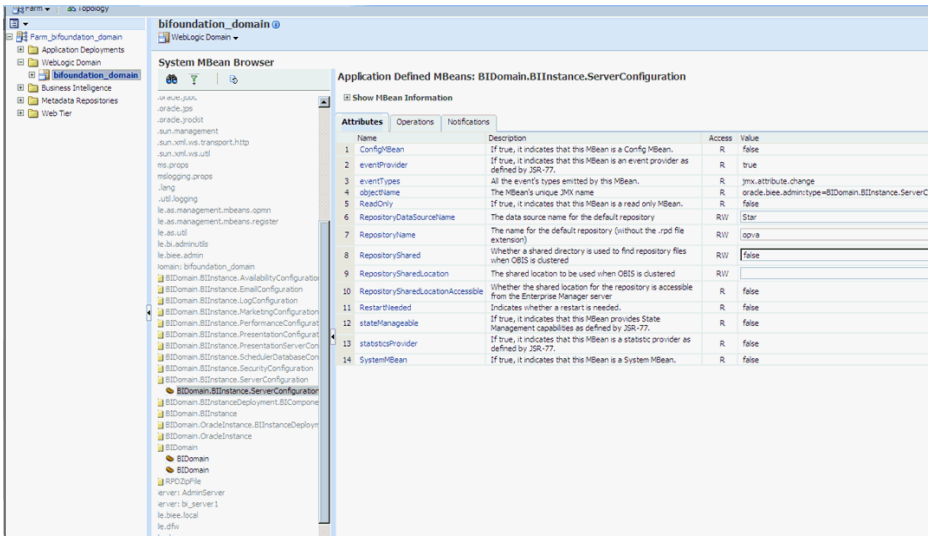
Figure 2–4 The Application Defined MBeans: Operations Screen



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

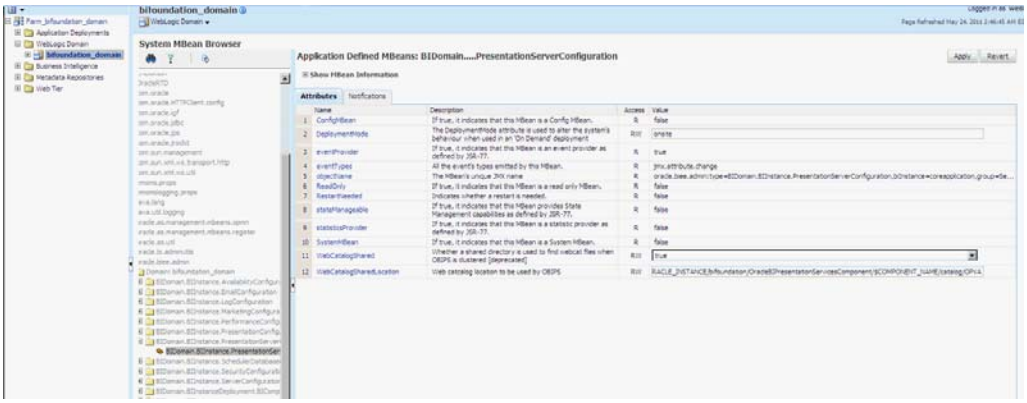
7. In the same window navigate to the Domain: bifoundation_domain -> BIDomain.BIInstance.ServerConfiguration - BIDomain.BIInstance.ServerConfiguration as shown below and in the Attributes tab, change the attribute RepositoryName as "opva", as shown below and click on Apply.

Figure 2–5 The Application Defined MBeans: Attributes Screen



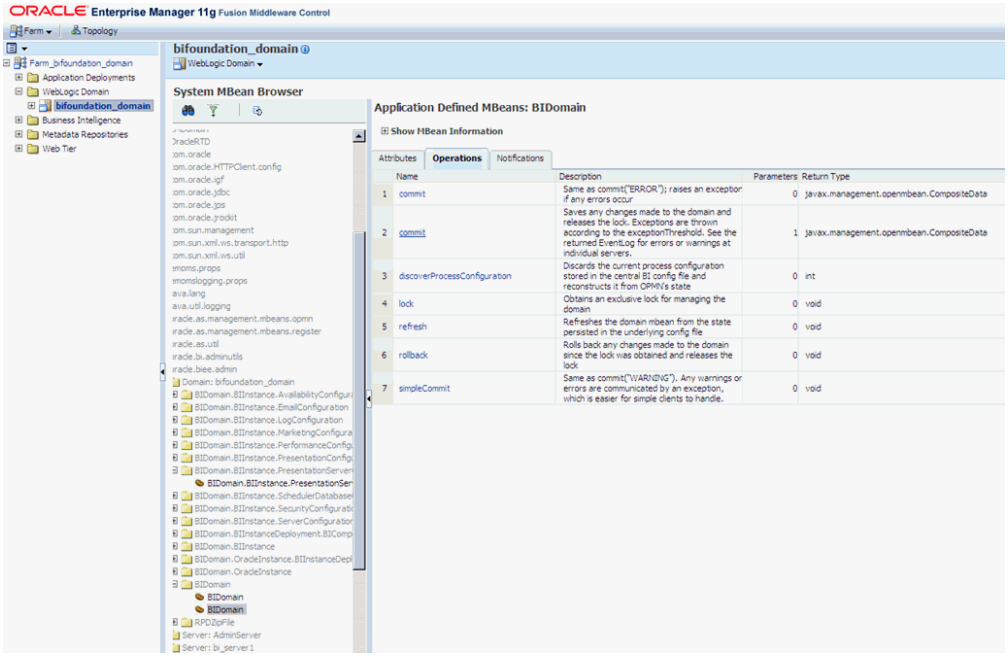
8. Next Navigate to Domain: bifoundation_domain -> BIDomain.BIInstance.PresentationServerConfiguration -> BIDomain.BIInstance.PresentationServerConfiguration and in the Attributes tab change the attribute WebCatalogSharedLocation as $ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/$COMPONENT_NAME/catalog/OPVA 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 <Argus Analytics home>\report\opva.rpd of Oracle Argus Analytics.
    - Repository Password: opva123 (or it must be the changed password in case it has been modified, as mentioned in the note before Step 1).

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

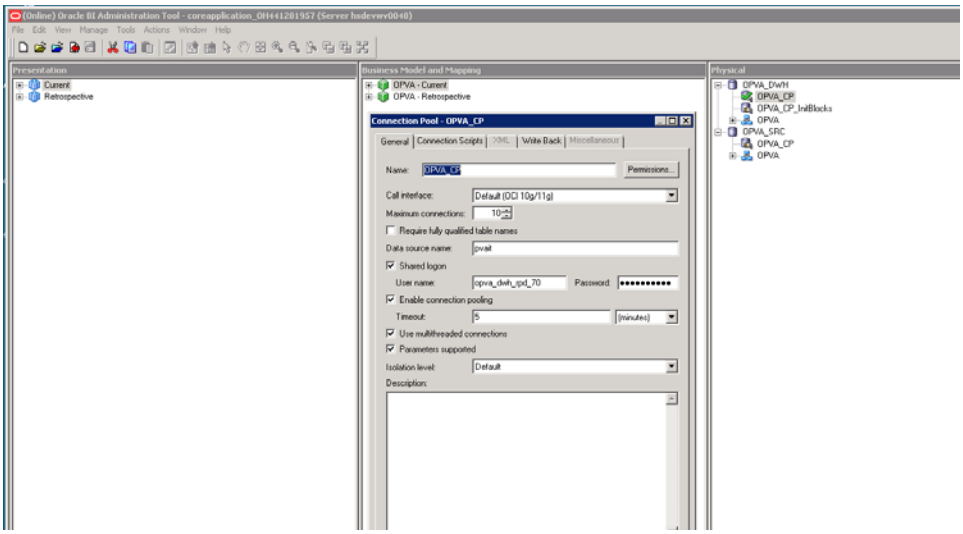
- Confirm the catalog location as $ORACLE_INSTANCE/bifoundation/OracleBIPresentationServicesComponent/$COMPONENT_NAME/catalog/opva
- Copy the Catalog from the Oracle Argus Analytics installed directory to the location mentioned above. Example: Installed location: d:\oan\report\catalog\opva.zip to the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

2.5.2.1 Post-deployment of the Oracle Argus Analytics RPD

Open the Oracle Argus Analytics RPD in the Administration Tool in online mode and change the connection pool settings for both <AN_DWH_RPD> and OPVA_DWH -> OPVA_CP_InitBlocks to point to the <AN_SRC_RPD> and the OPVA_SRC -> OPVA_CP to the Argus Safety Source RPD schema created during installation:

1. Repository Password: opva123 (or it must be the changed password in case it has been modified as mentioned in the note before Step 1 of Section 2.5.2, Deployment of OBIEE Repository and Catalog).
2. User: weblogic or BISystemUser
3. Password: Password for the user mentioned above

Figure 2–8 The Oracle Argus Analytics RPD Screen



2.5.3 Changing the OBIEE RPD Password

To change the default password for OBIEE RPD, execute the following steps:

1. Open the BI Administrator Tool and open <ARGUS_ANALYTICS_HOME>\report\opva.rpd in **Offline** mode.
2. Select **File** > **Change Password.**
3. Enter the old password as **opva123** (default password).
4. Enter the new password and confirm by entering it again. You must remember this password, instead of the default password, and use the same later in the installation process.

2.6 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 <Argus Analytics home>\help\opva_help.zip into the machine where OBIEE server is installed.

2.6.1 Configuring the Help links in the Dashboards and Reports

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

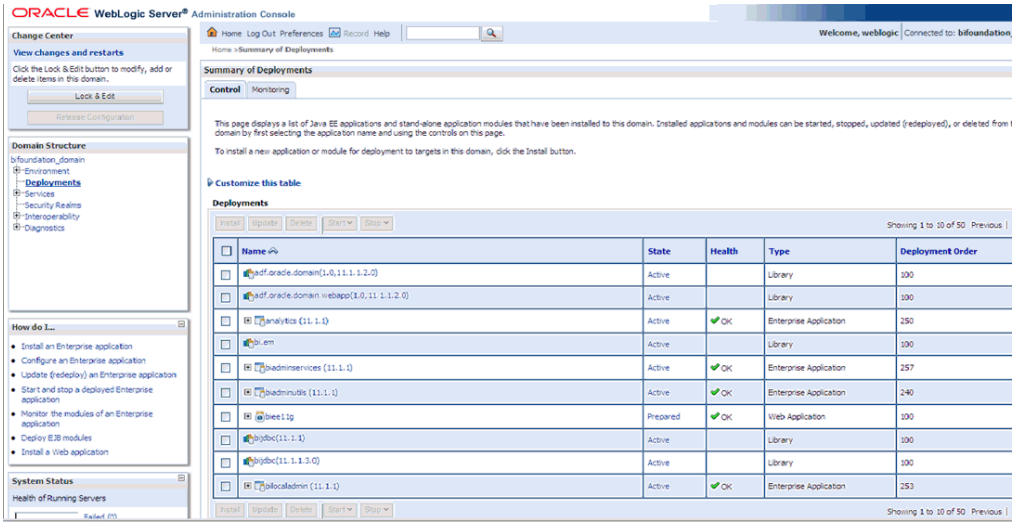
   <MIDDLEWARE_HOME>\fmw\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1\analyticsRes\

2. Extract the contents of the OPVA_HOME\report\help\opva_help.zip file into the path listed above.

3. Log in to Console (Log in to the Weblogic Server).

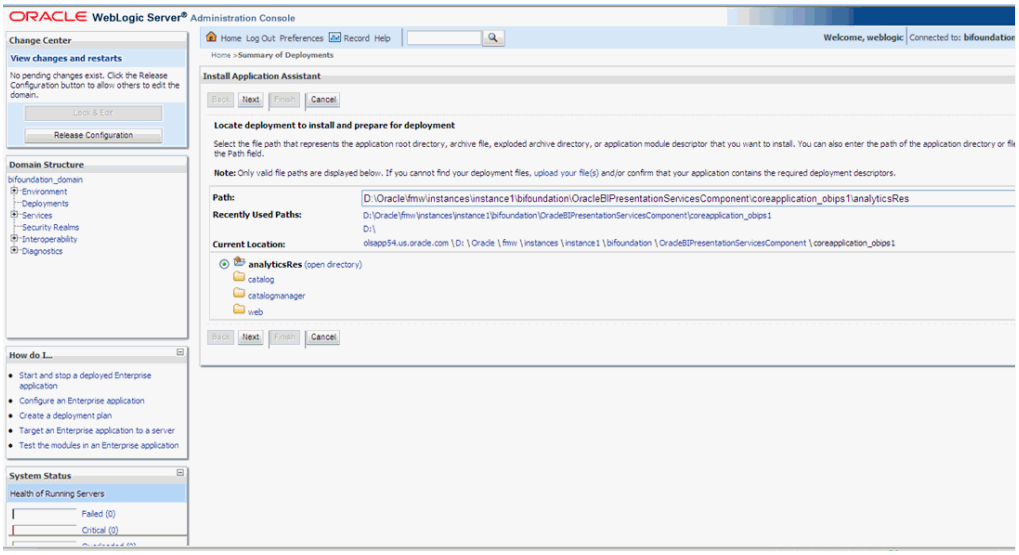
4. Navigate to Deployments.

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

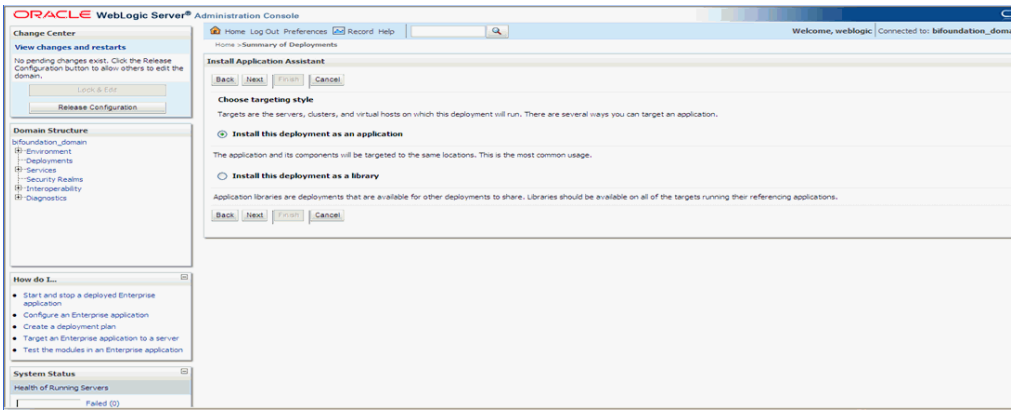


6. Click on Install and navigate to '<MIDDLEWARE_HOME>\instances\instance1\bifoundation\OracleBIPresentationServicesComponent\coreapplication_obips1'.

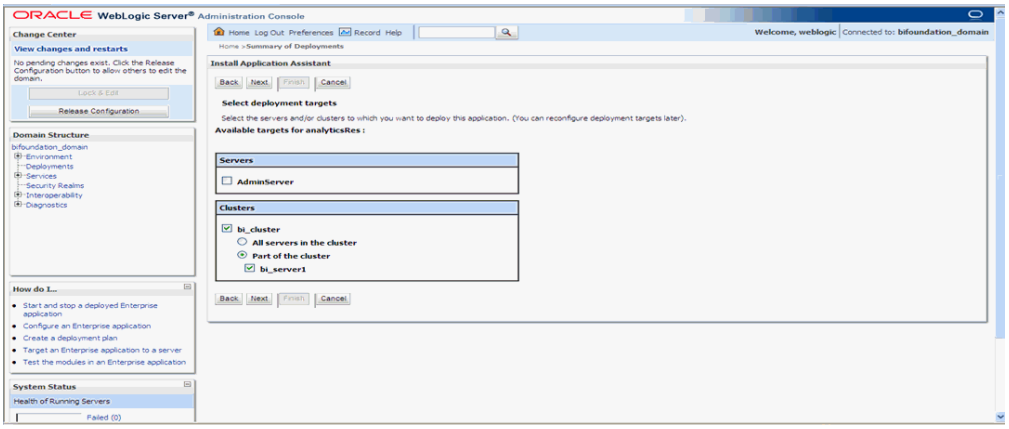
7. Select 'analyticsRes' and click 'Next'.



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



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

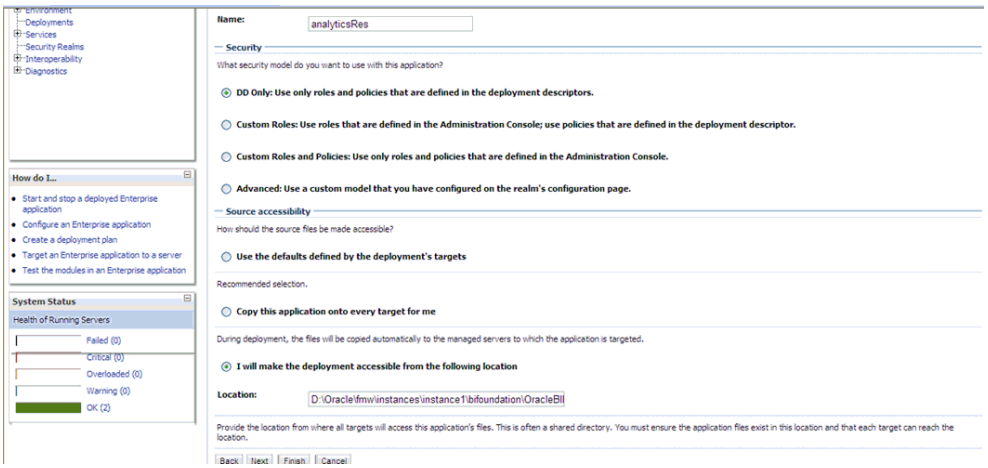


10. Under 'Source accessibility:'

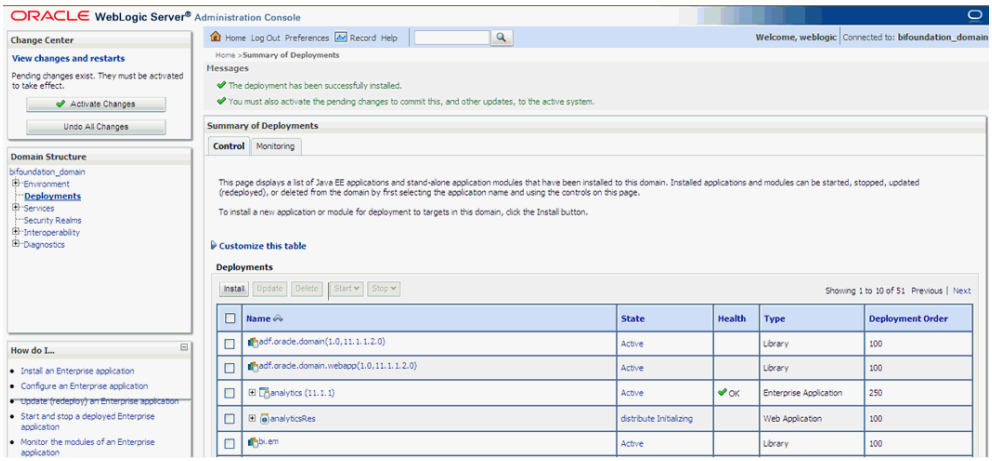
Select 'I will make the deployment accessible from the following location'

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

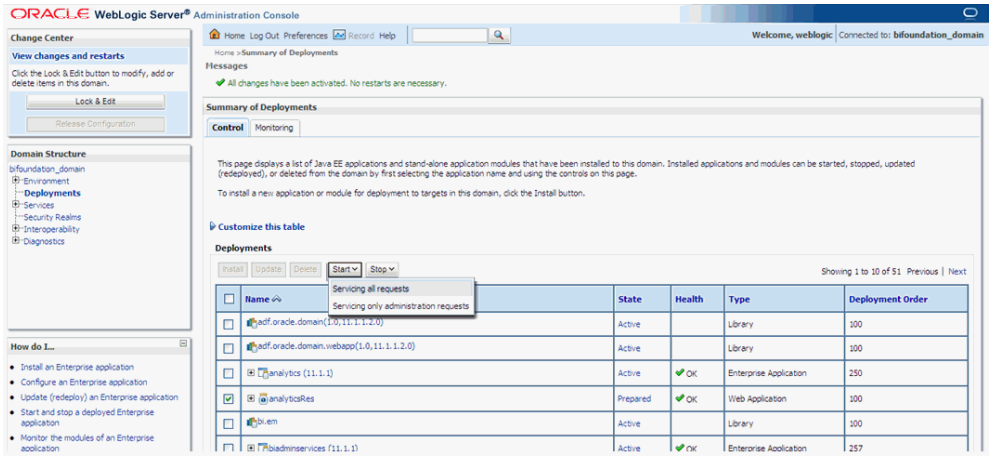
11. Click Finish.



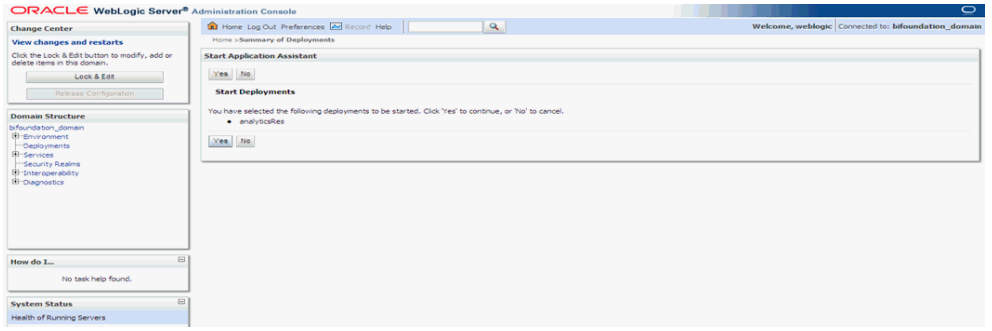
The 'analyticsRes' should appear under Deployments.



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

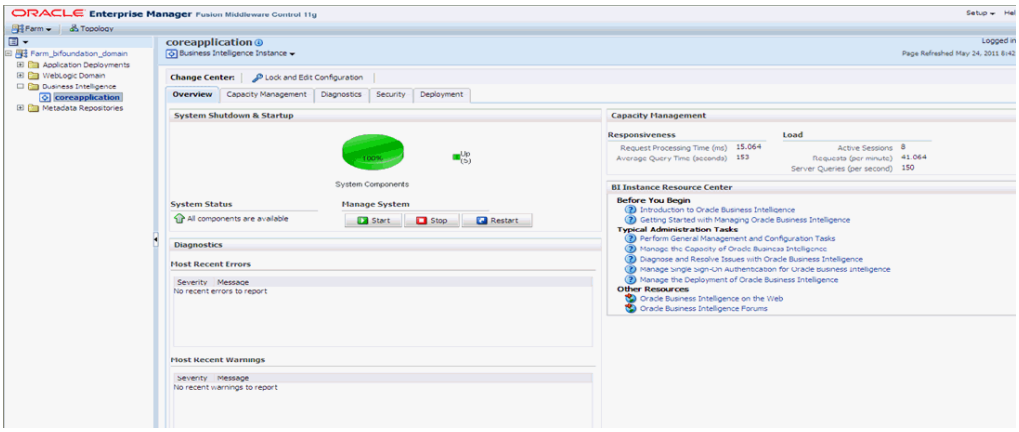


13. Start Application Assistant, and click Yes.



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.

2.7 Configuring SSO Using Oracle Access Manager 10g

Note: This section is only applicable if OAM 10g is used.

This section describes how to configure SSO in the Oracle Access Manager 10g (OAM 10g).

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.

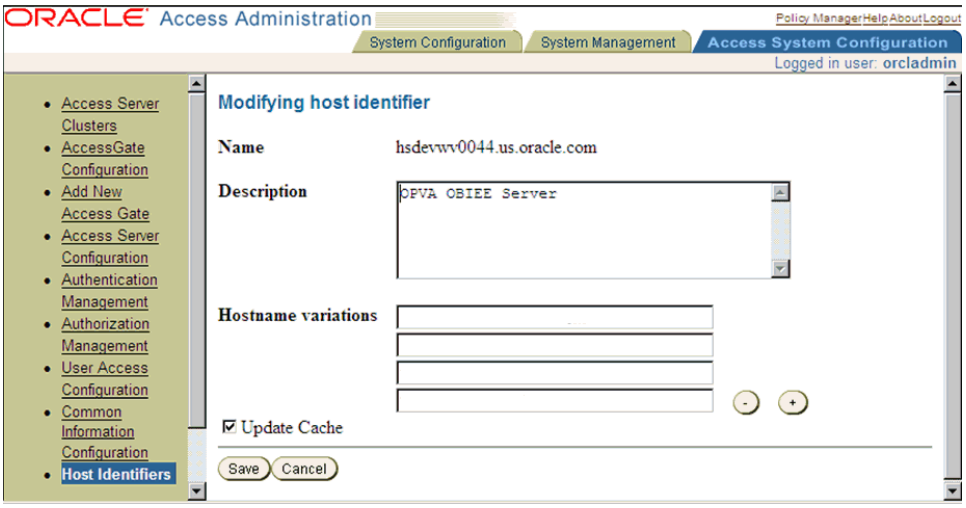
Perform the following steps to install SSO on the OAM:

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 Oracle Argus Analytics Web Tier machine. Click Save.

   For example:

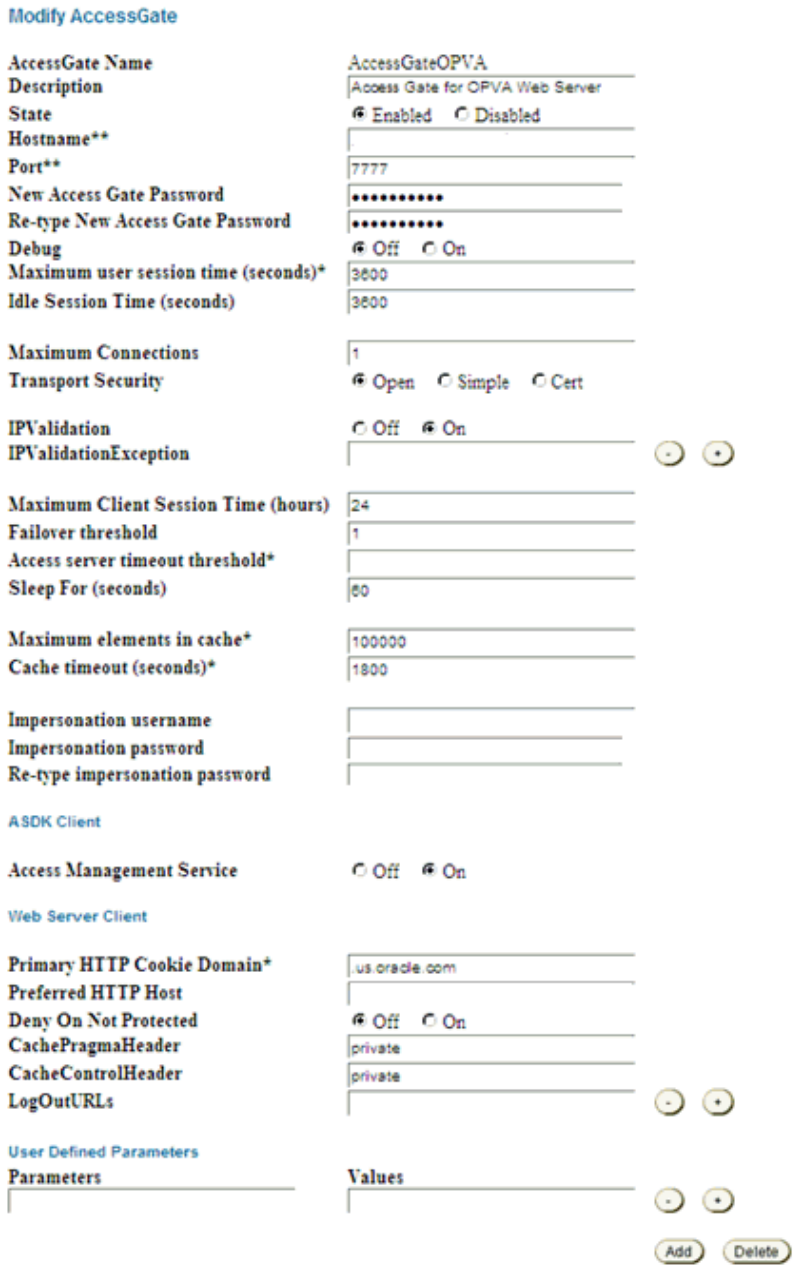
   - obiee_server.us.oracle.com
   - obiee_server.us.oracle.com:7777
   - <ip address>
   - <ip address>:7777

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



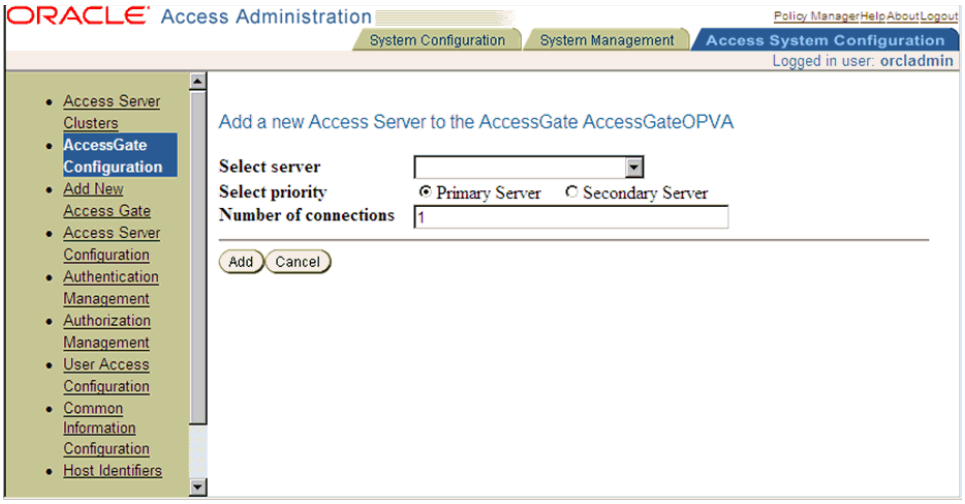
2. In the Access System console of OAM, click **Access System Configuration**.
3. Click **Add New Access Gate** link on the left panel.
4. Provide details like access gate name, port, and password. Also, enter the following details:
   - Hostname: Provide the FQDN of the Oracle Argus Analytics Web Tier 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.

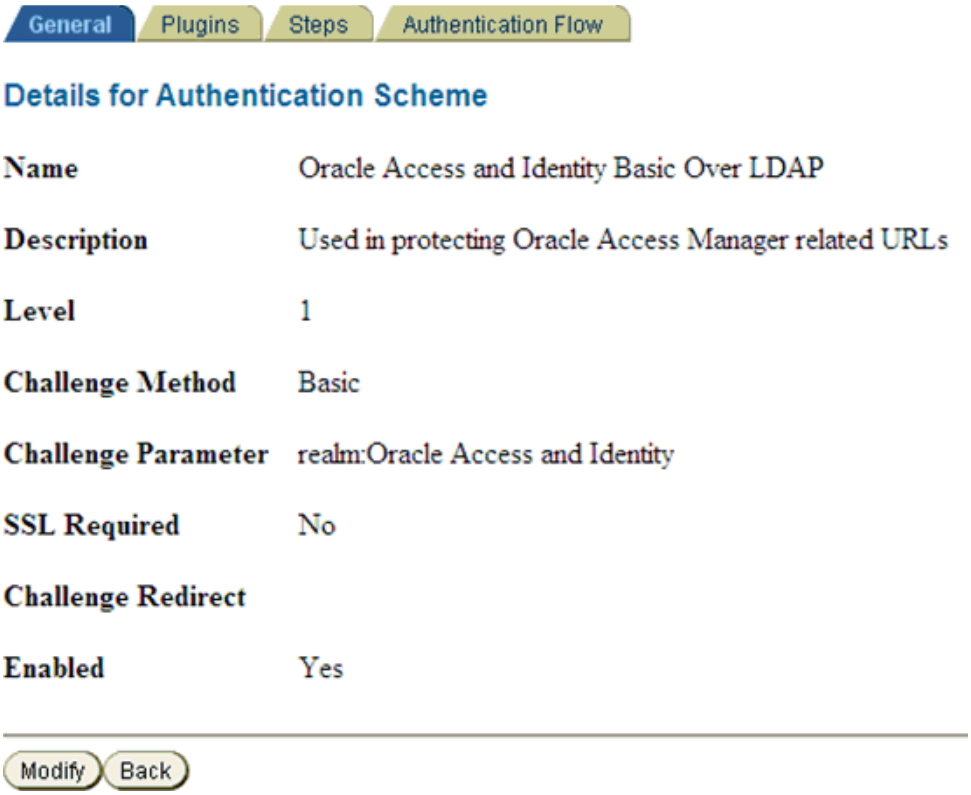
Figure 2–11 The Access System Configuration: Access Gate Configuration Screen



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.

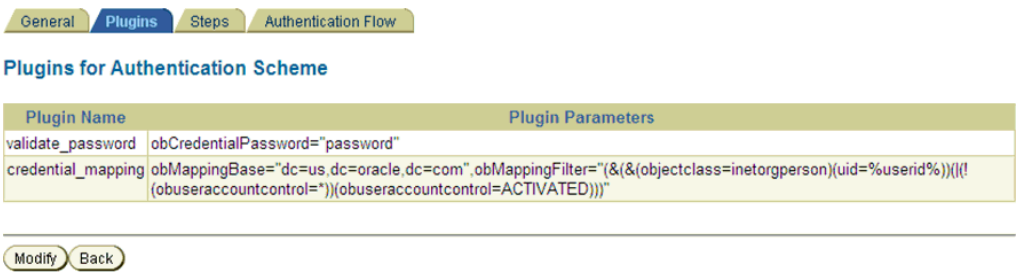
8. In the Access System Configuration Tab, click on Authentication Management and ensure that there is at least one schema for LDAP Authentication. If no schema exists, follow these steps:
   - Click on Add and enter the information as show here:

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

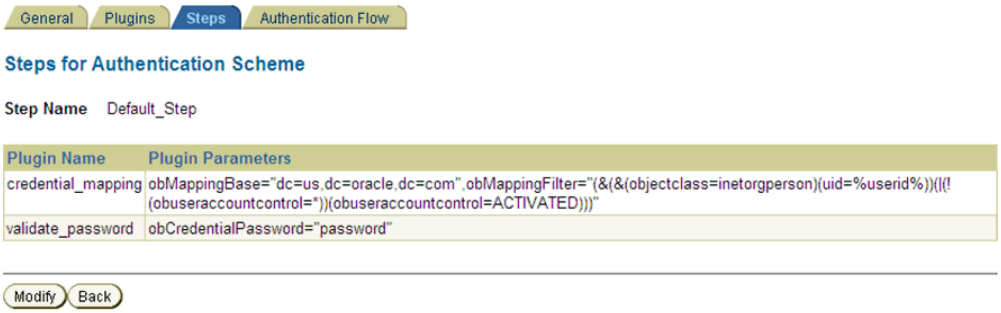


- Click on Save.
- Choose the Steps Tab next and add a new step 'Default_Step'. Add the 'Available Plugins' to the Active Plugins in the order:
  - credential_mapping

– validate_password

Note: The order of Plugins added is important.

Figure 2–14 Authentication Management: Steps tab

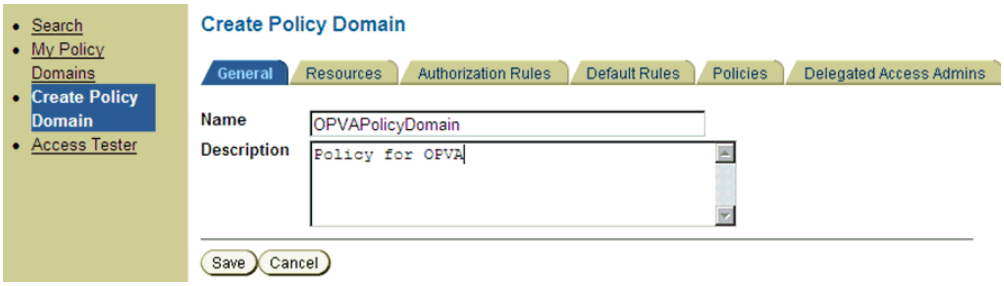


- Click on Save.
- Choose the Authentication Flow Tab and configure as shown below:

Figure 2–15 Authentication Management: Authentication Flow tab

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

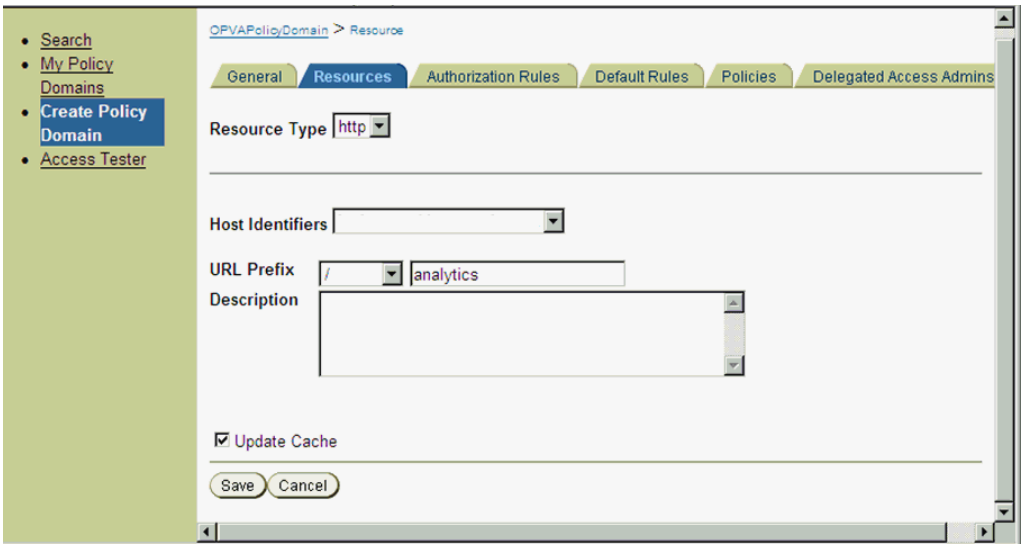
Figure 2–16 Create Policy Domain: General tab



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

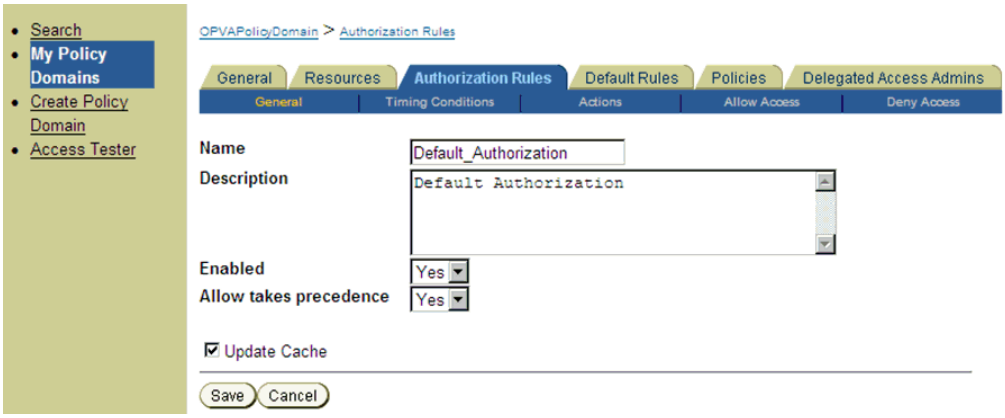
- Navigate to the 'Resources' tab and click on Add and enter details as shown here and click on Save:

Figure 2–17 Create Policy Domain: Resources tab



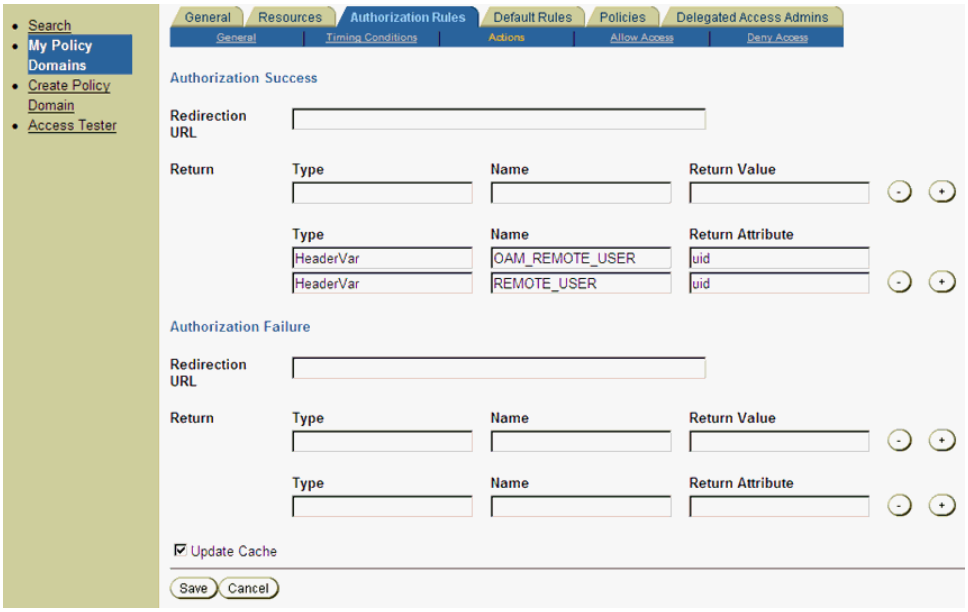
- Navigate to Authorization Rules and click on Add and enter details as given here and save the details:

Figure 2–18 My Policy Domains: Authorization Rules tab



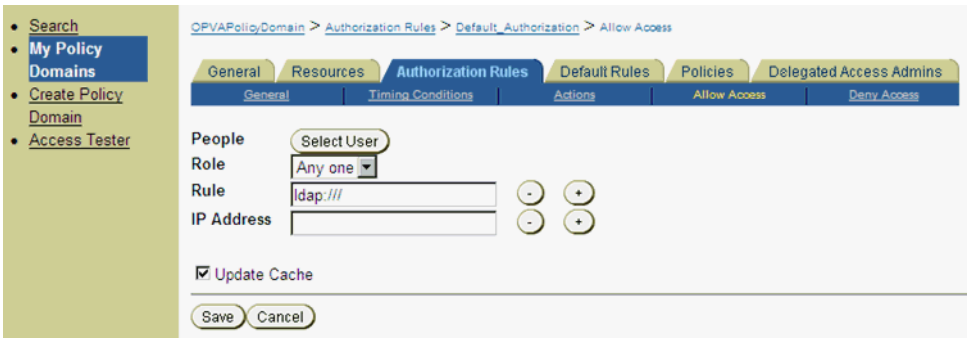
- Navigate to the Actions sub tab and click on add. Enter the details as shown here and click on Save:

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



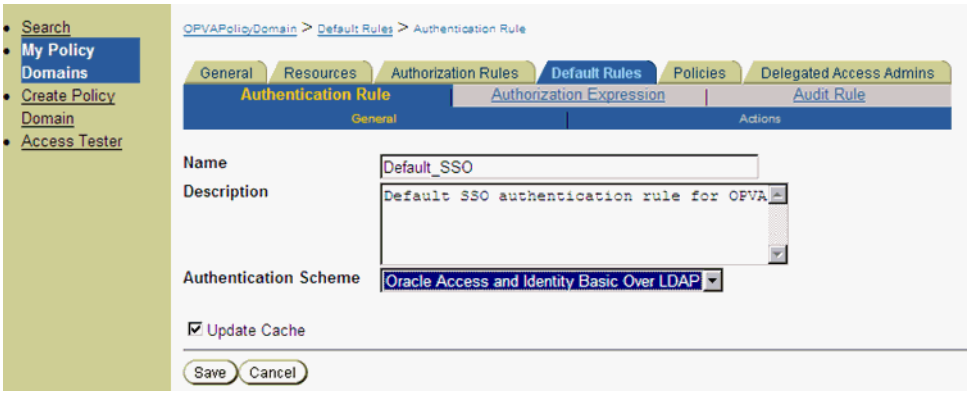
- After saving these details click on the Allow Access sub tab and click Add, enter the following details and click on Save:

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



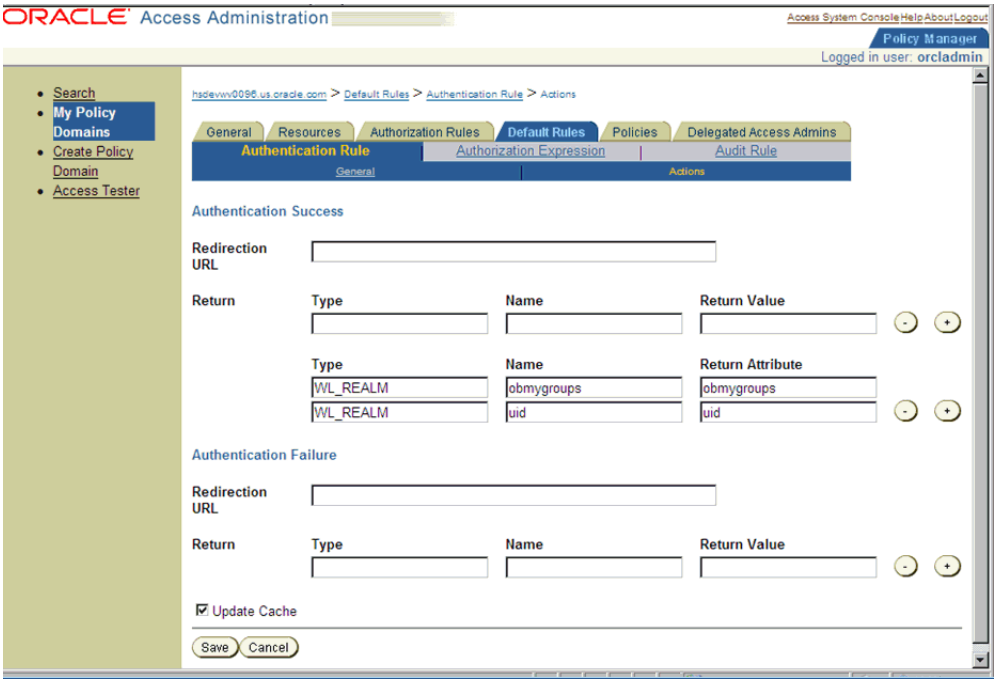
- Now click on Default Rules tab and add a new Authentication Rule by clicking on Add and entering information as given here in the General sub tab:

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



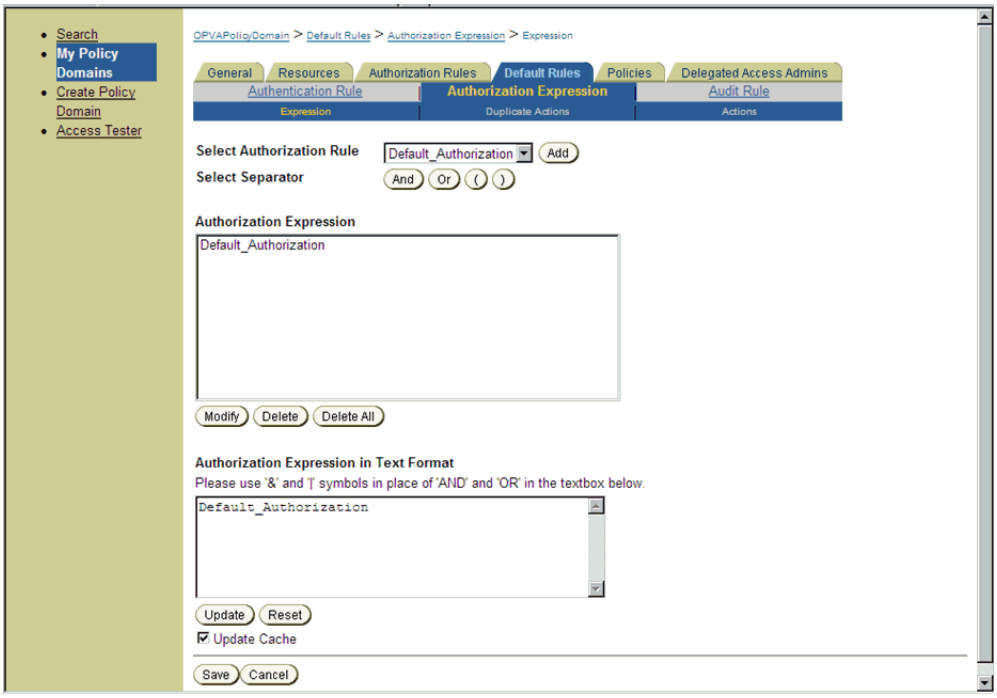
- Save the details in the General sub tab, and choose the Actions sub-tab.
- Click on Add and enter the details as shown here and save the details:

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



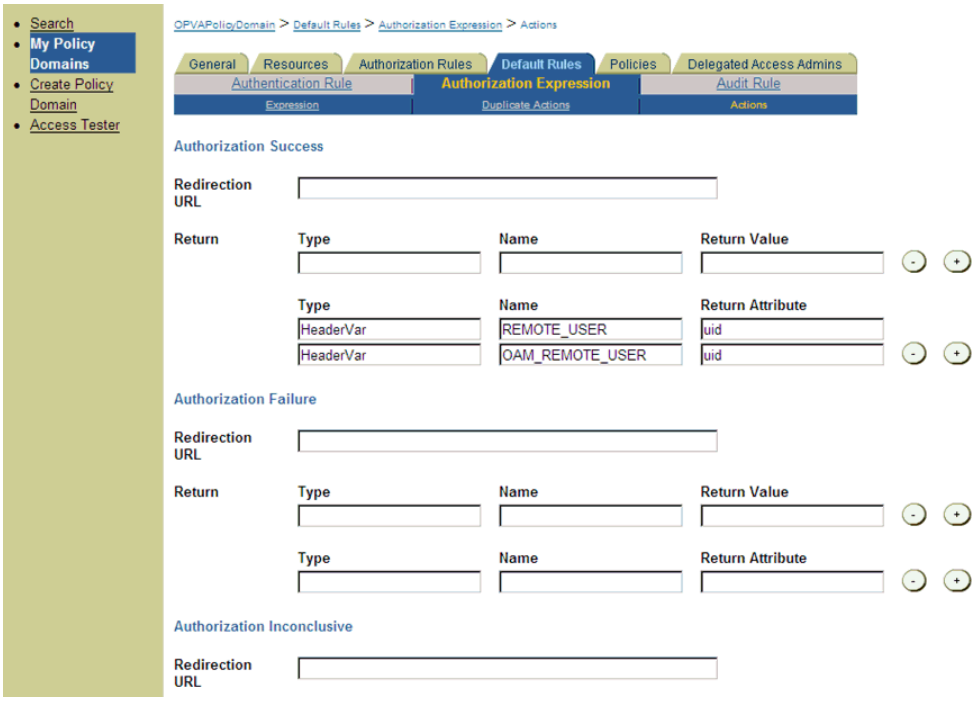
- Choose Authorization Expression tab and click on Add to add an entry per the details given here in the Expression sub tab:

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



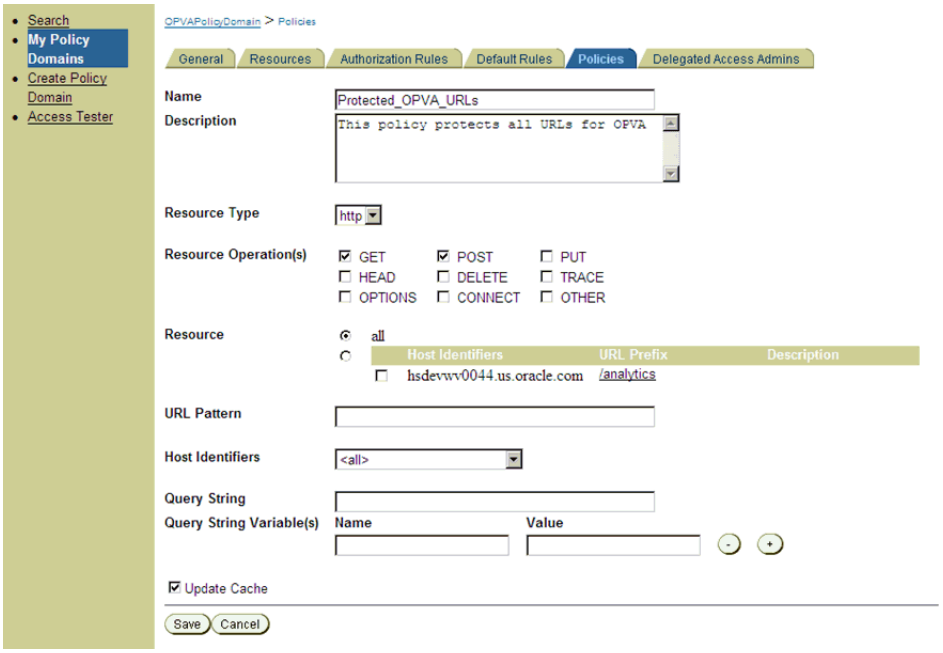
- Click on Save.
- Select the Actions sub tab and click on Add, enter the details as given here:

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



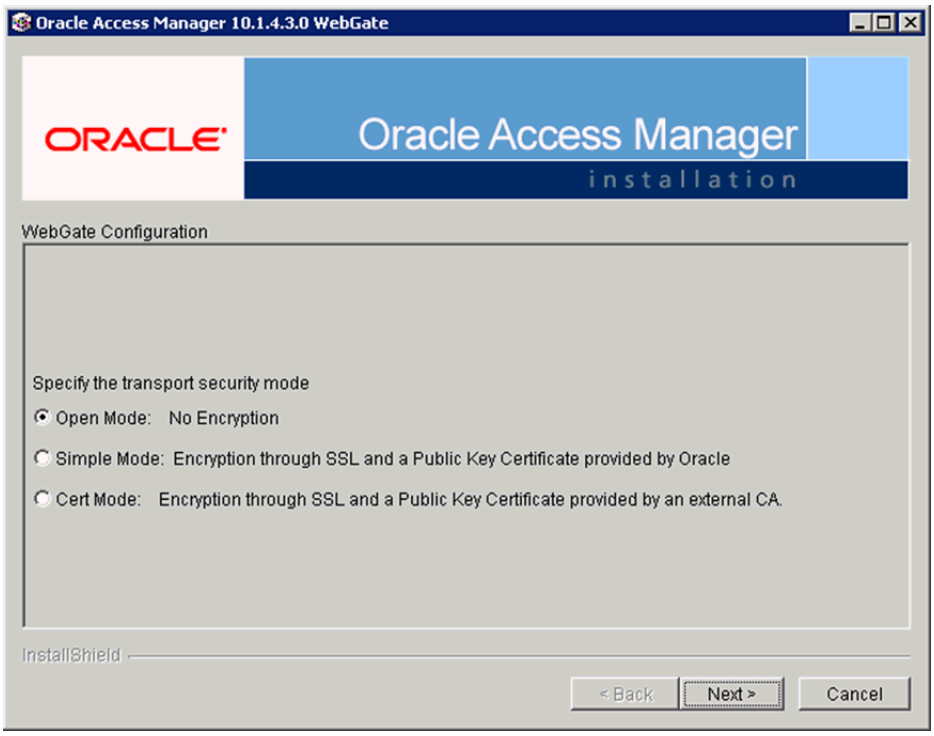
- Click on Save.
- Click on the Policies tab and choose the Add button, enter details as given here:

Figure 2–25 My Policy Domains: Policies tab



10. Navigate to the Oracle Argus Analytics Web Tier Machine, which is the machine where you have installed Oracle Argus Analytics 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

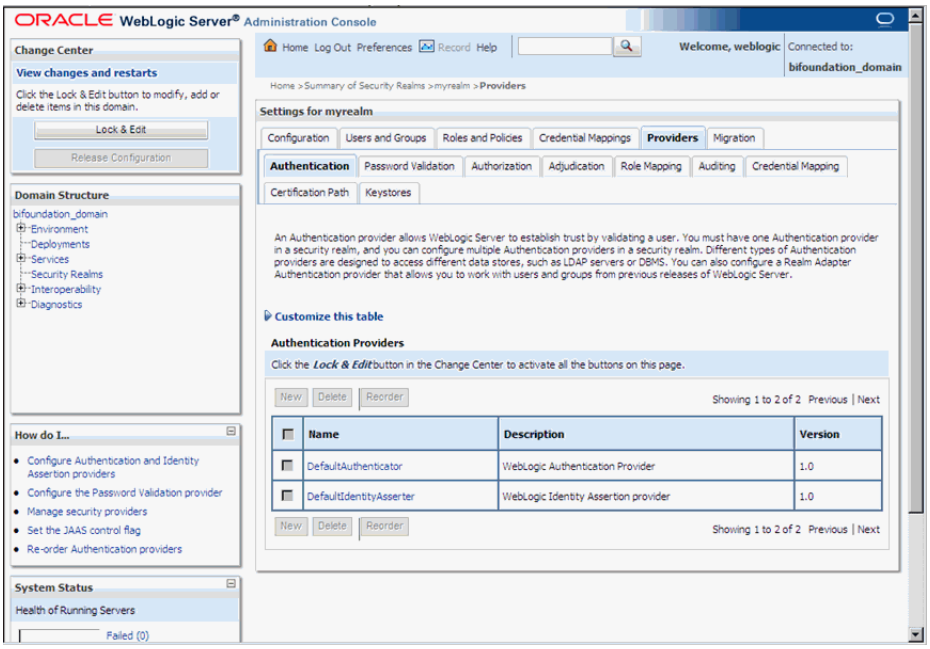
PathTrim /weblogic

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

- In the Providers tab, click Default Authenticator and change the Control Flag to Sufficient.
- 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

2.8 Configuring SSO Using Oracle Access Manager 11g

This section describes the steps to configure SSO in Oracle Access Manager (OAM) 11g.

Pre-requisites

The following are the pre-requisites to this task:

- There must be an OAM 11g installation configured to work with the desired LDAP (for example, OID), as the identity data-store.
- User profiles must exist in the LDAP server as well as in Argus Safety with the same credentials (login information).
- Oracle Web Tier 11.1.1.3 (or higher) must be installed on the same server where the OBIEE server is installed and configured with the Weblogic Server hosting OBIEE.
- Oracle Webgate 11g must be installed on the same server where the OBIEE server is installed, as mentioned above.

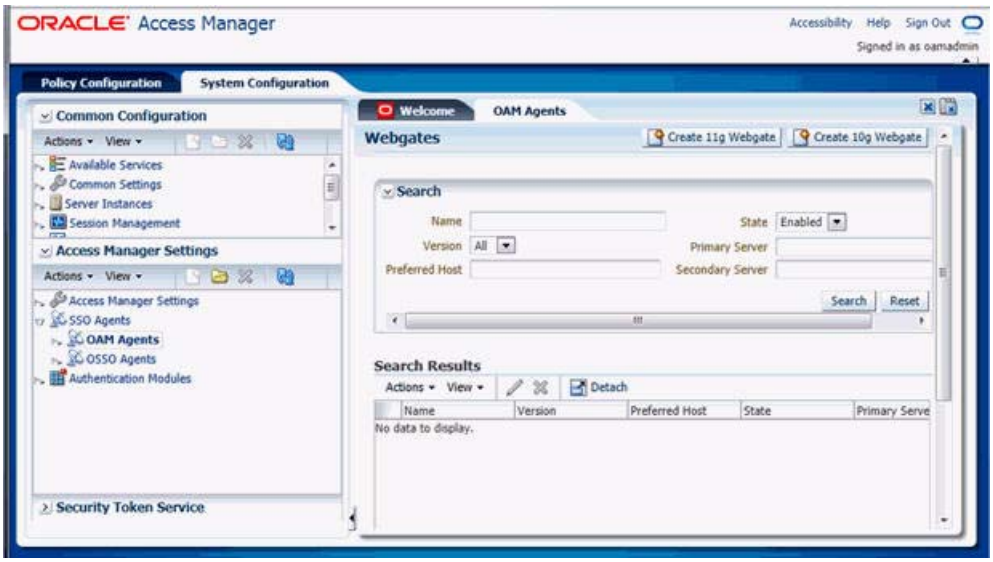
Installing SSO on OAM 11g

Execute the following steps to install SSO on OAM 11g:

1. Navigate to the OAM 11g OAM Console URL (http://oam_server:port/oamconsole) and login with the OAM Admin credentials.
2. Select the **System Configuration** Tab.
3. Select the **Access Manager Settings** sub menu in the left navigation window of the browser.

4. Double-click the **SSO Agents** > **OAM Agents** option to open the **OAM Agents** sub window.

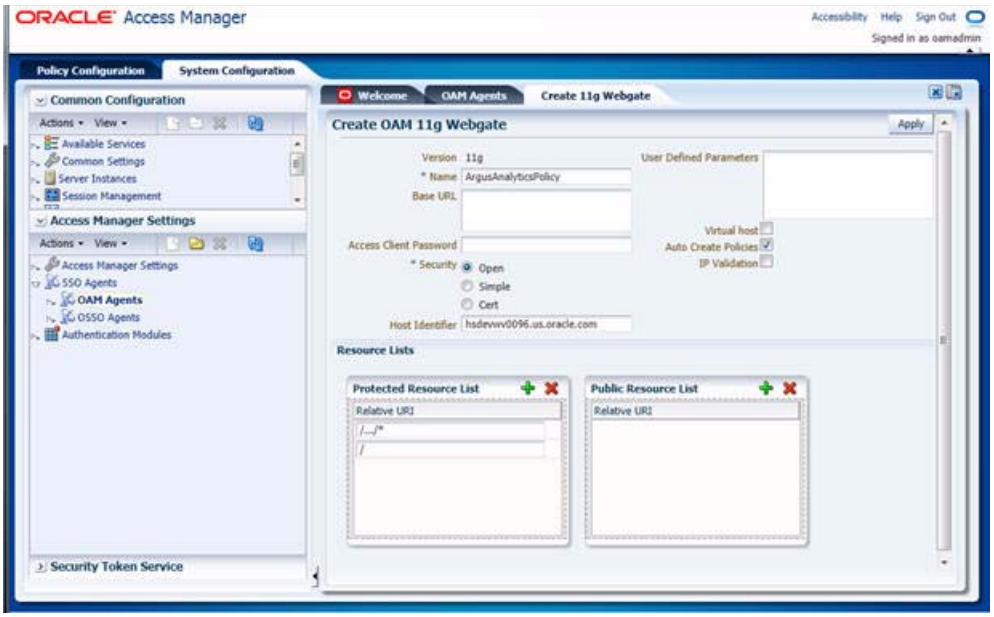
Figure 2–28 Viewing the OAM Agents Page



5. Click the **Create 11g Webgate** button and enter the following details:
   - **Name**: ArgusAnalyticsPolicy
   - **Security**: Open
   - **Host Identifier**: <obiee_server>
   - **Auto Create Policies**: Checked

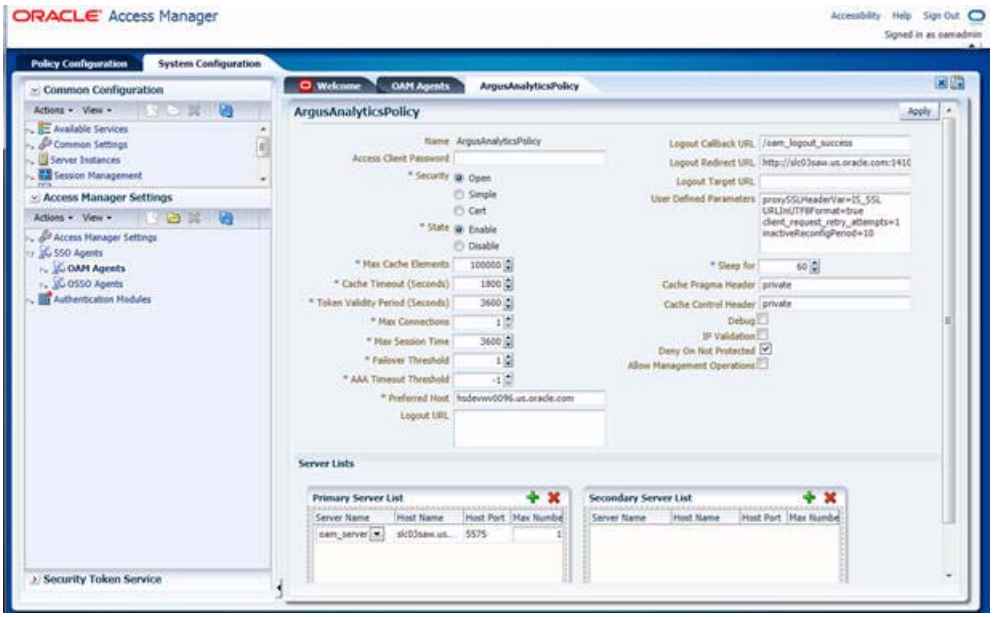
> **Note:** The <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate.

Figure 2–29 Create 11g Webgate Page



6. Click **Apply** to save and register the 11g Webgate and policies with OAM.
7. On the subsequent page, update the details for the **ArgusAnalyticsPolicy** created in the above step:
   - **Cache Pragma Header**: Private
   - **Cache Control Header**: Private

Figure 2–30 Updating Details for ArgusAnalyticsPolicy



8. Click **Apply**.
9. Navigate to the **Policy Configuration** tab.

10. Expand and double-click the **Shared Components** > **Resource Type** > **Host Identifiers** > <obiee_server> (For Example, hsdevwv0096.us.oracle.com) to open the **Host Identifiers** window and add the following details:
    - <obiee_server>
    - <obiee_server> <port>
    - <obiee_server_ip>
    - <obiee_server_ip> <port>

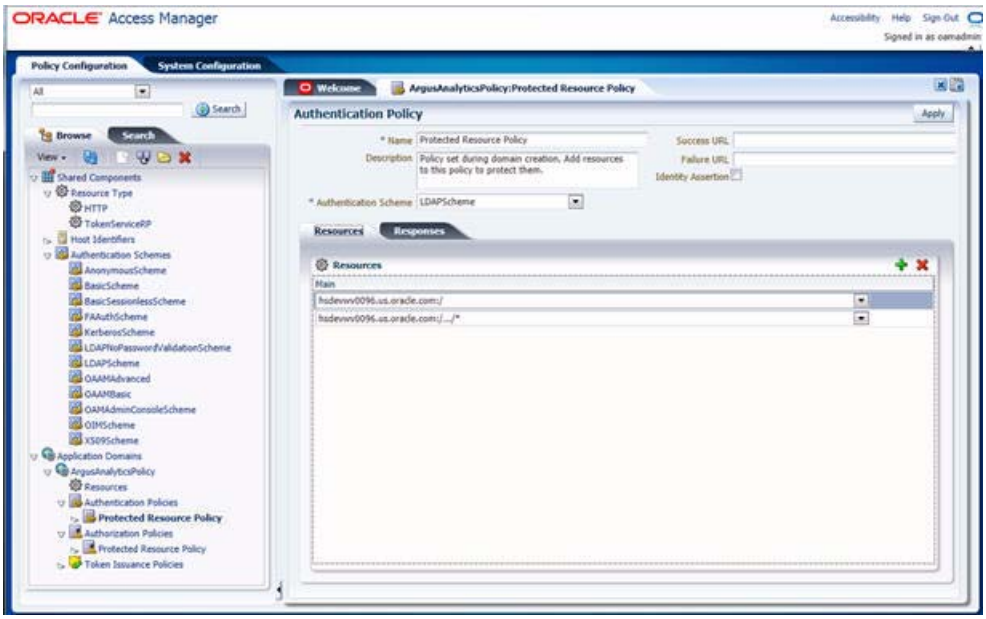
    Note: <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate. The port refers to the Oracle Web Tier Port.

    Example:

Hostname	Port
obiee_server.us.oracle.com	
obiee_server.us.oracle.com	7777
<ip address>	
<ip address>	7777

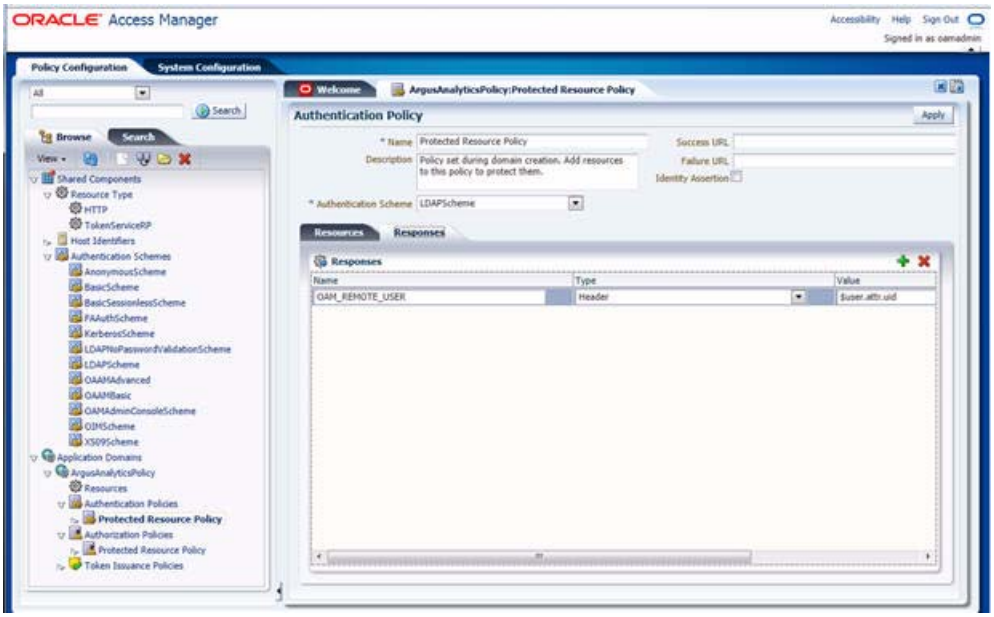
11. Expand and double-click **Application Domains** > **ArgusAnalyticsPolicy** > **Authentication Policies** > **Protected Resource Policy**.
12. Ensure that the Authentication Scheme is set as **LDAPScheme**.
13. Ensure that the following resources are present:
    - /
    - /…/*

Figure 2–31 Viewing the Authentication Protected Resource Policy



14. Add the following Response variables:
    - **Name**: OAM_REMOTE_USER
    - **Type**: Header
    - **Value**: $user.attr.uid [based on the LDAP schema setup]

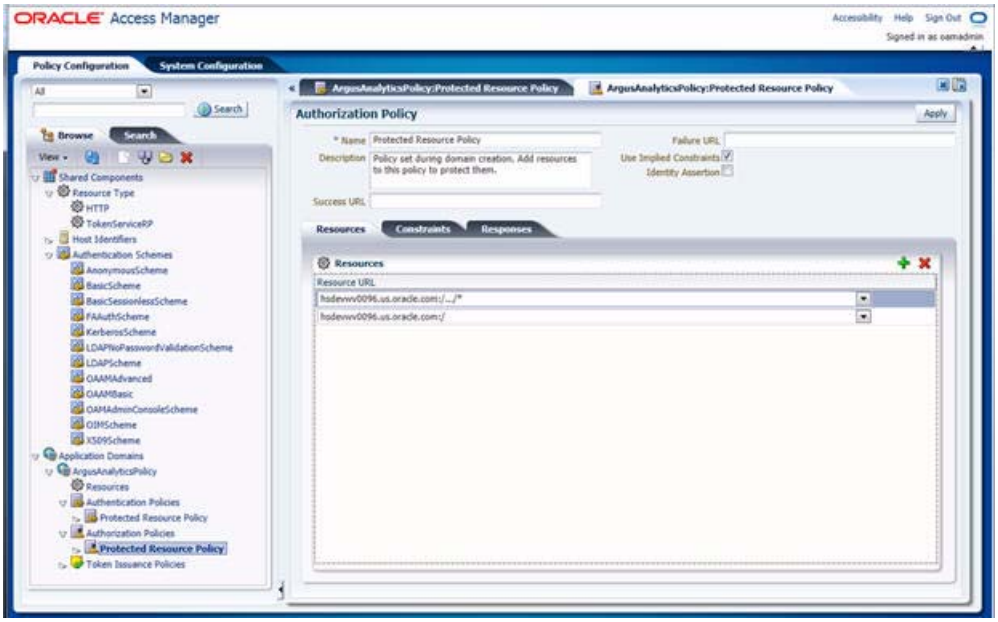
Figure 2–32 Adding the Response Variables to Authentication Protected Resource Policy



15. Click **Apply** and save the changes.
16. Expand and double-click **Application Domains** > **ArgusAnalyticsPolicy** > **Authorization Policies** > **Protected Resource Policy**

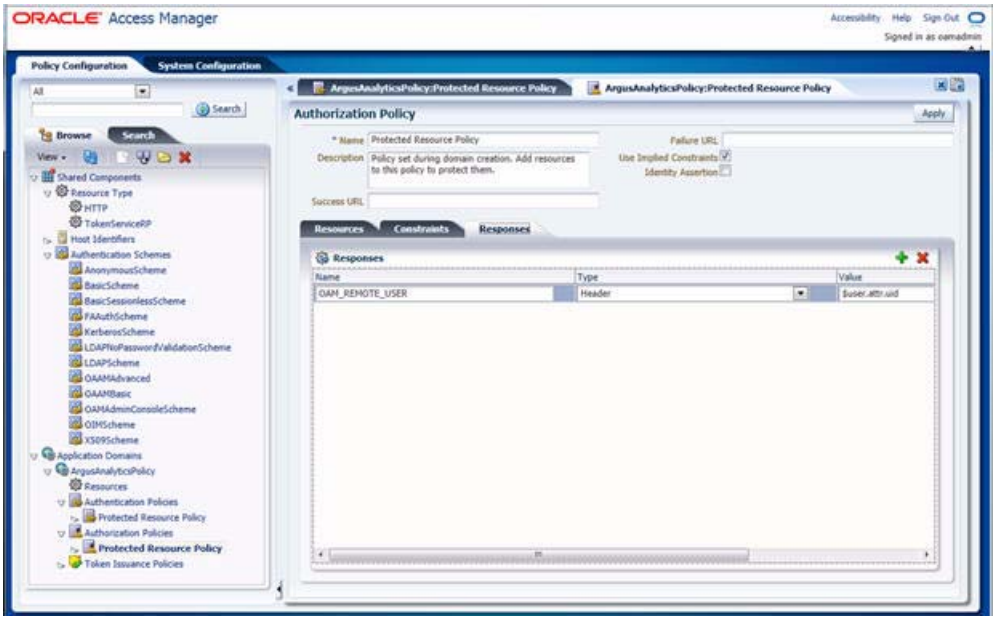
17. Ensure that the following resources are present:
    - /
    - /…/*

Figure 2–33 Viewing the Authorization Protected Resource Policy



18. Add the following Response variables:
    - **Name**: OAM_REMOTE_USER
    - **Type**: Header
    - **Value**: $user.attr.uid [as based on the LDAP schema setup]

Figure 2–34 Adding Response Variables to Authorization Protected Resource Policy



19. Click **Apply** to save the changes

20. Navigate to the OPVA Web Tier Machine [<obiee_server>], which is the machine where you have installed the OPVA OBIEE Server, and run the installer for Webgate (OFM Webgate 11g for OAM 11g) to complete the installation.

21. Configure the 11g Webgate using the following steps to communicate with the OAM 11g server:

    Note: Refer to the following link for advanced details:

    http://docs.oracle.com/cd/E21764_01/install.1111/e12002/webgate.htm

    ---

    a. Move to the following directory under your Oracle Home for Webgate:

       On UNIX Operating Systems:

       <Webgate_Home>/webgate/ohs/tools/deployWebGate

       On Windows Operating Systems:

       Webgate_Home>\webgate\ohs\tools\deployWebGate

    b. On the command line, run the following command to copy the required bits of agent from the **Webgate_Home** directory to the Webgate Instance location:

       On UNIX Operating Systems:

       ./deployWebgateInstance.sh -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>

       On Windows Operating Systems:

       deployWebgateInstance.bat -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home>

       Where **<Webgate_Oracle_Home>** is the directory where you have installed Oracle HTTP Server Webgate and created as the Oracle Home for Webgate, as shown in the following example:

       MW_HOME>/Oracle_OAMWebGate1

       The **<Webgate_Instance_Directory>** is the location of Webgate Instance Home, which is the same as the Instance Home of Oracle HTTP Server, as shown in the following example:

       <MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1

    c. Run the following command to ensure that the **LD_LIBRARY_PATH** variable contains <Oracle_Home_for_Oracle_HTTP_Server>/lib:

       On UNIX (depending on the shell):

       export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<Oracle_Home_for_Oracle_HTTP_Server>/lib

       On Windows:

       Set the <Webgate_Installation_Directory>\webgate\ohs\lib location and the <Oracle_Home_for_Oracle_HTTP_Server>\bin location in the PATH environment variable. Add a semicolon (;) followed by this path at the end of the entry for the PATH environment variable.

    d. From your present working directory, move up one directory level:

On UNIX Operating Systems, move to:

<Webgate_Home>/webgate/ohs/tools/setup/InstallTools

On Windows Operating Systems, move to:

<Webgate_Home>\webgate\ohs\tools\EditHttpConf

e. On the command line, run the following command to copy the **apache_webgate.template** from the **Webgate_Home** directory to the Webgate Instance location (renamed to webgate.conf) and update the **httpd.conf** file to add one line to include the name of **webgate.conf**:

On UNIX operating systems:

./EditHttpConf -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home> -o <output_file>

On Windows operating systems:

EditHttpConf.exe -w <Webgate_Instance_Directory> -oh <Webgate_Oracle_Home> -o <output_file>

Where **<Webgate_Oracle_Home>** is the directory where you have installed Oracle HTTP Server Webgate for Oracle Access Manager and created as the Oracle Home for Webgate, as shown in the following example:

<MW_HOME>/Oracle_OAMWebGate1

The **<Webgate_Instance_Directory>** is the location of Webgate Instance Home, which is the same as the Instance Home of Oracle HTTP Server, as shown in the following example:

<MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1

The **<output_file>** is the name of the temporary output file used by the tool, as shown in the following example:

Edithttpconf.log

f. Copy Generated Files (Artifacts) to the Webgate Instance Location from the OAM 11g server.

The 11g Webgate Agent (ArgusAnalyticsPolicy), which was created in the OAM 11g OAM Console earlier, would have also created the following artifacts on the OAM 11g server:

cwallet.sso

ObAccessClient.xml

This is based on the Security Mode that you have configured, which in this case is **Open**.
On the OAM 11g server, these files are present at the following location:

<OAM_FMW_HOME>/user_projects/domains/<OAM_domain>/output/ArgusAnalyticsPolicy

Copy these files to the <obiee_server> in the following directory:

<Webgate_Instance_Directory>/webgate/config directory [Example: <MW_HOME>/Oracle_
WT1/instances/instance2/config/OHS/ohs1/webgate/config]

g. Restart the Oracle HTTP Server Instance.

To stop the Oracle HTTP Server instance, run the following commands on the command line:

<MW_HOME>/Oracle_WT1/instances/instance2/bin/opmnctl stopall

To restart the Oracle HTTP Server instance, run the following commands on the command line:

<MW_HOME>/Oracle_WT1/instances/instance2/bin/opmnctl startall

22. Configure the HTTP Server as a reverse proxy for the WebLogic Server. To execute this, modify the **mod_wl_ohs.conf** file present at the following location:

OracleWebTierHome\instances\instance2\config\OHS\ohs1

The following 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

<Location /console>
   SetHandler weblogic-handler
   WebLogicHost hsdevwv0096.us.oracle.com
   WeblogicPort 7001
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>

<Location /em>
   SetHandler weblogic-handler
   WebLogicHost hsdevwv0096.us.oracle.com
   WeblogicPort 7001
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>

<Location /analytics>
```

```
  SetHandler weblogic-handler
  WebLogicHost hsdevwv0096.us.oracle.com
  WeblogicPort 9704
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

<Location /analyticsRes>
  SetHandler weblogic-handler
  WebLogicHost hsdevwv0096.us.oracle.com
  WeblogicPort 9704
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

<Location /xmlpserver>
  SetHandler weblogic-handler
  WebLogicHost hsdevwv0096.us.oracle.com
  WeblogicPort 9704
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>

</IfModule>

# <Location /weblogic>
#    SetHandler weblogic-handler
#    PathTrim /weblogic
#    ErrorPage  http:/WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>
```

Restart the Web Tier Instance in WebLogic EM or as described above.

23. Configure a new Authenticator for Oracle WebLogic Server on the OBIEE Server using the following steps:
    a. Login to the WebLogic Server Administrator Console and navigate to **Security Realms** > **myrealm**.
    b. Click the **Providers** tab.
    c. Click **Lock & Edit** on the right corner of the webpage, highlighted as Change Center.

d. Click **New** to create a new Authentication Provider and add the following details:

Name: OPVAOIDAuthenticator, or a name of your choice

Type: OracleInternetDirectoryAuthenticator

e. After saving the details, click the new Authenticator that you have created and enter the following details:

In the sub tab change the Control Flag as **SUFFICIENT**

f. Click **Save**.

g. Click the **Provider Specific** tab and enter the following required settings using values for your environment:

- **Host:** Your LDAP host.

  For example: oid_server.us.oracle.com

- **Port:** Your LDAP host listening port.

  For example: 3060

- **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**.

24. Configure a new Identity Asserter for WebLogic Server using the following steps:

a. In the Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm which you want to configure. For example, myrealm. Select Providers.

b. Click **New** and enter the following values in the fields:

Name: OPVAOAMIdentityAsserter, or a name of your choice

Type: OAMIdentityAsserter

c. Click **OK**.

d. Click on the newly created Asserter and set the Control Flag to **REQUIRED**.

e. Ensure that the Active Types that you have selected is **OAM_REMOTE_USER**.

f. Click **Save**.

g. Navigate to the **Provider Specific** tab and enter the following details:

- **Transport Security:** open
- **Application Domain:** ArgusAnalyticsPolicy, as set in the OAM 11g Console
- **Access Gate Name:** ArgusAnalyticsPolicy, as specified in the OAM 11g Console
- **Primary Access Server:** oam_server.us.oracle.com:5575, OAM 11g server with port
- Click **Save**.

h. 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 besides the list to order the following providers:

  OPVAOAMIdentityAsserter

  OPVAOIDAuthenticator

  DefaultAuthenticator

  DefaultIdentityAsserter
- Click **OK** to save your changes.

i. In the **Providers** tab, click **Default Authenticator** and change the Control Flag to **Sufficient**.

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

k. Restart Oracle WebLogic Server

25. The **BISystemUser** present in the default embedded LDAP must be deleted (using Security Realms in the **Administration Console** Link of the WebLogic Server) and the same/another user must be added in the newly added OID. This user also needs to be added to the BI Application Roles using the following steps:

a. Navigate to **Administration Console** > **Security Realms** > **myrealm** > **Users and Groups** > **Users** and select the checkbox against **BISystemUser** (from Provider: Default Authenticator)

b. Click **Delete**.

c. Navigate to **Security Realms** > **myrealm** > **Roles and Policies** > **Realm Roles.**

d. In the tree structure, expand **Global Roles** node and select the **Roles** link.

e. In the subsequent screen, click the **Admin Role** link

f. Click the **Add Conditions** button.

g. In the next screen, select the Predicate List as **User** and click **Next**.

h. In the **User Argument Name**, enter **BISystemUser** and click **ADD**.

i. Click **Finish**.

j. In the **Role Conditions** screen, ensure that the set operator is set to **Or**.

k. Save the configuration.

l. Navigate to the Enterprise Manager of OBIEE or the Fusion Middleware Control page and navigate in the tree structure to the **Business Intelligence** > **coreapplication** node.

m. In the Business Intelligence drop-down menu, select **Security** > **Application Roles**.

n. 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.

o. Add the trusted user's credentials to the oracle.bi.system credential map.

p. Using Fusion Middleware Control target navigation pane, navigate to **farm** > **WebLogic Domain**, and select **bifoundation_domain**.

- Using the WebLogic Domain menu, select **Security** > **Credentials.**
- Open the oracle.bi.system credential map, and select **system.user**.
- Click **Edit**.
- In the **Edit Key** dialog box, enter **BISystemUser** (or the name that you have 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**.

q. Restart the Managed Servers.

26. Enable the SSO Authentication in the Weblogic Server for OBIEE using the following steps:

a. Login to Fusion Middleware Control (EM) of the WebLogic Server.

b. Go to the **Business Intelligence Overview** page.

c. Go to the **Security** page.

d. Click **Lock and Edit Configuration**.

e. Check **Enable SSO,** this makes the SSO provider list active.

f. Select the configured SSO provider from the list, as **Oracle Access Manager**.

g. In **The SSO Provider Logoff URL**, specify the following URL:

http://<oam_server>:14100/oam/server/logout

h. Click **Apply**.

i. Click **Activate Changes**.

j. Restart the Oracle Business Intelligence components using Fusion Middleware Control.

2.9 Configuring SSL for Oracle Argus Analytics in OBIEE

Enable the default SSL configuration in OBIEE using the following steps:

1. Open the WLS Administrator console for OBIEE.
2. Navigate to **Environments** > **Servers** in the tree view displayed in the left pane.

3. Click **Lock & Edit** button for changing the configuration.
4. Click the **AdminServer(admin)** link and enable the SSL listen port in the **Configuration > General** tab by checking the **SSL Listen Port Enabled** checkbox.
5. Click **Save**.
6. In the **Servers** window, click **bi_server1** (or the link for the OBIEE Managed server which you have configured).
7. In the **Configuration** > **General** tab, enable the SSL Listen Port for the OBIEE server as well by checking the **SSL Listen Port Enabled** checkbox.
8. Select **Configuration/General** tab > **Advanced**.
9. Check the **WebLogicPluginEnabled** checkbox.
10. Click **Save**.
11. Click **Clusters** in the **Environment** section.
12. Click each Cluster name.
13. On the **Configuration/General** tab, click the **Advanced** option.
14. Check the **WebLogicPluginEnabled** checkbox and save the changes.
15. Activate the changes.
16. Edit the **setDomainEnv.cmd** file present in the <OracleBIHome>\user_projects\domains\bifoundation_domain\bin location and add the below entry to the file at the end.

    Note: Edit the Path names according to your installation directories where <OracleBIHome> refers to the Oracle BI Home directory (installed location)

    set JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.net.ssl.trustStore="<OracleBIHome>/wlserver_10.3/server/lib/DemoTrust.jks" -Djavax.net.ssl.trustStorePassword=""

17. Edit the **StartStopServices.cmd** present at the following location:

    <OracleBIHome>\instances\instance1\bifoundation\OracleBIApplication\coreapplication

    set wls.mgd.port=<ssl_port>

    set BI_URL=https://%wls.host%:%wls.mgd.port%/analytics

18. Restart all the Weblogic and the Managed BI Servers.
19. Login to EM.
20. Select **Weblogic Domain** > **System MBean Browser**.
21. Lock the **BIDomain MBean** (**oracle.biee.domain** > **Domain: bifoundation_domain** > **BiDomain** > **BIDomain**), to make changes by selecting the **BIDomain** in System MBean Browser.
22. In the **Operations** tab, click the **Lock** operation, and click **Invoke**.
23. Click **Return**.
24. Select **BIDomain > BIInstance > SecurityConfiguration** in System MBean browser.

25. Click **generateSSLCertificates** in the **Operations** tab.
26. Update the information passphrase, webServerCACertificatePath, and certificateEncoding, using the following details:
    - **passphrase:** <passphrase>
    - **webServerCACertificatePath:** <OracleBIHome>\wlserver_10.3\server\lib\CertGenCA.der
    - **certificateEncoding:** der
27. Click **Invoke**.
28. Select **BIDomain Mbean** in System Mbean browser and click **simpleCommit**.
29. Click **Invoke**.
30. Verify that SSL has been set by navigating to **Weblogic Domain** > **Security** > **Credentials** and check if the SSL credentials have been saved to the credential store. If successful, the following SSL credentials display in the oracle.bi.enterprise credential map:
    - ssl.java.private.key
    - ssl.java.public.certificate
    - config.version
31. Lock the **BIDomain MBean** again as mentioned above.
32. Navigate to **MBean BIDomain > BIInstance > SecurityConfiguration** in the System Mbean browser and update SSLEnabled attribute to **true** in the list of attributes.
33. Select **BIDomain Mbean** in System Mbean browser and click **simpleCommit**.
34. Click **Invoke**.
35. Restart the OBIEE system components.
36. To verify the SSL Configuration is successful, select **BIDomain > BIInstance > SecurityConfiguration** in the System Mbean browser.
37. Click **runSSLReport** operation and it should report the status as **OK**.

Note: For detailed information on Configuring SSL Certificates in OBIEE 11g, refer to the following guides:

- Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1) section - SSL Configuration in Oracle Business Intelligence
- OBIEE11g SSL Setup and Configuration [ID 1326781.1 in Oracle Support Website]

2.10 Configuring SSL for SSO in Oracle Argus Analytics with OAM 11g

To configure SSL for SSO in Argus Analytics with OAM 11g, execute the following steps:

- Configure OBIEE in SSL mode as given in the previous section: Configuring SSL for Oracle Argus Analytics in OBIEE

- Follow the steps as mentioned in the Configuring SSO Using Oracle Access Manager 11g section, except for the deviations as mentioned here:

  Update/Create the Webgate Registration in OAM 11g, which you have created in the Configuring SSO Using Oracle Access Manager 11g section.

  Note: The OAM Server configured in OAM 11g must be running with Security set to **Simple**, else it does not let you create a Webgate with Security set as **Simple**.

  – Open the OAM 11g OAM Console.

  – Navigate to the **Policy Configuration** tab.

  – Expand and double-click **Shared Components** > **Resource Type** > **Host Identifiers** > **<obiee_server>** (for example, oamserver.tmp.domain.com) to open the Host Identifiers window and add the following details in addition to the ones that are already present:

  <obiee_server>

  <obiee_server> <ssl port>

  <obiee_server_ip>

  <obiee_server_ip> <ssl port>

  Note: **<obiee_server>** refers to the server, where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate. The <ssl port> refers to the Oracle Web Tier SSL Port.

  – Click **Apply**.

  – From the **System Configuration** tab, access the **Manager Settings** section, expand the **SSO Agents** node, and expand **OAM Agents**.

  – On the **Search** page, define your criteria in the **Name** field as **ArgusAnalyticsPolicy** and click **Search**.

  – In the Search results, click **ArgusAnalyticsPolicy** to edit the Agent Registration.

  – Locate the Security options and click **Simple**.

  – Click **Apply** to submit the changes.

  – This generates the artifacts again or afresh. Copy the generated Files (Artifacts) to the Webgate Instance Location from the OAM 11g server.

  The 11g Webgate Agent (ArgusAnalyticsPolicy), which is updated/created in the OAM 11g OAM Console, also creates the following artifacts on the OAM 11g server:

  cwallet.sso

  ObAccessClient.xml

  aaa_cert.pem

  aaa_key.pem

  password.xml

This is based on the Security Mode that you have configured, which in this case now is **Simple**. On the OAM 11g server, these files are present at the following location:
<OAM_FMW_HOME>/user_projects/domains/<OAM_domain>/output/ArgusAnalyticsPolicy.

Copy the **password.xml**, **cwallet.sso**, and **ObAccessClient.xml** files to the **<obiee_server>** in the <Webgate_Instance_Directory>/webgate/config directory (Example: <MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1/webgate/config)

Copy the **aaa_cert.pem** and **aaa_key.pem** files to the **<obiee_server>** in the <Webgate_Instance_Directory>/webgate/config/simple directory (Example: <MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1/webgate/config/simple)

– Restart the OAM Server

- The Oracle Web Tier is configured with OBIEE as a reverse proxy, as mentioned in step 22 of the Configuring SSO Using Oracle Access Manager 11g section. In addition to those steps, you also need to enable SSL for the Oracle Web Tier using the following steps:

  a. Locate and edit the <ORACLE_WT_INSTANCE>/config/OHS/ohs1/ssl.conf

  b. Find the **VirtualHost** section and ensure the following entry is present:

  SSLWallet "${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/default"

  c. Save the file and restart the HTTP Server.

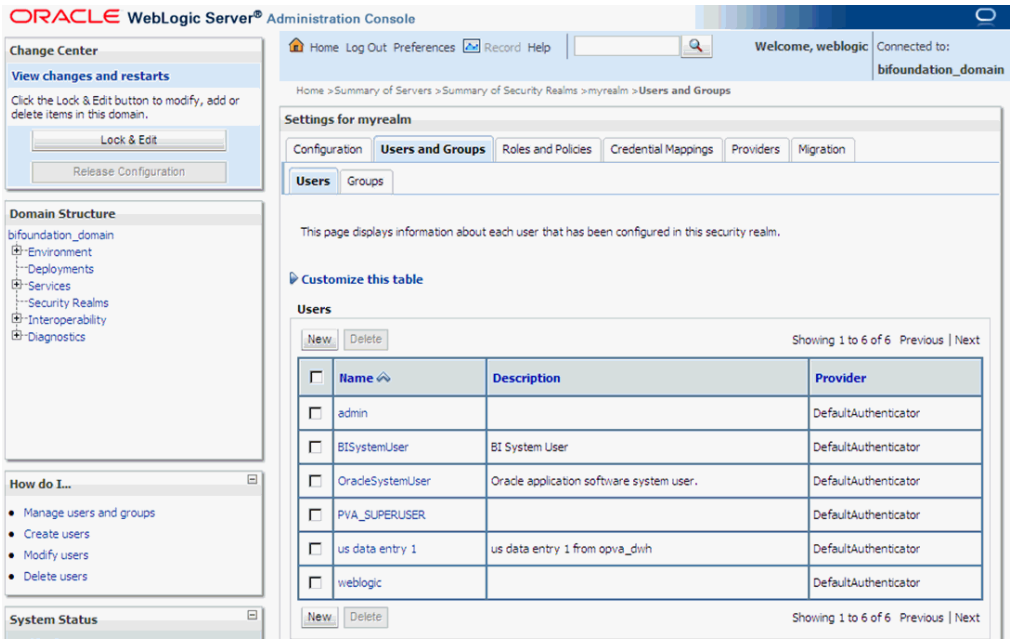
2.11 Creating Users and Groups in Oracle Argus Analytics

2.11.1 Creating Groups for Oracle Argus Analytics 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 Oracle Argus Analytics. If not using the embedded LDAP then these groups should be created in the external LDAP provider.

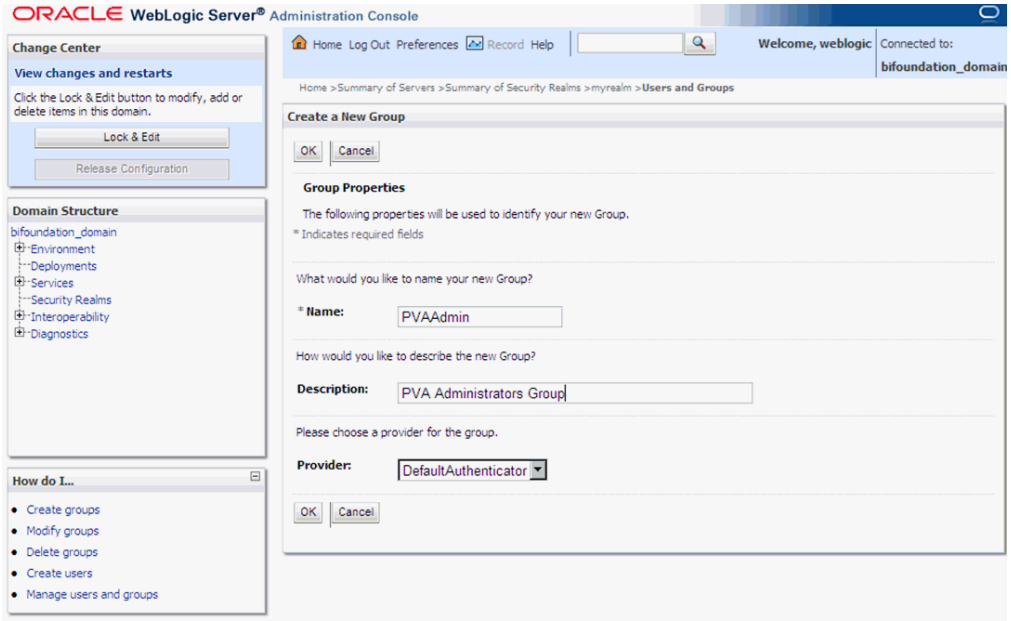
1. Open a new browser window for the WebLogic Administration Console.
2. Navigate to Security Realms -> myrealm -> Users and Groups tab.

Figure 2–35 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 2–36 myrealm Settings: Groups tab: New Group



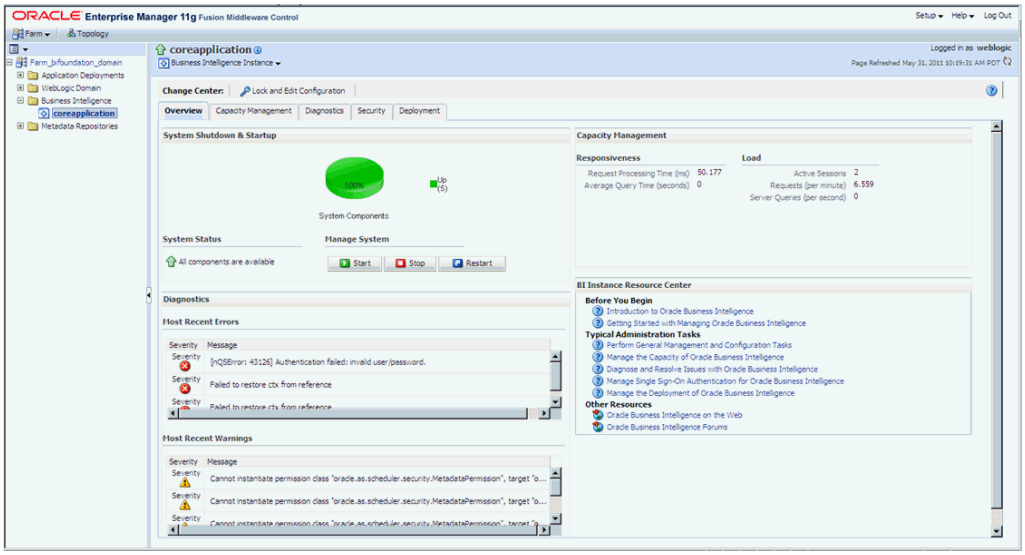
5. Follow the above process to create the groups 'PVASafetyGroup' and 'PVASafetyConsumersGroup'.

2.11.2 Assigning OBIEE Application Roles for Oracle Argus Analytics Groups

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

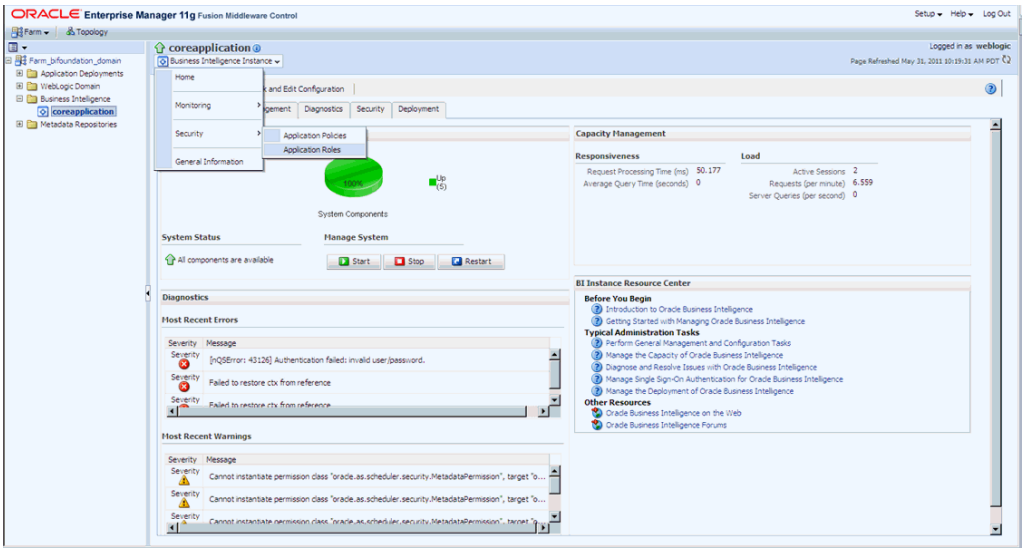
1. Start a new browser window for the Enterprise Manager for Fusion Middleware Control and navigate to the Business Intelligence -> coreapplication overview page as shown here:

Figure 2–37 coreapplication Screen



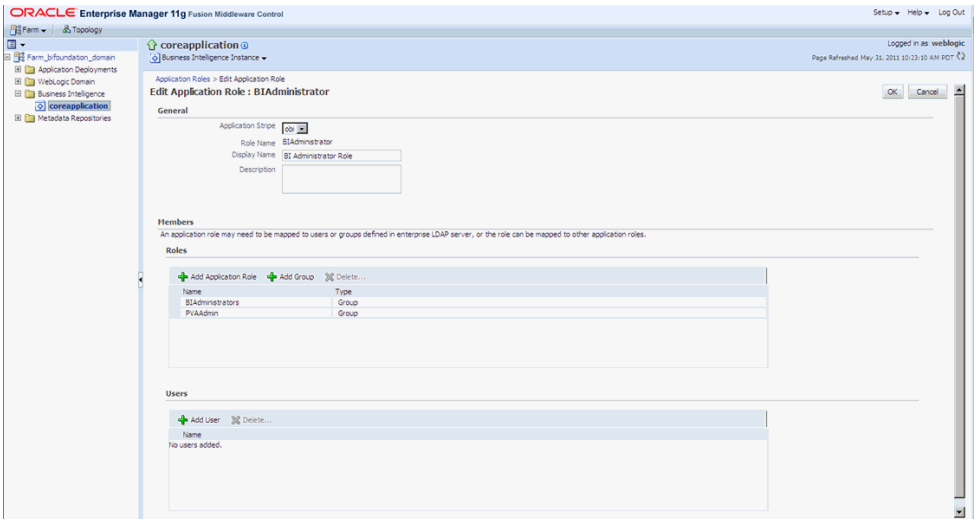
2. Invoke the Application Roles by choosing from the menu drop down at Business Intelligence Instance -> Security -> Application Roles

Figure 2–38 coreapplication: Application Roles Screen



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

Figure 2–39 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 2.13, OBIEE Default Application Roles for a list of privileges present as per the BIApplication Role specified above.

2.11.3 Creating Users for Oracle Argus Analytics 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 Oracle Argus Analytics. 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.

IMPORTANT: The users created for Argus Analytics should have the same login name as the Argus Safety application users created in Argus Safety application through the:

Argus Safety Web Application > Access Management > Argus > Users menu

This is a vital step and needs to be adhered to, as Argus Analytics implements Row Level Security in the Warehouse Data at the Enterprise Level, Case Processing Site Level, Study Level and Product Level as present/configured in the Argus Safety Application it is installed with.

This information for each specific Argus Safety User access in the Argus Safety Application is brought over to the Argus Analytics Warehouse via the ETLs.

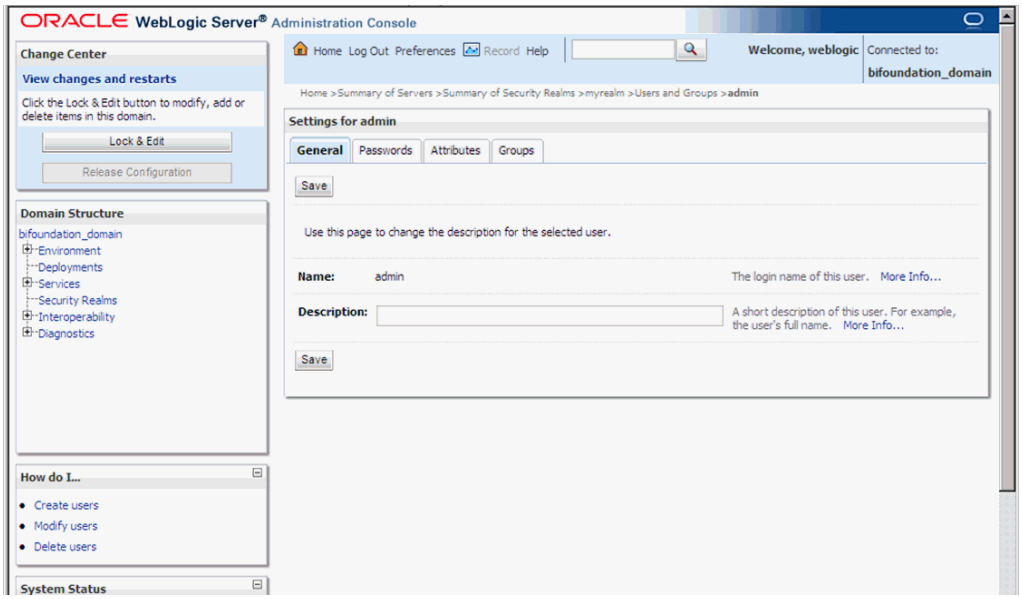
At the time of logging into the Argus Analytics OBIEE web URL the AN application verifies if the logged user is a valid user in Argus Safety Application as well and implements the Row Level Security according to the access prevailing for the user in the Argus Safety Application.

Failing this will result in errors in the Dashboards and Answers page as the session variables will not get initialized accordingly.

If you view certain errors while accessing reports, you can refer to Appendix C of the User Guide.

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 2–40 Administration Console: General tab



7. Click the 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).

> **Note:** For Oracle Argus Analytics on a very large database with more than a million cases, it is best to enforce the end users to store customizations for the Personal User dashboard.
>
> This enables users to select a default product and enables better response time for the queries submitted to the warehouse.

Execute the following steps to store the customizations for the Personal User dashboard:

1. Log in to the OBIEE application using the credentials of the newly created user.
2. Navigate to the dashboard. Example: Menu > Dashboards > Personal User Dashboard.
3. Go to the Personal User Case History page.
4. Select a Product Name and click Apply.
5. On the Page Options menu that is displayed on the right, click the Save Current Customization option.
6. Enter an appropriate name for this customization.
7. Check the 'Make this my default for this page' checkbox to make it your default customization option.
8. Click OK.

By following the steps listed above, the selected filter is always applied on initial load of the Dashboards page. Repeat these steps for every Dashboard page in case of longer response time.

2.11.4 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 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.
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.

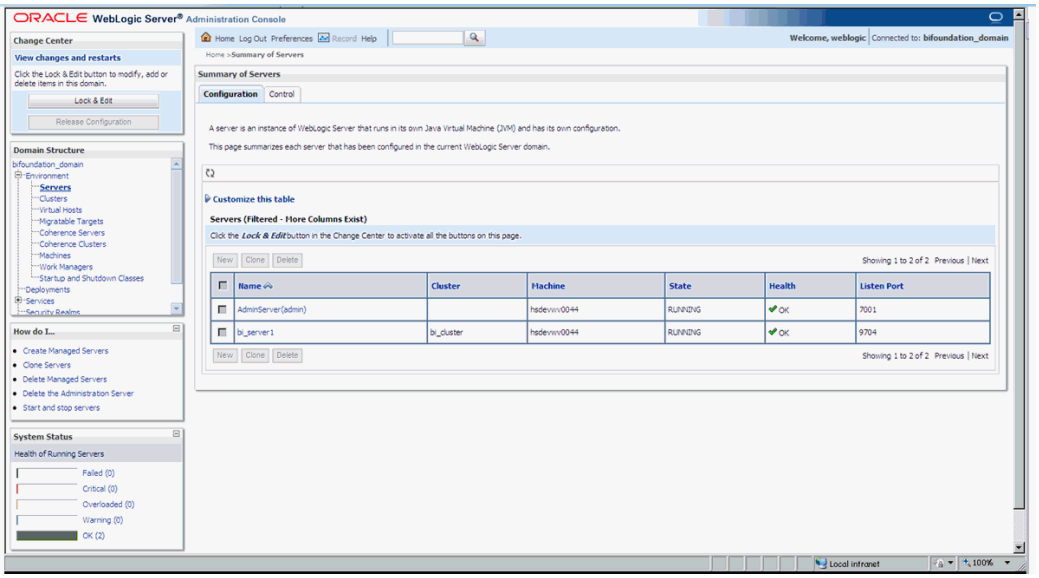
Note: It is recommended to create at least one user to be added with the Administrator Role in DAC to manage the DAC PVA metadata.

2.12 Configuring SSL for Oracle Argus Analytics in OBIEE

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

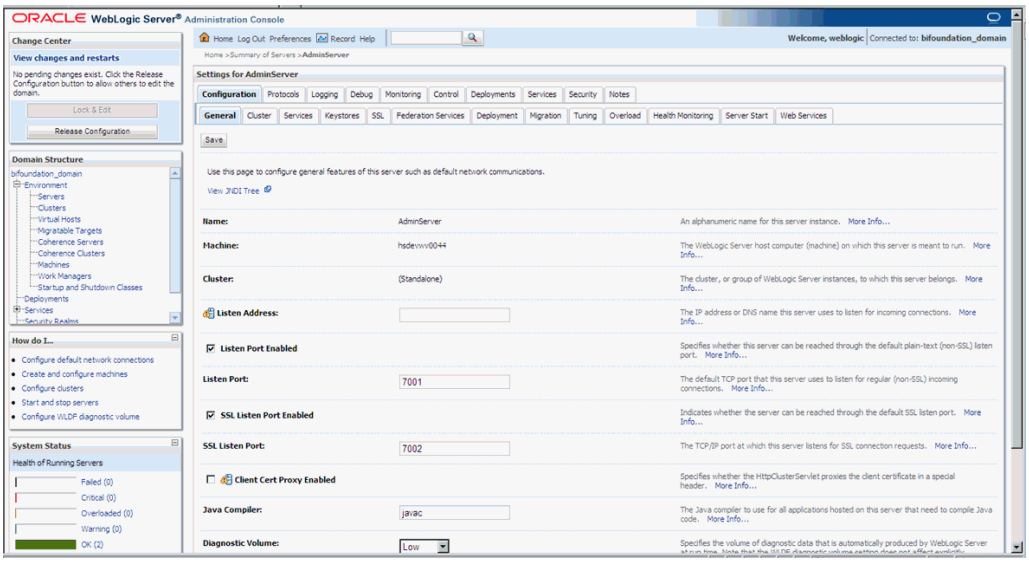
1. Open the WLS Administrator console for OBIEE.
2. Navigate to Environment -> Servers in the tree view displayed on the left side.

Figure 2–41 Servers: Configuration tab



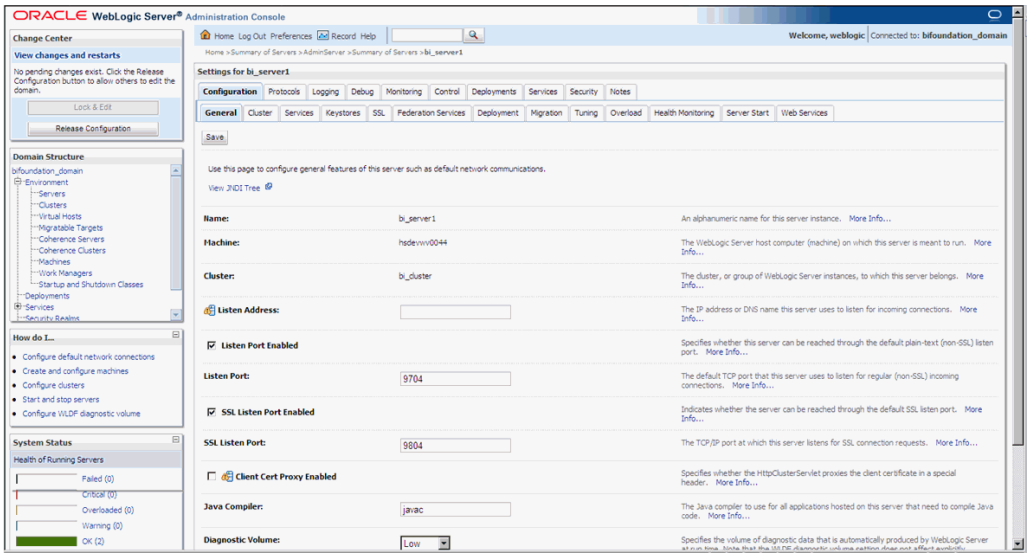
3. Click the Lock & Edit button to change the configuration.
4. Click the AdminServer(admin) link and in the General Tab, enable the SSL listen port, as displayed below:

Figure 2–42 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 2–43 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.

2.13 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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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
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

Component	Privilege	Description	Default Role Granted
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 ScorecardAssessmentService	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
SOAP	Access KPIAssessmentService	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

Component	Privilege	Description	Default Role Granted
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
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

Part II

Appendix

This part of the Installation Guide discusses topics and tasks related to installing Oracle Argus Analytics.

Part II contains the following chapter:

- Chapter A, Managing Catalog Permissions and Privileges

A

Managing Catalog Permissions and Privileges

This appendix comprises the following sections:

- Creating Users and Groups
- Creating Application Roles and Assigning User Groups to Roles
- Maintaining Catalog Privileges
- Managing Permissions for Catalog Folders and Requests

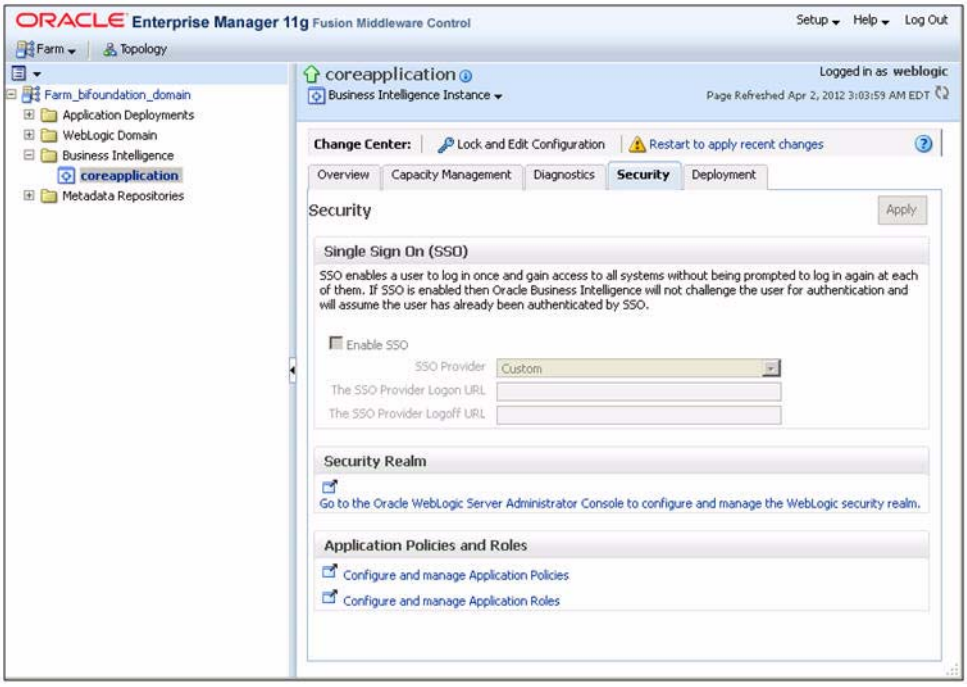
A.1 Creating Users and Groups

To create users and groups, refer to the Creating Users and Groups in Oracle Argus Analytics section in this Installation Guide.

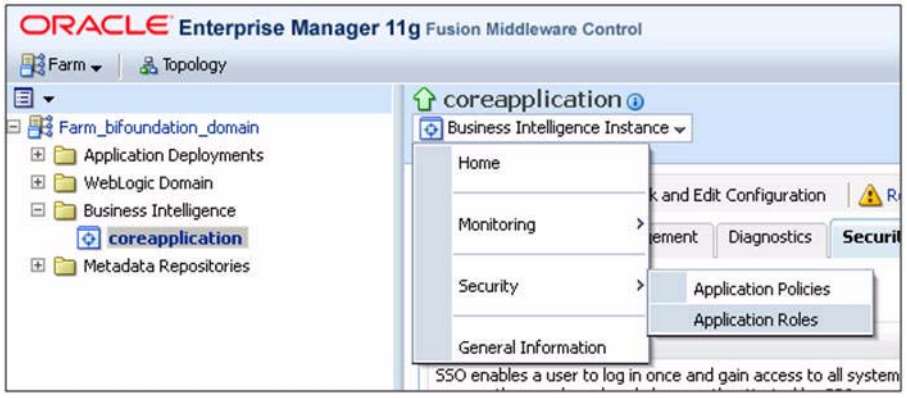
A.2 Creating Application Roles and Assigning User Groups to Roles

Follow the steps listed below, to create new application role(s):

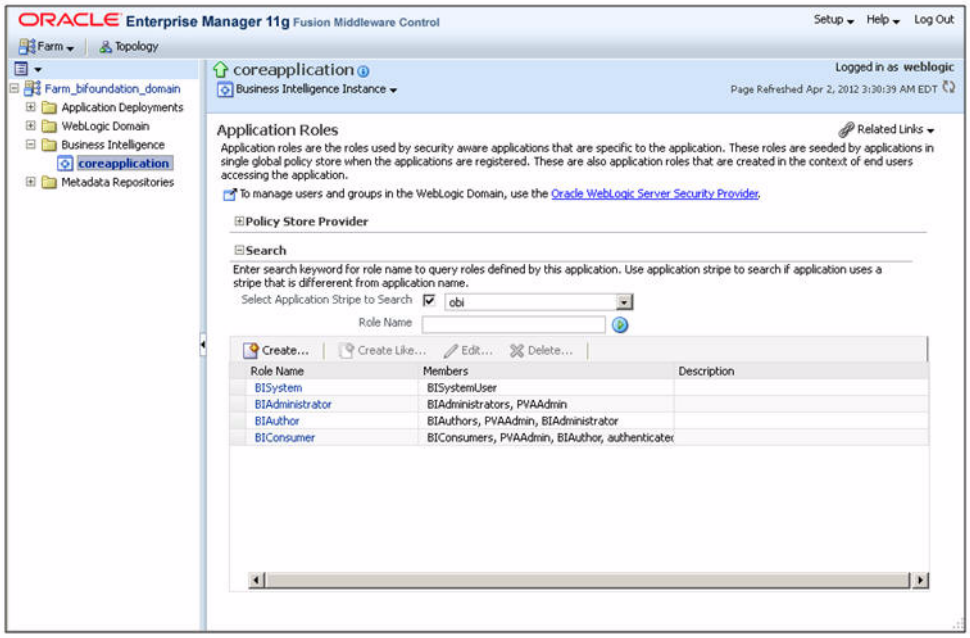
1. Open a new browser window for the Enterprise Manager for Fusion Middleware Control and navigate to the Business Intelligence > coreapplication overview page, as shown below:



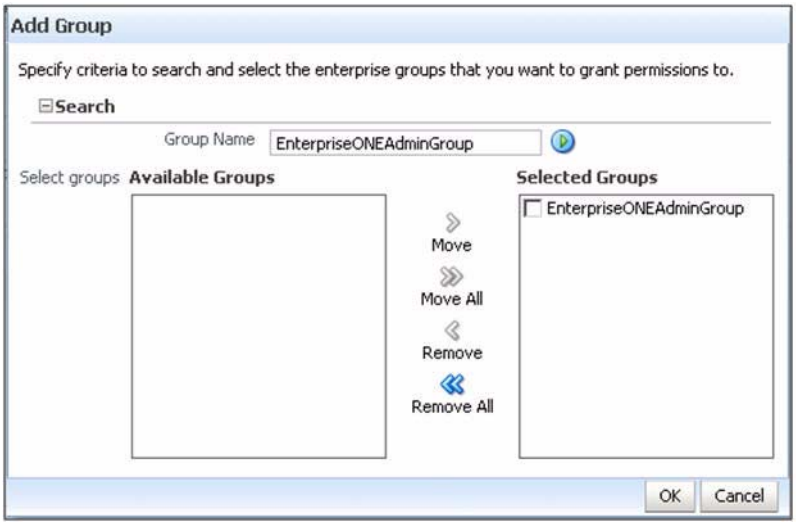
2. Invoke the Application Roles by choosing from the menu drop-down list at Business Intelligence Instance > Security > Application Roles, as shown below:



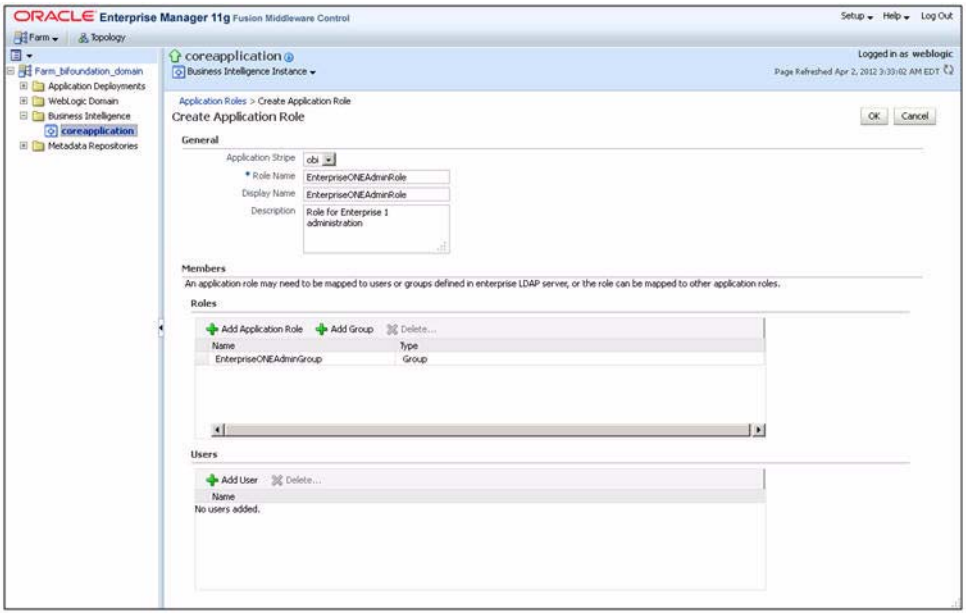
3. Click Create and provide the new role details to be created, as shown below:
   Example:
   Role Name: EnterpriseONEAdminRole
   Display Name: EnterpriseONEAdminRole
   Description: Role for Enterprise 1 Administration



4. Click Add Group and search for the Group.
   Example: EnterpriseONEAdminGroup
   On the search results, select the group and click the Move button.

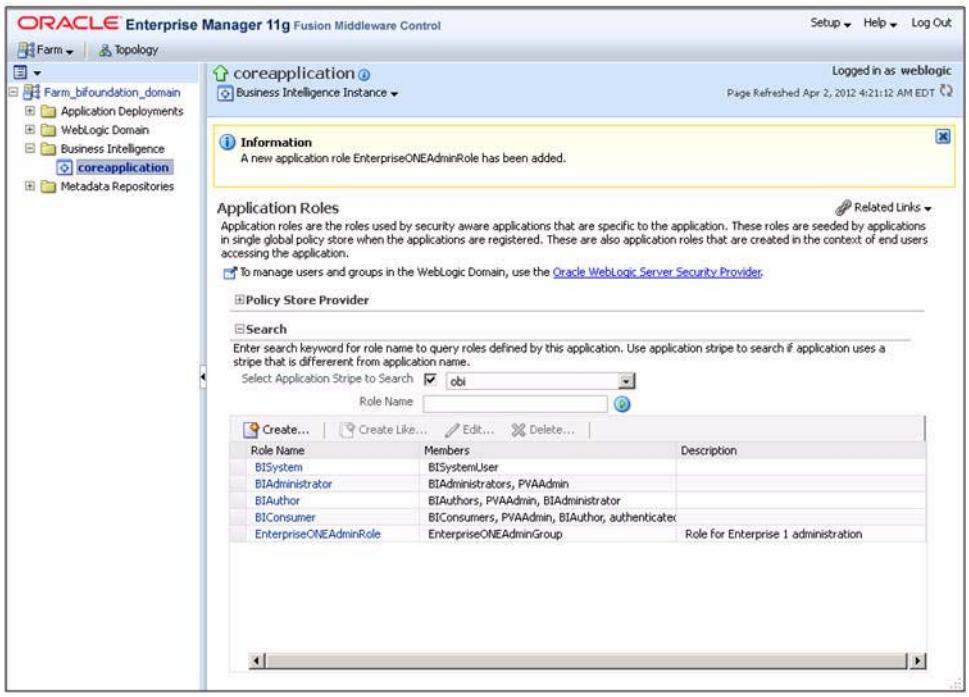


5. Click OK.



6. Click OK.

Repeat the steps listed above, to create roles and assign the required user group(s) to the role(s).



Note: For further details, refer to the *Managing Security Using the Default Security Configuration* section in the *Oracle® Fusion Middleware Security Guide* for *Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*.

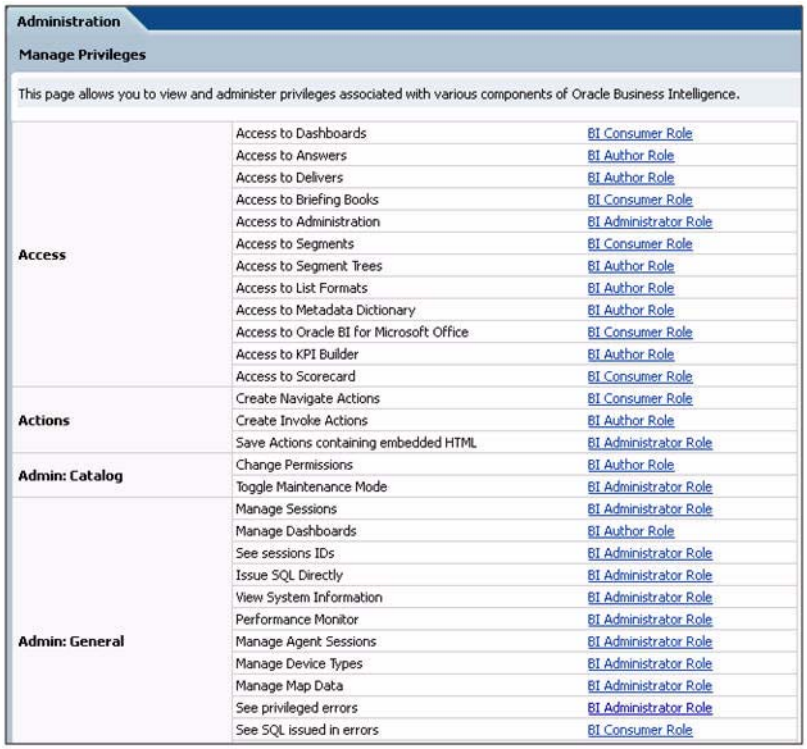
Click **here** to view the section referred above.

A.3 Maintaining Catalog Privileges

Follow the steps listed below, to maintain catalog privileges:

1. Login to the OBIEE application using any admin user credentials.
2. Click the Administration link and navigate to Security > Manage Privileges.

3. The Manage Privileges page is displayed, as shown below:

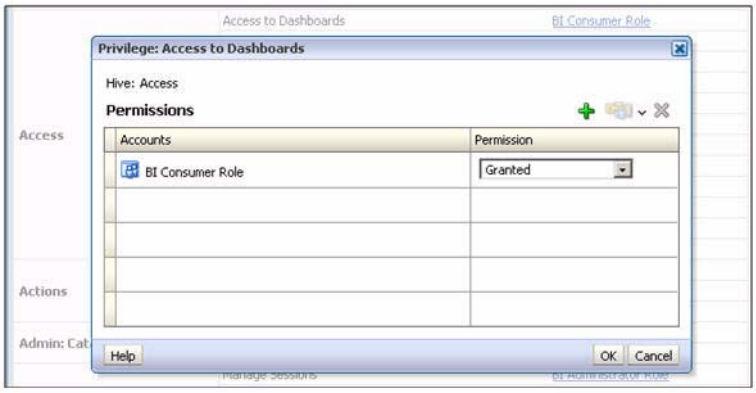


Access	Access to Dashboards	BI Consumer Role
	Access to Answers	BI Author Role
	Access to Delivers	BI Author Role
	Access to Briefing Books	BI Consumer Role
	Access to Administration	BI Administrator Role
	Access to Segments	BI Consumer Role
	Access to Segment Trees	BI Author Role
	Access to List Formats	BI Author Role
	Access to Metadata Dictionary	BI Author Role
	Access to Oracle BI for Microsoft Office	BI Consumer Role
	Access to KPI Builder	BI Author Role
	Access to Scorecard	BI Consumer Role
Actions	Create Navigate Actions	BI Consumer Role
	Create Invoke Actions	BI Author Role
	Save Actions containing embedded HTML	BI Administrator Role
Admin: Catalog	Change Permissions	BI Author Role
	Toggle Maintenance Mode	BI Administrator Role
Admin: General	Manage Sessions	BI Administrator Role
	Manage Dashboards	BI Author Role
	See sessions IDs	BI Administrator Role
	Issue SQL Directly	BI Administrator Role
	View System Information	BI Administrator Role
	Performance Monitor	BI Administrator Role
	Manage Agent Sessions	BI Administrator Role
	Manage Device Types	BI Administrator Role
	Manage Map Data	BI Administrator Role
	See privileged errors	BI Administrator Role
	See SQL issued in errors	BI Consumer Role

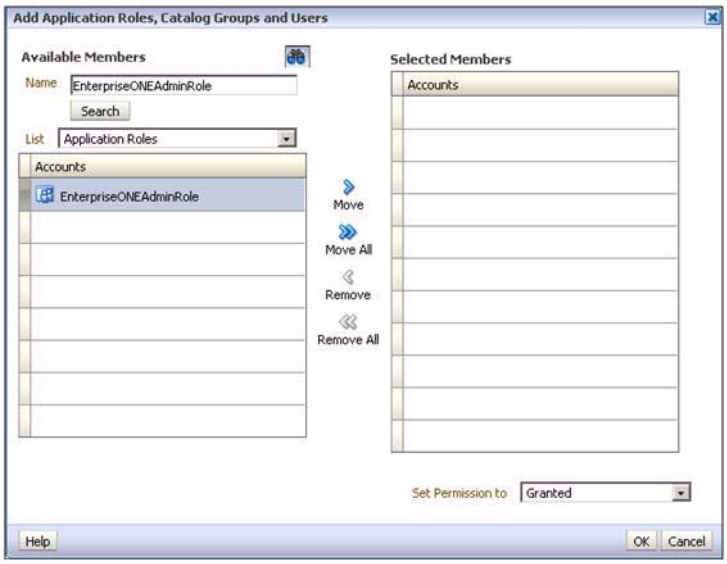
This page lists all the privileges associated with various components of Oracle Business Intelligence. This page allows you to view and administer the listed privileges.

Example: Modify the Access to Dashboards privilege, to provide EnterpriseONEAdminRole with Access privilege. To modify this privilege, execute the following steps:

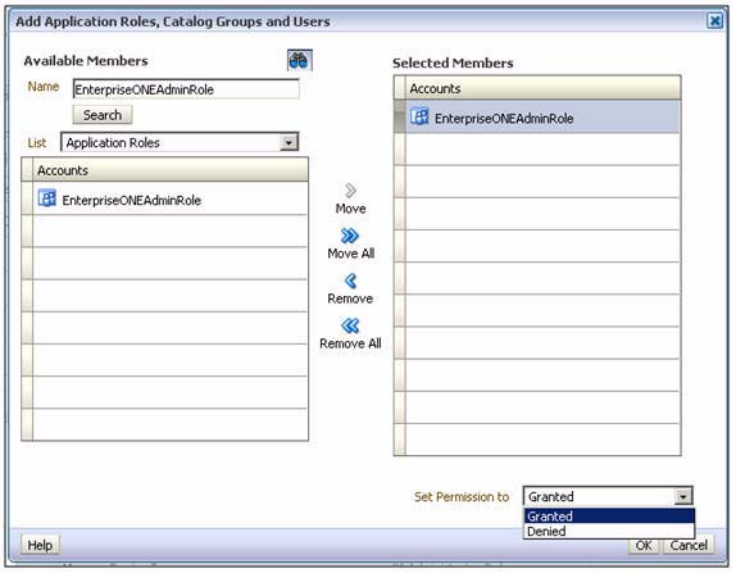
- Click the BI Consumer Role link adjacent to Access to Dashboard. This will open up the Privilege window, as shown below:



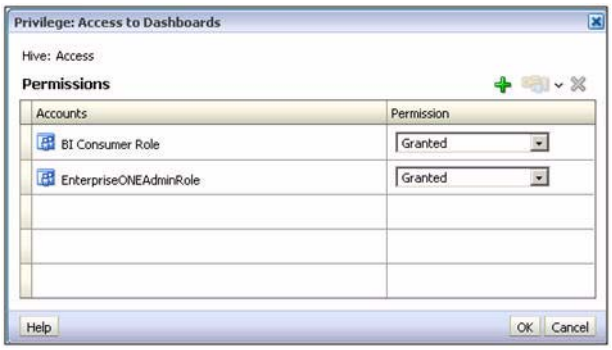
- Click the + (Add) sign. This opens a selection window.
- Enter the required application role, such as EnterpriseONEAdminRole. Select Application Role from the list and click Search. This will list the available application roles based on the entered criteria, as shown below:



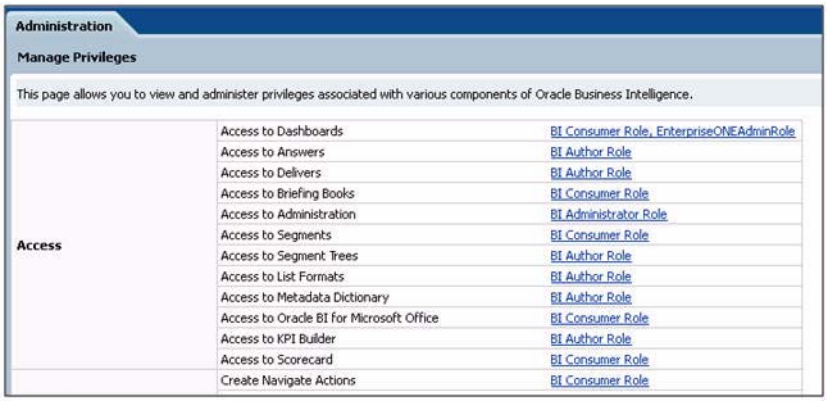
- Select the required role and click **Move**.
- Select **Set Permission to** as **Granted** [Permission can either be Granted or Denied], as shown below:



- Click OK. This system will return to the Privileges window with the newly added role. The following screen is displayed:



- Click OK to complete. The following screen is displayed:



- In this way, you can grant or deny privileges for any given role.

Note: For further details, refer to the *Managing Security for Dashboards and Analyses* section in the *Oracle® Fusion Middleware Security Guide* for *Oracle Business Intelligence Enterprise Edition 11g Release 1 (11.1.1)*.

Click **here** to view the section referred above.

A.4 Managing Permissions for Catalog Folders and Requests

This section comprises the following sub-sections:

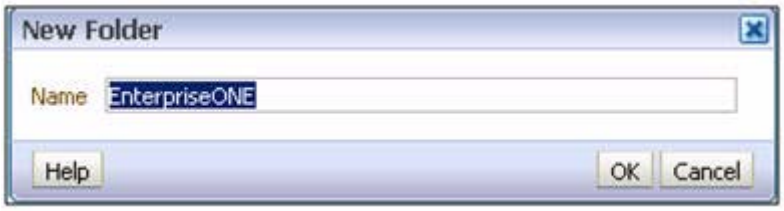
- Creating a New Catalog Folder under Shared Folders
- Managing Permissions for Catalog Folders or Saved Requests

A.4.1 Creating a New Catalog Folder under Shared Folders

Execute the following steps to create a new catalog folder:

1. Login to the OBIEE application using any administrator user credentials.
2. Navigate to *Catalog*.
3. Click Shared Folders under the Folders tree. Click New from the Folders toolbar.

4. Click Folder. Enter the required folder name, such as EnterpriseONE.

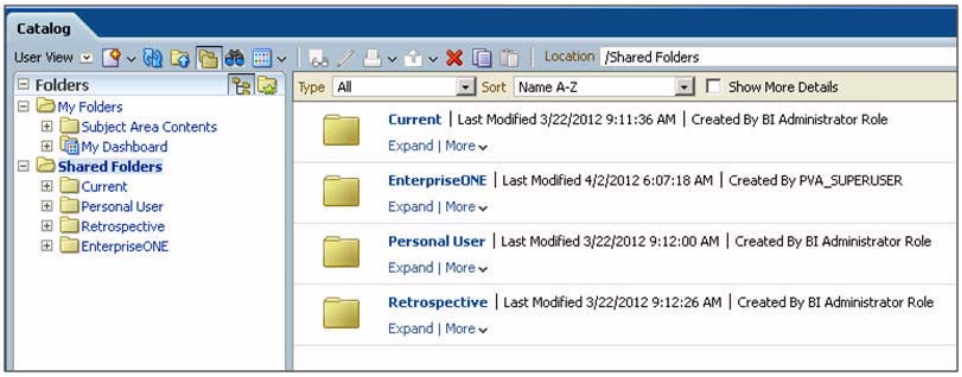


5. Click OK. The new folder is created, as per the given name.

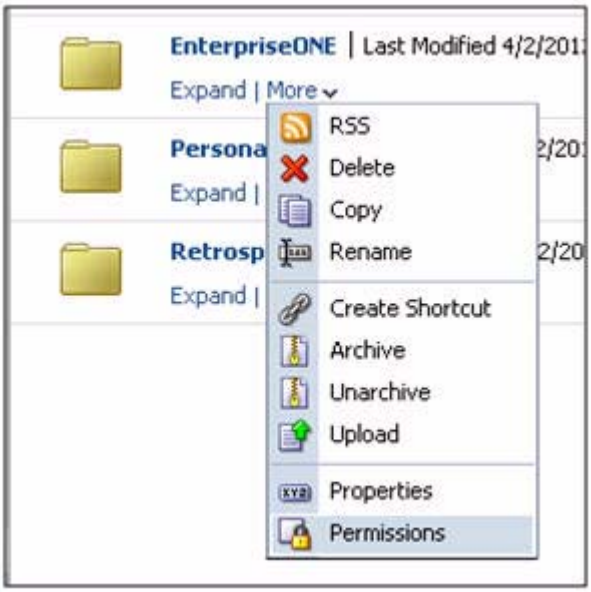
A.4.2 Managing Permissions for Catalog Folders or Saved Requests

Execute the following steps to manage permissions for catalog folders or saved requests:

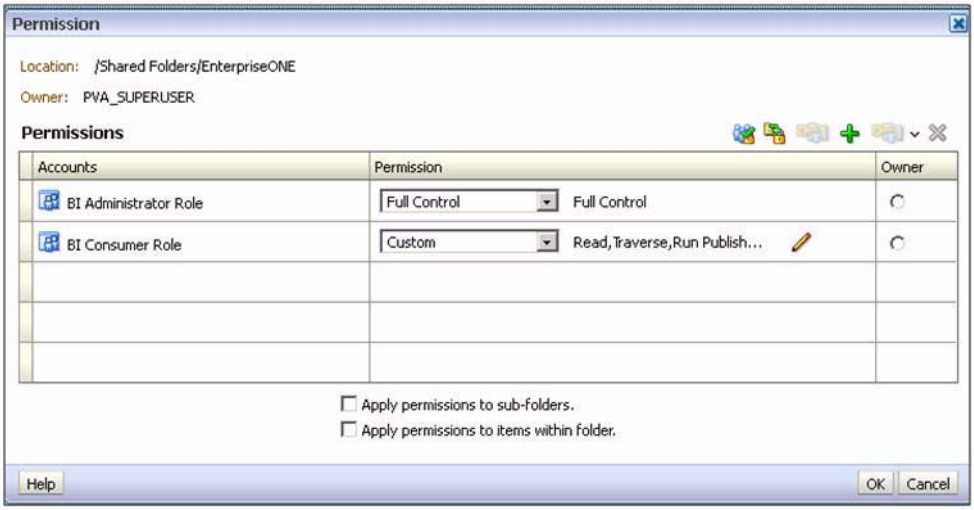
1. Login to the OBIEE application using any administrative user credentials.
2. Navigate to *Catalog*.
3. Click Shared Folders under the Folders tree. The right-hand panel lists all the catalog folders available under Shared Folders. [For the request, select the folder in which the request is saved. Click the More corresponding to the specific request]



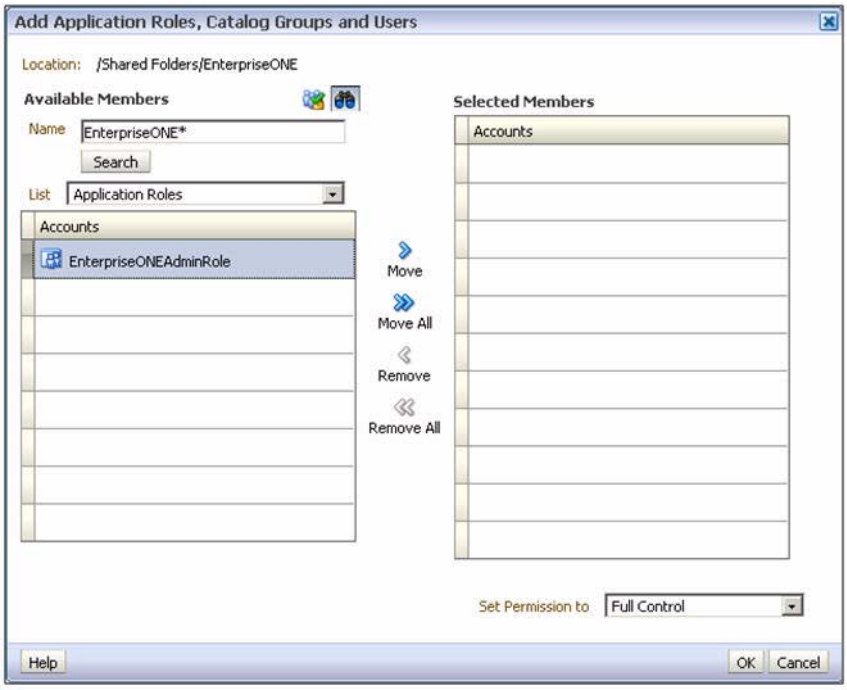
4. Click More for the folder for which you need to manage the permissions, such as for the EnterpriseONE folder. Click Permissions.



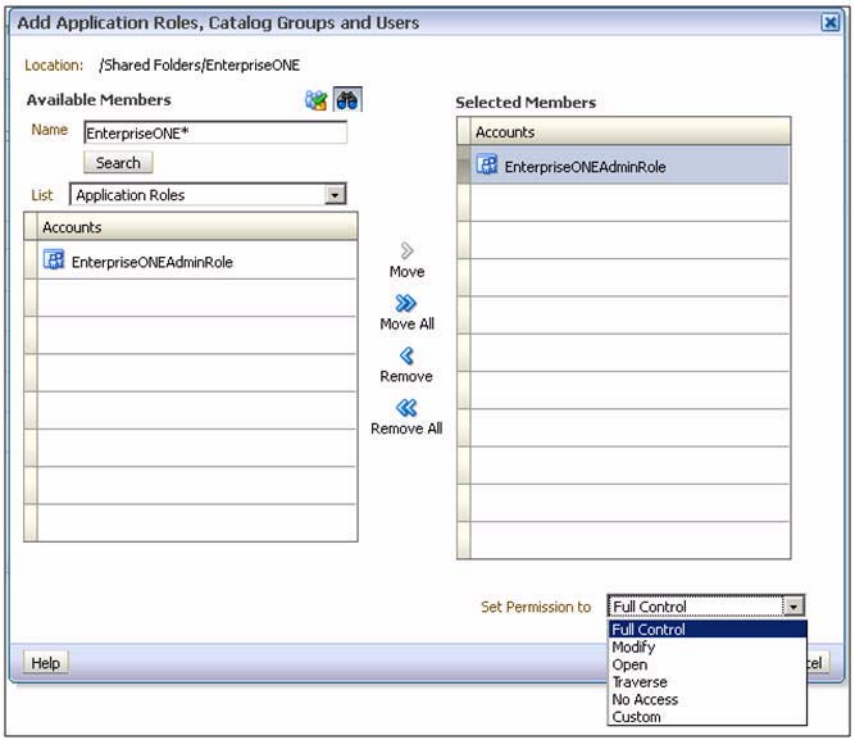
5. The Permissions window is displayed, as shown below:



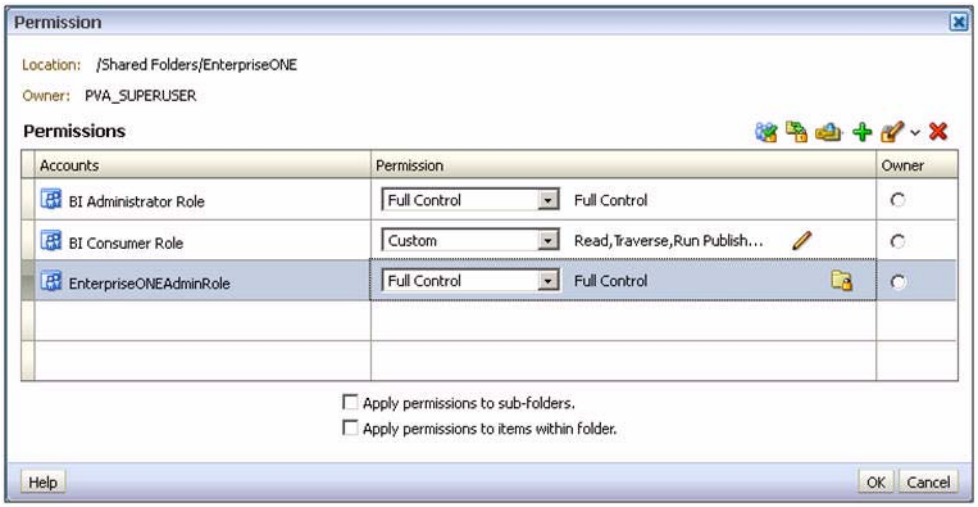
6. Click the + (Add) symbol to add the new Application Roles/Catalog Groups or Users. This will open up the Selection window. For example, to provide Full Control access to this folder for application role called EnterpriseONEAdminRole, enter the required Application Role. Select Application Role under List and click Search. This will list the available Application Roles for the given criteria.



7. Select the required Application Role and click Move. Select the Role and select **Set Permission to** as **Full Control**.



8. Click OK. The system will return to the Permissions window, listing the newly added role and the associated permissions.



9. To apply the same permissions to the sub-folders and items within the folders appropriately, select the checkboxes and click OK.