Oracle® Argus Analytics

Installation Guide

Release 8.1.1

E84917-01

September 2017

ORACLE®

Oracle Argus Analytics Installation Guide, Release 8.1.1

E84917-01

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Contents

Preface

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.

Where to Find More Information

Oracle Help Center

The latest user documentation for Oracle Health Sciences products is available at http://docs.oracle.com/en/industries/health-sciences/.

My Oracle Support

The latest release notes, patches and white papers are on My Oracle Support (MOS) at https://support.oracle.com. For help with using MOS, see https://docs.oracle.com/cd/E74665_01/MOSHP/toc.htm.

Documentation Accessibility

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

Access to Oracle Support

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

1

Oracle Argus Analytics Requirements

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 Server Components

- **Oracle Argus Analytics Database Server**

  (Enterprise Edition or Standard Edition 2 (SE2) 12.1.0.2)

  - Operating System as certified by the database
  - Microsoft Windows Server 2012 Standard (64 bit)
  - Microsoft Windows Server 2012 R2 Standard (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

- **Oracle Argus Analytics ETL Server**

  - **Oracle Argus Analytics Informatica Server**
    - Informatica PowerCenter 9.0.1 with Hotfix2 and PowerCenter 9.6.1.

      Refer to the *Informatica PowerCenter Installation Guide* for recommended hardware and supported platforms.
    - Operating System: As certified by Informatica
    - Memory: At least 8 GB RAM. HDD – at least 250 GB free space
    - CPU: At least 4 Dual Core CPUs
  - **Oracle Data Integrator (ODI) Server**
    - Oracle Data Integrator 12.1.3 or 12.2.1.

      Refer to the *ODI Installation Guide* for recommended hardware and supported platforms.
    - Operating System: As certified by ODI
    - Memory: At least 8 GB RAM. HDD – at least 250 GB free space
    - CPU: At least 4 Dual Core CPUs

- **Oracle Argus Analytics OBIEE Server**
  - Oracle Business Intelligence Enterprise Edition 12.2.1 with latest patch set (the following patch has been verified with AN 8.1.1: 12.2.1.160419 at the time of the release).

    Refer to the *OBIEE Installation Guide* for further hardware and software requirements.
  - Operating System: As certified by OBIEE
  - Memory: RAM at least 16 GB, HDD – at least 250 GB free space
  - CPU: At least 4 Dual Core CPUs

    Note: If Unix-based OS is used for the OBIEE server, then the Oracle Business Intelligence Developer Client Tool must be installed separately on a Microsoft Windows box.

    Refer to the version-specific certification matrix for detailed information on OS certification.

- **Oracle Argus Analytics Data Warehouse Administration Console Server**
  - Oracle Data Warehouse Administration Console Server 11.1.1.6.4
  - Oracle Enterprise Linux 5 or above (32/64 bit)
  - Operating System: As certified by DAC
  - Memory: RAM 4-16 GB (based on organization size), HDD – at least 500 GB free space
  - CPU: At least 2 Dual Core CPUs

1.1.2 Client Components

- **Oracle Database Client**
  - Oracle Argus Analytics requires Oracle database client to connect to the database server. The supported client software version is 12.1.0.2.
- **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 11.1.1.6.4
- **ETL Client**
  - **Informatica PowerCenter Client**
    * An Informatica PowerCenter Client 9.0.1 with Hotfix 2 or PowerCenter Client 9.6.1 is required to connect to the Informatica Server.
    * Supported Operating System: Microsoft Windows Server 2008 or above (32/64 bit), Microsoft Windows Server 2012 or above (64 bit)
  - **ODI Studio**
    * An ODI Studio 12.1.3 or 12.2.1 is required to connect to the ODI Repository.

- **Oracle Business Intelligence Developer Client Tool**
  - Oracle Business Intelligence Developer Client Tool 12.2.1 must be installed for configuring the repository file (RPD).
- **Security Component** (Optional)

  You can also configure Single Sign On Support for your reports and dashboards using Oracle Access Manager 11g. For more information regarding the Oracle Access Manager installation and supported platforms, refer to the *Oracle Access Manager Installation Guide*.
- **Miscellaneous Components**
  - For running the reports and dashboards, your machine should have the Adobe Flash Player 10 or above installed.
  - Although OBIEE 12.2.1 reports are supported on Microsoft Internet Explorer, Mozilla Firefox, Chrome, and Safari, Oracle Argus Analytics is certified only for Microsoft Internet Explorer 11, or above.

1.1.3 Supported Sources

Oracle Argus Analytics, by default, supports only Oracle Argus Safety. It supports Oracle Argus Safety 8.1.1

1.1.4 Technology Stack Matrix

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
Operating System	As certified by OBIEE	As certified by Oracle Database	As certified by Oracle Informatica	As certified by ODI	
Oracle Database	12.1.0.2 Client	12.1.0.2 (Enterprise) - AL32UTF8 character set (Supports both CDB-PDB/Non CDB)			
OBIEE	OBIEE 12.2.1 (With the latest patch set)				
Informatica	Informatica Server 9.0.1 HF2 or Informatica Server 9.6.1		Informatica Server 9.0.1 HF2 or Informatica Server 9.6.1		
DAC	DAC Server 11.1.1.6.4		DAC Server 11.1.1.6.4		
Browser	IE 11.0				IE 11.0
Adobe Reader	Acrobat Reader DC Acrobat Reader XI				Acrobat Reader DC Acrobat Reader XI
Single Sign On Solution (Optional)	Oracle Access Manager 11.1.2.2				

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
Resolution					1280 x 1024

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.

Oracle Business Intelligence Developer Client Tool can be installed along with the OBIEE Server, provided the Operating System is Microsoft Windows.

***Note 1:** Oracle Client Patch required for the SQL Loader

1. Download the patch 19720843: WINDOWS DB BUNDLE PATCH 12.1.0.2.1 from the Oracle Support.
2. Install the patch, and apply the following workaround:

   a. Set the **oracle_home** as your client home location. For example:

   SET ORACLE_HOME=C:\app\client32\product\12.1.0\client_1

   i. On the client machine, go to %oracle_home%\bin\

   ii. From \p19720843_121020_WINNT\19720843\files\bin\, copy the file **oranfsodm12.dll**, and paste it under %oracle_home%\bin

   b. Run **sqlldr help=y** or **sqlldr.exe**.

1.1.4.1 Supported Security Configuration (Optional)

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

Note: If OAM is used, then the OBIEE Server must have Oracle Web Tier 12c with in-built WebGate.

1.1.5 Typical Hardware Architecture

- **Servers**:
  - An Oracle Database Server with Oracle Database 12.1.0.2
  - An OBIEE 12.2.1 Server with latest patch set
  - ETL Server
    * Informatica PowerCenter 9.0.1 with Hotfix 2 or PowerCenter 9.6.1 Server + DAC Server 11.1.1.6.4

    OR

    * ODI Studio 12.1.3 or 12.2.1

Note: These servers can run on any of the supported platforms: Linux, Solaris, or Windows.

- **Clients**:
  - ETL Clients
    * Informatica PowerCenter Client 9.0.1 + Hotfix 2 or Informatica PowerCenter Client 9.6.1

    OR

    * ODI Studio 12.1.3 or 12.2.1
  - Oracle Database Client 12.1.0.2
  - DAC Client 11.1.1.6.4
  - Oracle Business Intelligence Developer Client Tool (12.2.1.0.0)

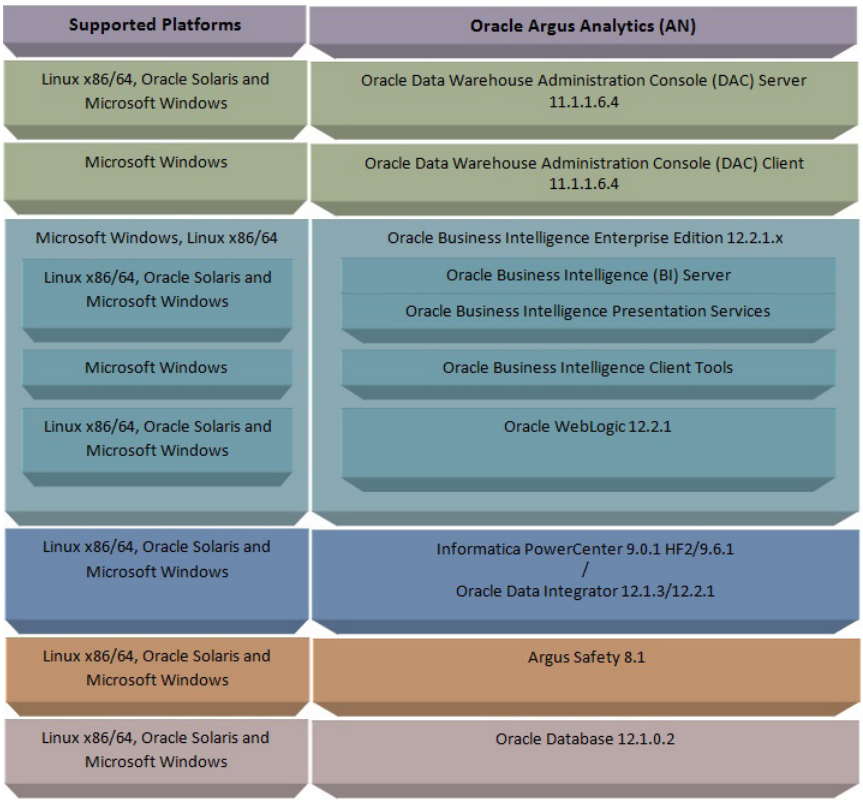
Note: All tools can be installed in a single Microsoft Windows box.

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



1.1.6 Installation Process Overview

The following steps describes the overview of the installation process:

- Follow the steps described in Section 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, go to My Oracle Support > Certifications.

1.2 Pre-requisites

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

- Oracle Database Server – An Oracle 12.1.0.2 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 or PowerCenter 9.6.1 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 12.1.0.2 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 11.1.1.6.4 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 12.1.3 or 12.2.1 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 12.2.1 Server must be installed before the Oracle Argus Analytics Installation. Follow platform-specific OBIEE Installation Guide for installation instructions.

1.2.1 Client Tools

- ETL Client Tools
- Informatica PowerCenter Client - An Informatica PowerCenter Client 9.0.1 with Hotfix 2 or PowerCenter Client 9.6.1 must be present. Supported only on a Microsoft Windows 32-bit machine.
- DAC Client - A DAC Client 11.1.1.6.4 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 12.1.0.2 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 Server 2012 R2 Standard (64 bit) with OBIEE Server, 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.

Argus Analytics Upgrade Matrix

Before deciding on an upgrade for Argus Analytics, it is important that we first map ourselves as per our current Argus Analytics version and the tasks required to upgrade from one version to another.

The following matrix provides a high-level overview of the tasks to be performed to upgrade from one Argus Analytics version to another:

Current Argus Analytics Version	Upgrade to Argus Analytics Version:					
	1.1	1.1.1	7.0.3	8.0	8.1	8.1.1
1.0	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.
1.1	Not applicable	Use Argus Analytics 1.1.1 Installer to upgrade.	Use Argus Analytics 7.0.3 installer to make the upgrade.	Use Argus Analytics 8.0 installer to make the upgrade.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.

Current Argus Analytics Version	Upgrade to Argus Analytics Version:					
	1.1	1.1.1	7.0.3	8.0	8.1	8.1.1
1.1.1	Not applicable	Not applicable	Follow the steps given below: 1. Apply patch Argus Analytics 1.1.1.1 (Please follow the patch release notes for complete details). 2. Get the latest Context Sensitive Help files and deploy the same. Follow the steps given below: a) Extract the Argus Analytics 7.0.3 installer to any temporary folder. Example: C:\temp\AN80 b) Navigate to the folder <Installer ExtractionFolder>\stage\Components\oracle.hsgbu.opva\7.0.3.0.0\1\DataFiles\Expanded\filegroup19 . Copy the opva_help.zip. c) Navigate to <Argus Analytics Home>\report\help. Rename the existing opva_help.zip to opva_help_<Argus Analytics version>.zip (Example: opva_help_AN1.1.zip). d) Paste the copied opva_help.zip file. e) Please follow the steps mentioned in section Configuring the Help links in the Dashboards and Reports to deploy the latest help file. 3. (Optional Setup): Argus Analytics 7.0.3 is certified with Oracle Data Integrator(ODI) 11.1.1.7. It is optional to upgrade the existing ODI from 11.1.1.6.3 to 11.1.1.7.0. Please follow the documentation Oracle® Fusion Middleware Upgrade Guide for Oracle Data Integrator 11g Release 1 (11.1.1.7.0) to upgrade the existing ODI 11.1.1.6.3 to 11.1.1.7.0.	Use Argus Analytics 8.0 installer to make the upgrade.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.
7.0.3	Not applicable	Not applicable	Not applicable	Use Argus Analytics 8.0 installer to make the upgrade.	Cannot upgrade. Need to perform a fresh installation.	Cannot upgrade. Need to perform a fresh installation.
8.0	Not applicable	Not applicable	Not applicable	Not applicable	Use Argus Analytics 8.1 installer to make the upgrade.	Cannot upgrade. Need to perform a fresh installation.

Current Argus Analytics Version	Upgrade to Argus Analytics Version:					
	1.1	1.1.1	7.0.3	8.0	8.1	8.1.1
8.1	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	Use Argus Analytics 8.1.1 installer to make the upgrade.

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.

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.

2.1 Preinstallation Configuration

1. The TNS entries for both the Data Mart Schema and the Argus Safety Database Schema should be present in the OBIEE 12c home in the path:

   <OracleBI Home>\user_projects\domains\<BI Domain Name>\config\fmwconfig\bienv\core\

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. Set up an INSTALL(DBA) user:

a. Execute the **ancreatedbauser.bat** file from <*Argus Analytics Installer directory*>*install**utils*.

b. Enter the following inputs:

- Database Connection String for Argus Safety or Argus Analytics DB

- Enter the user with SYSDBA privileges in <Argus Analytics/Argus Safety> database

- Enter password for <SYSDBA user> in <Argus Analytics/Argus Safety> database

- Enter DBA User to be created in <Argus Analytics/Argus Safety> database

- Enter password for <DBA user> in <Argus Analytics/Argus Safety> database

Repeat the procedure to create INSTALL(DBA) user for Argus Safety database, and Argus Analytics database.

Note:

- If the INSTALL(DBA) user already exits in the database, then the script provides the required additional grants to the user. If the user does not exists in the database, a new user is created, and necessary grants are provided.
- When the installation is complete, you may drop this user from the database by executing the following command:

```
DROP USER <INSTALL(DBA) USER> CASCADE;
```

---

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 '/DatafilePath/<AN_DATA_TS>_01.dbf'
SIZE 100M
AUTOEXTEND ON
NEXT 1M
LOGGING;
```

Example:

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

```
CREATE TEMPORARY TABLESPACE <AN_TEMP_TS>
TEMPFILE '/Tempfile Path/<AN_TEMP_TS>_01.dbf'
SIZE 100M
AUTOEXTEND ON
NEXT 1M;
```

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 one as required.

2.1.1.1 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 Installing ODI Studio and Creating Master and Work Repository

Before configuring ODI Settings, you must install ODI Studio and configure an agent (either Standalone Agent, Java EE Agent, or Colocated Agent).

ODI 12c has the following types of installation:

- Enterprise Installation—Enables you to deploy ODI Studio along with the binaries to configure either Java EE Agent, or Colocated Agent.
- Standalone Installation—Enables you to deploy ODI Studio along with the binaries to configure Standalone Agent.

To understand the agent topologies for the best suitable installation, Oracle recommends you to refer *ODI Install and Configuration Guide* > *Planning the Oracle Data Integrator Installation section*.

When installing the ODI, note down the SUPERVISOR credentials, and Master and Work Repository credentials.

For more details, refer to the *Oracle Data Integrator Install and Configuration Guide*:

- For ODI 12.1.3

https://docs.oracle.com/middleware/1213/core/ODING/toc.htm

- For ODI 12.2.1

  https://docs.oracle.com/middleware/1221/core/ODING/toc.htm

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 Previous Versions

Select if Argus Analytics is a fresh installation or an upgrade installation which is supported from Argus Analytics 8.1 to 8.1.1.

> **Note:** The upgrade path installation needs information to be provided on the previous Argus Analytics 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 8.1

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 DBA User: Enter the custom INSTALL(DBA) user name (created in Section 2.1, "Preinstallation Configuration" > Step 5).
- Argus Safety DBA Password: Password of the INSTALL(DBA) user
- 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 respectively.

Example:

- AS Database Connect String: AS70X_SID
- AS Schema: ARGUS_APP
- AS Password: <ARGUS_APP user's password>
- AS DBA User Name: <INSTALL user name>
- AS DBA User Name: <INSTALL 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 DBA User name: Enter the customer INSTALL(DBA) User Name (created in Section 2.1, "Preinstallation Configuration" > Step 5).
- DWH Data Mart DBA User Password: Password of the INSTALL(DBA) user
- 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 respectively.

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 DBA User Name: <INSTALL user name>
- DW DBA User Password: <INSTALL user's password>
- 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 Argus Analytics.
>
> 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 verified from the following path or from your local Oracle Inventory logs folder.

<Argus Analytics Home>\install\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 Data Warehouse Load 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

The 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
$$p_enterprise_id	The specific Enterprise ID to run the ETL for.	-1: Runs the Incremental ETL for the entire Warehouse 0: Runs the Incremental ETL for all the enterprises the user ($$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

Table 2–1 (Cont.) DAC Configurable Parameters

Parameters	Description	Allowed Values
$$p_user_name	The user name for which the Incremental ETL shall use to set the VPD Context for the specified enterprise in the parameter: $$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

7. For the choice of the ETL Tool as Informatica, if the installation path chosen is a fresh install, then an Initial/Full load must be run in DAC using the 'OPVA Data Warehouse Load' execution plan.

   Typically, customers would only need to run an Initial/Full ETL load during the initial deployment of the product.

   Note: During the execution of Initial/Full load on a multi-tenant Argus Analytics installation, the VPD Policies present on the warehouse tables will be disabled, in turn disabling the Enterprise Security.

   The VPD Policies will get re-enabled at the end of a successful Initial/Full load run in DAC. It becomes imperative, therefore, that during the execution of Initial/Full Load, the Argus Analytics OBIEE URL should not be made available to the end users.

   Besides this, it is also worth observing that the VPD Policies on the warehouse tables will not get disabled during subsequent Incremental load runs of the "OPVA Data Warehouse Load" execution plan in DAC and the Argus Analytics OBIEE URL can be made available to the end users during its execution.

   Note: If you are upgrading the Argus Analytics from 8.0 to 8.1, it is not necessary to run/force a Full Load ETL again in DAC for Argus Analytics.

2.4 ODI Smart Import and Topology Configuration (ODI only)

This section comprises the following sub-sections:

- Connecting to ODI Studio
- ODI Smart Import
- Configuring the Topology in ODI Studio
- Configuring ODI Agent

2.4.1 Connecting to ODI Studio

1. Execute the following procedures from:
   a. *Oracle Data Integrator Install and Configuration Guide* > *Configuring Oracle Data Integrator Studio* > *Starting ODI Studio*.
   b. *Oracle Data Integrator Install and Configuration Guide* > *Configuring Oracle Data Integrator Studio* > *Connecting to the Master Repository*.
2. Create a Work Repository Login by following the same steps as in *Step 1 b* > *Connecting to the Master Repository*.

   In the Work Repository section, select a work repository from the find list instead on **Master Repository Only** option. For example, name the repository as **AN Work Repository**.

Refer to the *Oracle Data Integrator Install and Configuration Guide*:

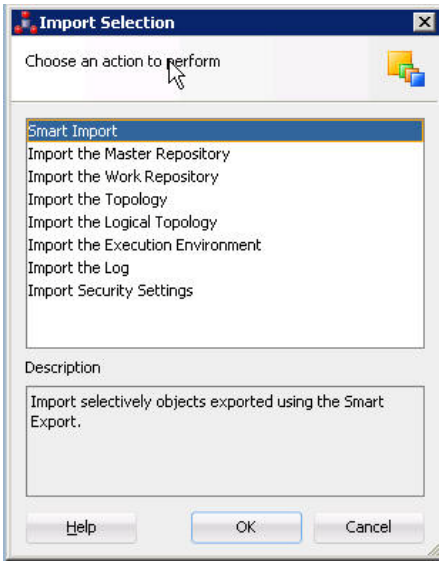
- For ODI 12.1.3 https://docs.oracle.com/middleware/1213/core/ODING/configure_studio.htm#ODING940
- For ODI 12.2.1 https://docs.oracle.com/middleware/1221/core/ODING/GUID-C273EFBE-C0A8-49A2-908B-255BCF9DA468.htm#ODING939

2.4.2 ODI Smart Import

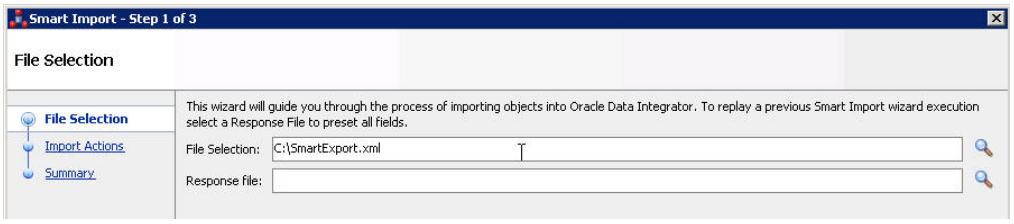
Follow the steps listed below to execute ODI Smart Import:

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.

2.4.3 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 =(SERVICE_NAME=<DWH_DB_SERVICE_NAME>)))

- 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>

     or

     jdbc:oracle:thin: <DWH_DB_SERVER>:<DWH_DB_LISTENER_PORT>/<DWH_DB_SERVICE_NAME>

     Please use the jdbc connection string with database SERVICE_NAME in case the database version is 12c.
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 =(SERVICE_NAME=<AS_DB_SERVICE_NAME>)))

    - 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>

  or

  jdbc:oracle:thin: <AS_DB_SERVER>:<AS_DB_LISTENER_PORT>/<AS_DB_SERVICE_NAME>

  Please use the jdbc connection string with database SERVICE_NAME in case the database version is 12c.

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.

2.4.4 Configuring ODI Agent

You need to configure either one of the agents: Java EE Agent, Colocated Agent, or Standalone Agent.

To understand the agent topologies for the best suitable installation, Oracle recommends you to refer the *ODI Install and Configuration Guide* > *Planning the Oracle Data Integrator Installation section*.

When installing the ODI, use SUPERVISOR credentials, and Master and Work Repository credentials as created in the Section 2.1.1.2, "Installing ODI Studio and Creating Master and Work Repository."

> **Note:** Make sure to create the agent with name **PA_AN**, as the same is available in Argus Analytics ODI code.

For more details, refer to the following:

- For ODI 12.1.3

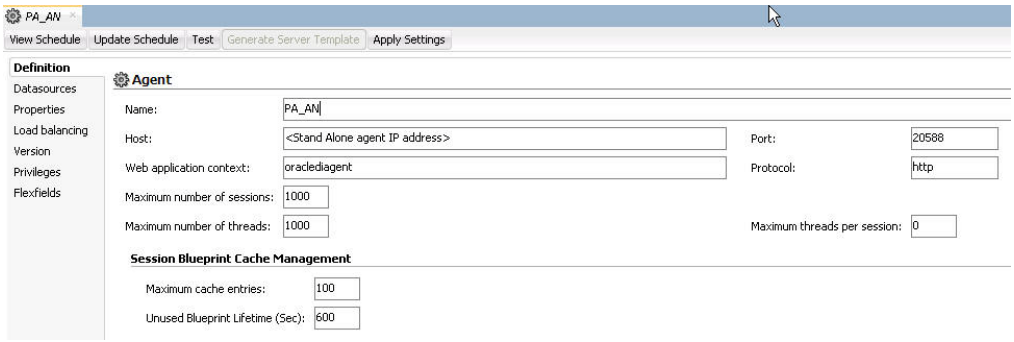
  `https://docs.oracle.com/middleware/1213/core/ODING/toc.htm`

- For ODI 12.2.1

  `https://docs.oracle.com/middleware/1221/core/ODING/toc.htm`

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 ODI 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).

Note: Before making Argus Analytics OBIEE URL available to the end users, the Initial/Full load ETL (LP_FL_AN) in ODI should be successfully run.

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

Refer to the following table: **Table 2-2 ODI Parameters**. In ODI, unlike in the Informatica ETLs, the VPD Policies on the warehouse tables do not get disabled during the execution of the ETLs (Full/Incremental) for a multi-tenant installation.

Table 2–2 ODI Parameters

Parameters	Load Type	Description	Allowed Values
VAR_ALN_PERIOD_FROM_DATE	Full Load	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	Date values such as: 01/01/1980 Recommended value: 01/01/1980
VAR_ALN_PERIOD_TO_DATE	Full Load	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	Date values such as: 12/31/2019 Recommended Value: 12/31/2019

Table 2–2 (Cont.) ODI Parameters

Parameters	Load Type	Description	Allowed Values
VAR_INT_TRUNCATE_STAGE	Both	This variable is used to decide whether to truncate the stage table or not and is useful in multiple Argus Safety DB support	Valid values: 0: Does not truncate Stage table 1: Truncate Stage table Should be specified as 1 always in case of Single Argus Safety Instance as source information Recommended Value: 1
VAR_INT_COLLECT_STATISTICS	Both	This variable is used to decide whether the statistics of the target tables need to be collected or not.	Default Value: 1 Values Accepted: 0,1 0: Load Plans will not collect statistics 1: Load Plans will collect statistics after loading data
VAR_ALN_ENTERPRISE	Both	The specific Enterprise ID to run the ETL for.	-1: Runs the ETL for the entire Warehouse 0: Runs the 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. **Note:** For Full Load, this value has to be -1.
VAR_ALN_ERROR_REJECT_LIMIT	Both	This variable is used to set the number of rows that will be tracked in the respective error tables prior to aborting the ETL in case of errors.	Valid Values: Positive Integer numbers: (E.g. 0, 100, 1000, etc.) UNLIMITED: All the error records are logged Recommended Value: UNLIMITED
VAR_ALN_USER_NAME	Both	The user name for which the ETL shall use to set the VPD Context for the specified enterprise in the parameter: VAR_ALN_ENTERPRISE. This value should be passed inside single quotes: such as 'username'.	Default value: 'admin'

Table 2–2 (Cont.) ODI Parameters

Parameters	Load Type	Description	Allowed Values
VAR_INT_RAISE_ERROR	Both	Setting this variable to 0 or 1 will appropriately either stop a Load Plan/Interface or continue the same when data errors are encountered during the load.	0: Do not raise data error when encountered during ETLs 1: Raise data error when encountered during ETLs Recommended Value: 1
VAR_INT_CONFIG_DAYS	Incremental Load	Reduces the incremental extract window by the specified number of days. Example: Extract all changed rows between LAST_EXTRACT_DATE and (SYSDATE - $$p_config_days)	Integers Recommended Value: 0

2.4.5 Modifying ODI Java EE Agent Connection Pool Settings

Note: This section is applicable only if you are using ODI Java EE Agent.

After configuring the ODI 12c Java EE Agent, follow these steps to increase the size of the connection pool to enable parallel step executions as appropriate for Argus Analytics:

1. Open the ODI WLS administration console (ex: http://<ODI server name>:<ODI port number>/Console)

2. Navigate to Services -> Datasources -> odiMasterRepository

3. Go to the tab Configuration -> Connection Pool

4. Change the Maximum Capacity to 50.

5. Repeat these steps for increasing the connection pool size for the datasource odiWorkRepository as well.

Please note that without increasing the connection pool size the Argus Analytics ETLs will fail.

2.5 Configuring the OBIEE Repository and Webcatalog

2.5.1 Prerequisites

Make sure OBIEE 12c (12.2.1) with latest patch set 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 9500 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 RPD and Catalog (Upgrade Install Only)

Note: Catalog and RPD upgrade are not available from Argus Analytics 1.1/1.1.1/7.0.3/8.0. Use the latest catalog provided with the AN 8.1.1 installation (present at <AN_INSTALL_HOME>/catalog/opva.zip) for deployment.

2.5.1.1.1 Upgrading the RPD

The following steps upgrades the AN 8.1 RPD to the latest code in AN 8.1.1.

Note that `if there have been no customizations to the existing AN RPD, you can skip this section`, because the latest RPD is already present at <AN_INSTALL_HOME>/repository/opva.rpd.

To upgrade the AN RPD (if required):

1. Open the existing AN RPD file that you wish to upgrade to AN 8.1.1 in the BI Administration 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 existing AN 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 8.1.1 RPD file present at <AN_INSTALL_HOME>/repository/opva.rpd.
10. Enter the repository password as opva1234.
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 8.1.1 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 Catalog

Catalog upgrade from Argus Analytics 1.1/1.1.1/7.0.3/8.0/8.1 is not available. Use the latest catalog provided with the AN 8.1.1 installation (present at <AN_INSTALL_HOME>/catalog/opva.zip) for deployment.

2.5.2 Deployment of OBIEE Repository and Catalog

2.5.2.1 Configuring the OBIEE Repository and Web Catalog using the BAR File

> **Note:** The default password for the **opva.rpd** repository file is **opva1234**. You should 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.

Oracle Business Intelligence Application Archive (BAR) file is a compressed archive file that contains a cohesive set of BI metadata artifacts (data model, content model, and authorization model). The OBIEE BAR file for Argus Analytics is available at the following location:

<Argus Analytics Home>\report\ssi.bar

A BAR file contains the following BI application module artifacts:

- Data model metadata for the Oracle BI Server. This metadata is xml-based but functionally equivalent to a .RPD file.
- Presentation Services catalog metadata for a service instance.
- Security policy metadata containing application role and application role memberships, and permission and permission set grants for a service instance.
- A manifest file declaring the dependencies of the BAR file.

This section comprises the following:

- Importing the BAR file in an existing OBIEE instance
- Importing the BAR file when creating a new OBIEE Instance

> **Note:** Importing a BAR file replaces all the Catalog files, RPD files, and the Security Model in an existing OBIEE instance with any customization.
>
> It is recommended that the BAR file import is done on a new OBIEE instance.

2.5.2.1.1 Importing the BAR file in an existing OBIEE instance

Before importing the BAR file, make sure:

- OBIEE 12.2.1 is installed
- The Administrator Console is up and running

  (validate it from *http://<machinename>.<port>/console*)
- The Enterprise Manager (Fusion Middleware Control) is up and running

  (validate it from *http://<machinename>.<port>/em*)

To import the BAR file:

1. Copy the BAR file from *<Argus Analytics Home>\report\ssi.bar* to a machine where the OBIEE is installed.
2. Login to the Enterprise Manager with the WebLogic credentials.
3. Click **Target Navigation.**

   The Target Navigation drop-down menu appears.
4. Go to Business Intelligence > biinstance.

   The Business Intelligence Instance screen appears.
5. From the Availability tab, select **Processes**, and click **Stop All**.

   A confirmation dialog box appears.
6. Click **Yes**.

   All the running processes are stopped.
7. Go to the command prompt, and start the WebLogic Scripting Tool (using wlst.cmd (for Windows), or wlst.sh (for Unix or Linux)) from the following path:

   <Middleware Home>\oracle_common\common\bin
8. To know the **BI Service Instance key**, type the following command, and press Enter.

   listBIServiceInstances(<BI DomainHome path>)

   where, Domain Home is the directory of the BI Install domain, the default path is:

   <obiee_home>/user_projects/domains/bi

   The Key appears at the end of the command.
9. To import the BAR file, execute the following command:

   importServiceInstance('<BI Domain Home path>','BI ServiceInstance key', '<Complete Path of Bar file to import>')

   For example,

   Domain Home path: *<obiee_home>/user_projects/domains/bi>*

   BI Service Instance Key: *ssi* (This key must be **ssi** for Argus Analytics deployment)

   Warning: While executing the WLST on Windows server, you must use forward slash (/) to avoid any error messages. For example:

   ```
   importServiceInstance('C:/Oracle/Middleware/Oracle_Home/user_
   projects/domains/bi','ssi', 'C:/AN81/report/ssi.bar')
   ```
10. When the import of BAR file is complete, exit WLST using the **exit ()** command.
11. Go to Enterprise Manager, from the Availability tab, select **Processes**, and click **Start All**.

    A confirmation dialog box appears.

12. Click **Yes**.

    The BAR file imports the RPD, Catalog and the Security model.

    Note: All the WLST commands are case sensitive.

    To start the WebLogic Scripting Tool on Unix or Linux, use wlst.sh command, rest all of the commands mentioned in the procedure remains same.

To check if the BAR file has imported RPD, Catalog, and the Security Model:

1. To verify the Roles and Policies imported by BAR file in the Enterprise Manager, go to Business Intelligence Instance > Security > Application Roles and Application Policies.

   The following roles are imported as default application roles:

   - PVAAdminRole
   - PVASafetyRole
   - PVASafetyConsumersRole

2. To modify the Connection Pool Settings:

   a. From the following path, right click the **admintool.cmd** file, and click **Run as Administrator**.

      <MiddlewareHome>\user_projects\domains\bi\bitools\bin

      The Oracle BI Administration Tool opens.

      Note: If OBIEE is installed on a Unix or Linux machine, then you must setup the Oracle Business Intelligence Developer Client tool on any Windows machine to access the BI Administration Tool.

      See Appendix A, "Creating ODBC Connection for OBIEE Administration Tool."

      ---

   b. To open the RPD, select the online mode, and enter the WebLogic user credentials.

      Note: You must set the Open Database Connectivity (ODBC).

      To open the RPD in online mode on Unix or Linux, set the ODBC on a Windows machine where OBIEE client is installed, and open the RPD.

      ---

   c. Click the **Connection Pool**, and modify the **Data source name**, **User name**, and **Password**.

      Modify both the following connection pools:

      -Under OPVA_DWH database:

      * OPVA_CP:

        Data Source Name—Argus Analytics database TNS Name

        User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

Password—Password for Argus Analytics DWH RPD schema

* OPVA_CP_InitBlocks:

Data Source Name—Argus Analytics database TNS Name

User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

Password—Password for Argus Analytics DWH RPD schema

- Under OPVA_SRC database:

* OPVA_CP:

Data Source Name—Argus Safety database TNS Name

User name—Argus Analytics SRC RPD schema <AN_SRC_RPD>

Password—Password for Argus Analytics SRC RPD schema

3. Check-in the changes, and save the RPD.

   Ignore the warning messages that appear during the consistency check.

4. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics (*http://obieeser.com:port/analytics*) with WebLogic user credentials.

5. Go to Security > Administration > Manage Privileges.

   For a list of privileges assigned to the BI Application roles, refer to Section 2.5.6, "OBIEE Default Application Roles."

6. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 2.5.5, "OBIEE Catalog Folder-level Permissions")

7. Create OBIEE Groups and Users. (See Section 2.5.3, "Creating Users and Groups in OBIEE")

2.5.2.1.2 Importing the BAR file when creating a new OBIEE Instance

1. Copy the BAR file from *<Argus Analytics Home>\report\ssi.bar* to a machine where the OBIEE is installed.

   Or, when creating an instance in OBIEE 12c, on the OBIEE Initial Application wizard screen, select **Your own existing BI Application from export bunder (.jar file)** option, and enter the **Path** of the *Argus Analytics ssi.bar* file.

2. To modify the Connection Pool Settings:

   a. From the following path, right click the **admintool.cmd** file, and click **Run as Administrator**.

      <MiddlewareHome>\user_projects\domains\bi\bitools\bin

      The Oracle BI Administration Tool opens.

Note: If OBIEE is installed on a Unix or Linux machine, then you must setup the Oracle Business Intelligence Developer Client tool on any Windows machine to access the BI Administration Tool.

See Appendix A, "Creating ODBC Connection for OBIEE Administration Tool."

---

b. To open the RPD, select the online mode, and enter the WebLogic user credentials.

Note:

You must set the Open Database Connectivity (ODBC).

To open the RPD in online mode on Unix or Linux, set the ODBC on a Windows machine where OBIEE client is installed, and open the RPD.

---

c. Click the **Connection Pool**, and modify the **Data source name**, **User name**, and **Password**.

Modify both the following connection pools:

-Under OPVA_DWH database:

* OPVA_CP:

Data Source Name—Argus Analytics database TNS Name

User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

Password—Password for Argus Analytics DWH RPD schema

* OPVA_CP_InitBlocks:

Data Source Name—Argus Analytics database TNS Name

User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

Password—Password for Argus Analytics DWH RPD schema

- Under OPVA_SRC database:

* OPVA_CP:

Data Source Name—Argus Safety database TNS Name

User name—Argus Analytics SRC RPD schema <AN_SRC_RPD>

Password—Password for Argus Analytics SRC RPD schema

3. Check-in the changes, and save the RPD.

Ignore the warning messages that appear during the consistency check.

4. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics (*http://obieeser.com:port/analytics*) with WebLogic user credentials.

5. Go to Security > Administration > Manage Privileges.

For a list of privileges assigned to the BI Application roles, refer to Section 2.5.6, "OBIEE Default Application Roles."

6. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 2.5.5, "OBIEE Catalog Folder-level Permissions")

7. Create OBIEE Groups and Users. (See Section 2.5.3, "Creating Users and Groups in OBIEE")

2.5.2.2 Configuring OBIEE Repository and Web Catalog Manually

1. Copy the RPD, and Catalog files from *<Argus Analytics Home>\report\opva.rpd and report\catalog\opva.zip folders* to a machine where the OBIEE is installed.

2. Open the RPD Admin tool in offline mode from the following path:

   <Middleware Home>\user_projects\domains\bi\bitools\bin\admintool.cmd

3. Open the **opva.rpd** file in offline mode. (The default password of the repository is opva1234.)

4. Click the **Connection Pool**, and modify the **Data source name**, **User name**, and **Password**.

   Modify the following connection pools:

   -Under OPVA_DWH database:

   * OPVA_CP:

     Data Source Name—Argus Analytics database TNS Name

     User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

     Password—Password for Argus Analytics DWH RPD schema

   * OPVA_CP_InitBlocks:

     Data Source Name—Argus Analytics database TNS Name

     User name—Argus Analytics DWH RPD schema <AN_DWH_RPD>

     Password—Password for Argus Analytics DWH RPD schema

   - Under OPVA_SRC database:

   * OPVA_CP:

     Data Source Name—Argus Safety database TNS Name

     User name—Argus Analytics SRC RPD schema <AN_SRC_RPD>

     Password—Password for Argus Analytics SRC RPD schema

5. Save the changes, and close the RPD.

6. From the command prompt:

   a. Navigate to the *<Middleware Home>\user_projects\domains\bi\bitools\bin*

   b. Run the following command:

      data-model-cmd.cmd uploadrpd -I <RPDname> [-W <RPDpwd>] -U <cred_username> [-P <cred_password>] -SI <service_instance>

      For example,

      data-model-cmd.cmd uploadrpd -I C:\temp\opva.rpd -W opva1234 -U weblogic -P weblogic1 -SI ssi

      Note: In Linux, execute the data-model-cmd.sh command with same inputs.

7. Login to the Enterprise Manager with the WebLogic credentials.

8. Click **Target Navigation**.

The Target Navigation drop-down menu appears.

9. Go to Business Intelligence > biinstance.

   The Business Intelligence Instance screen appears.

10. From the Availability tab, select **Processes**, and click **Stop All**.

    A confirmation dialog box appears.

11. Click **Yes**.

    All the running processes are stopped.

12. Extract the contents of Argus Analytics catalog **opva.zip** into <*Oracle_Home*>*user_projects**domains**bi**bidata**service_instances**ssi**metadata**content**catalog**root**shared* folder.

13. Go to Enterprise Manager, from the Availability tab, select **Processes**, and click **Start All.**

    A confirmation dialog box appears.

14. Click **Yes**.

15. Create User Groups and Users manually in Admin Console. (See Section 2.5.3, "Creating Users and Groups in OBIEE.").

16. Create Roles and policies manually in Enterprise Manager. (See Section 2.5.4, "Creating Roles and Policies with Fusion Middleware Control.")

17. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics (*http://obieeser.com:port/analytics*) with WebLogic user credentials.

18. Go to Security > Administration > Manage Privileges.

    For a list of privileges assigned to these roles, refer to Section 2.5.6, "OBIEE Default Application Roles."

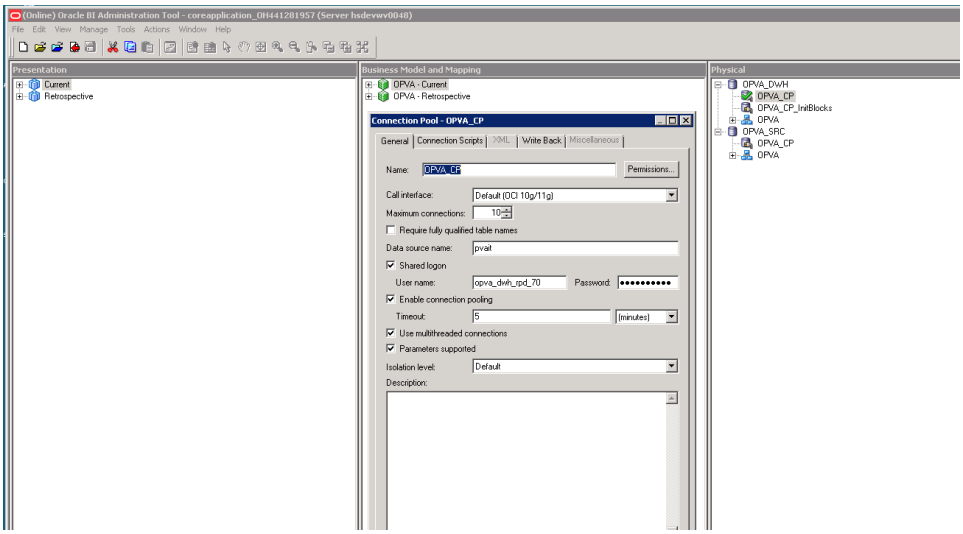
19. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 2.5.5, "OBIEE Catalog Folder-level Permissions")

2.5.2.3 Post-deployment of the Oracle Argus Analytics RPD

Open the Oracle Argus Analytics RPD in the Administration Tool in online mode and specify the details, as mentioned below:

1. Repository Password: Enter the password set in Section 2.5.2, "Deployment of OBIEE Repository and Catalog", as mentioned in the **Note** before Step 1.
2. User: weblogic
3. Password: Password for the user mentioned above

Figure 2–1 The Oracle Argus Analytics RPD Screen



Changing the Connection Pool Settings

Once the Argus Analytics RPD is opened in online mode, change the Connection Pool settings, as follows:

1. Change the OPVA_DWH -> OPVA_CP and OPVA_CP_InitBlocks to point to the Argus Analytics DWH RPD Schema <AN_DWH_RPD>, created during installation, on the Argus Analytics DB Instance.
2. Data Source Name: TNS name entry for Argus Analytics DB Instance.
3. User Name: <AN_DWH_RPD> [the schema name specified for the AN DWH RPD Schema during instalation].
4. Password: The password specified for the <AN_DWH_RPD> schema.
5. Change the OPVA_SRC -> OPVA_CP to the Argus Safety Source RPD schema <AN_SRC_RPD>, created during installation, on the Argus Safety Instance.
6. Data Source Name: TNS name entry for Argus Safety DB Instance.
7. User Name: <AN_SRC_RPD> [the schema name specified for the AN Source RPD schema during installation].
8. Password: The password specified for the <AN_SRC_RPD> schema.
9. Save the RPD.

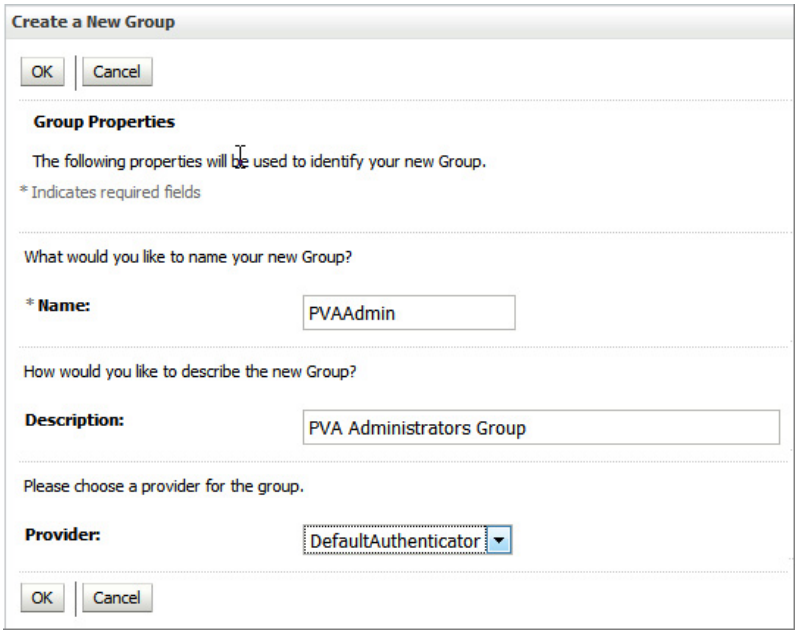
2.5.3 Creating Users and Groups in OBIEE

To create groups in Fusion Middleware Control:

1. Open the WebLogic Administration Console.
2. Navigate to Security Realms > myrealm > Users and Groups > Groups tab.
3. From the Groups section, and click **New**.

   The Create a New Group dialog box appears.
4. Create the following groups by entering the **Name** and **Description**, and click **OK.**
   - PVAAdmin

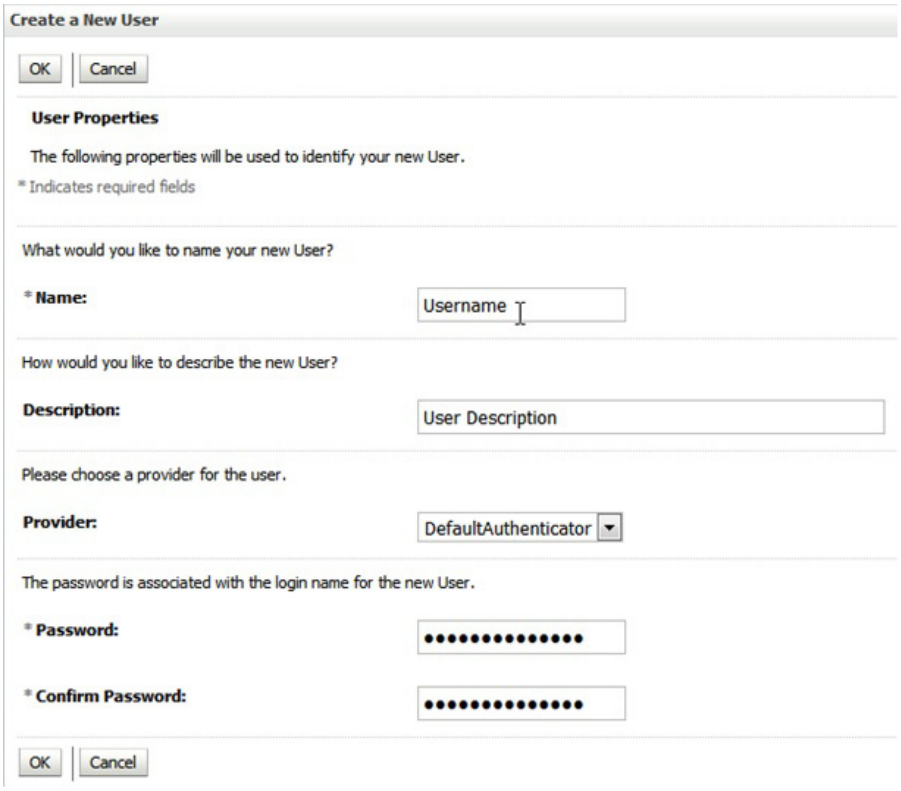
- PVASafetyGroup
- PVASafetyConsumersGroup



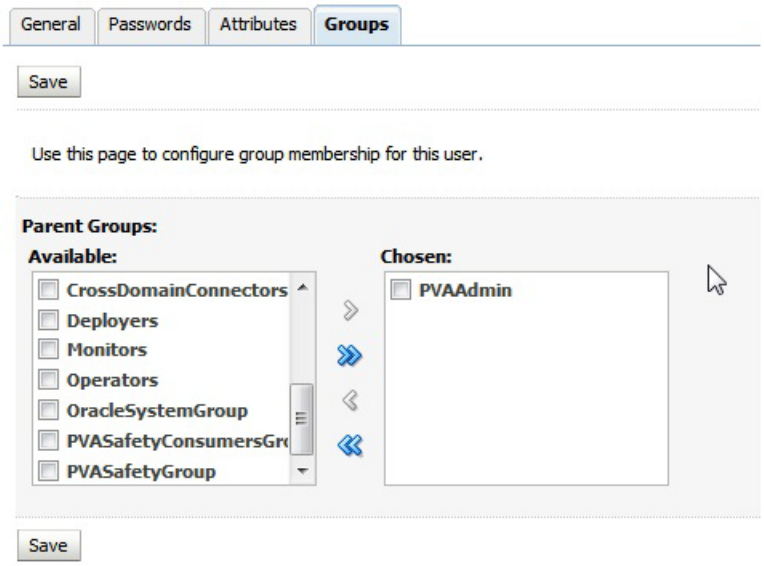
To create users in the Fusion Middleware Control:

1. Open the WebLogic Administration Console.
2. Navigate to Security Realms > myrealm > Users and Groups > Users.
3. From the Users section, and click **New**.

   The Create a New User dialog box appears.



4. Enter the following fields, and click **OK**.
   a. Name
   b. Description
   c. Provider
   d. Password
   e. Confirm Password
5. To assign a group to the user, from the Groups tab, select a Group, and click **Save**.



2.5.4 Creating Roles and Policies with Fusion Middleware Control

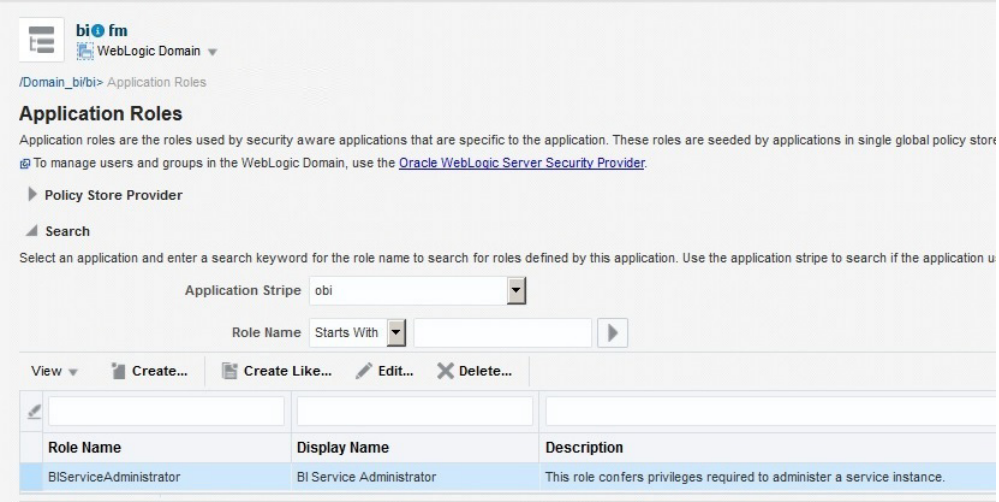
> **Note:** This section is applicable only when you manually upload the RPD file and Catalog. For more details, refer to Section 2.5, "Configuring the OBIEE Repository and Webcatalog.".

To create new application roles:

1. Login to Fusion Middleware Control Enterprise Manager.
2. Go to WebLogic Domain > Security > Application Roles.

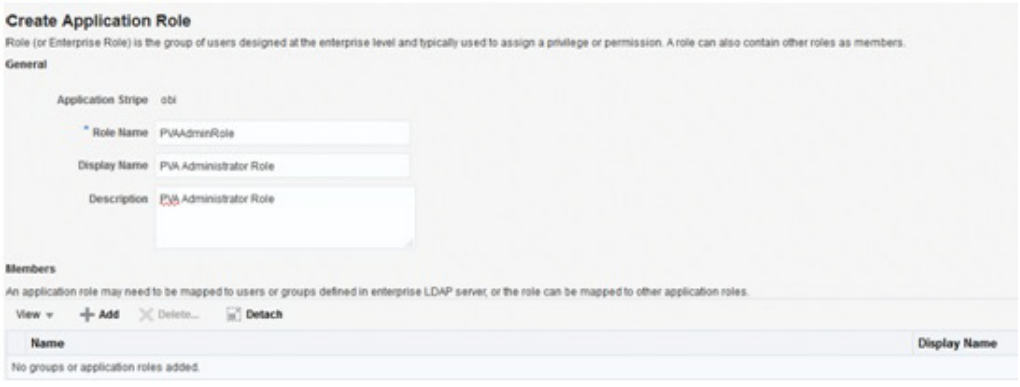
   The Application Roles dialog box appears.
3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search** .

   The default role available in clean slate installation appears.



4. Click **Create**.

   The Create Application Role dialog box appears.
5. In the **Role Name** field, enter **PVAAdminRole**.

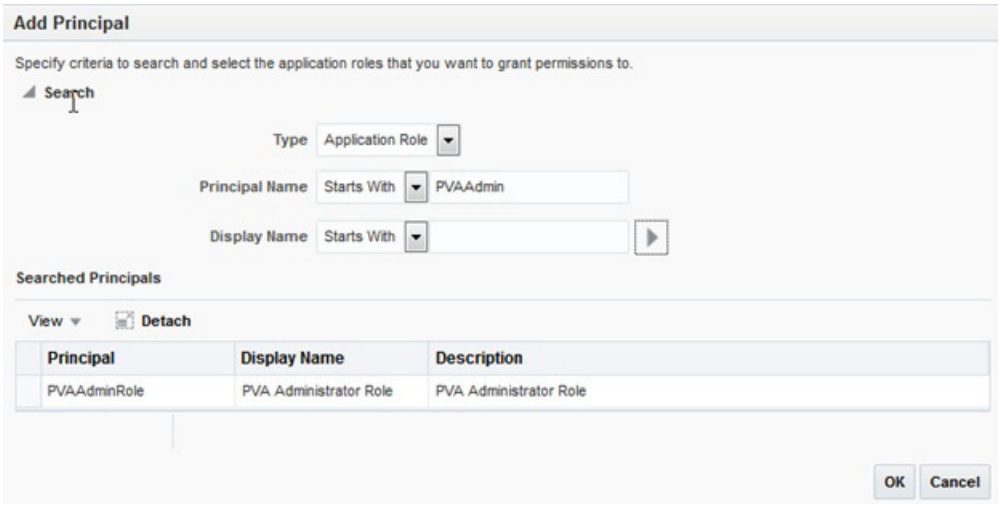


6. From the Members section, click **+Add**.

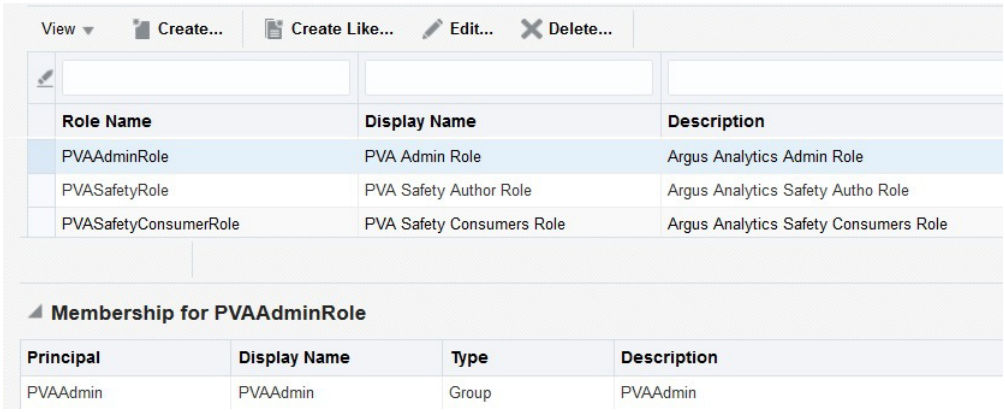
   The Add Principal dialog box appears.
7. From the **Type** drop-down list, select **Group**, and click **Search**.

A list of principals appears.

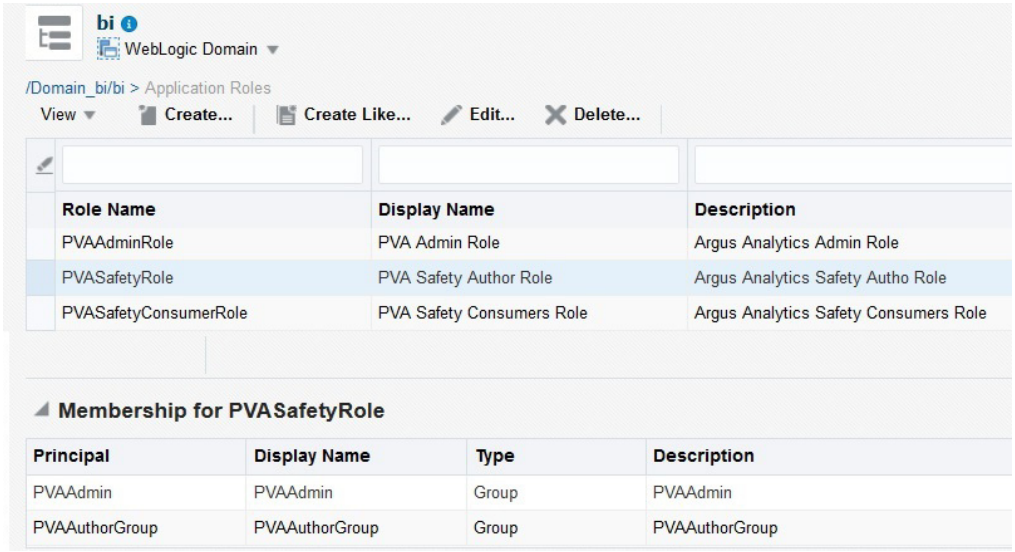
8. From the list of Searched Principals, select **PVAAdmin**, and click **OK**.



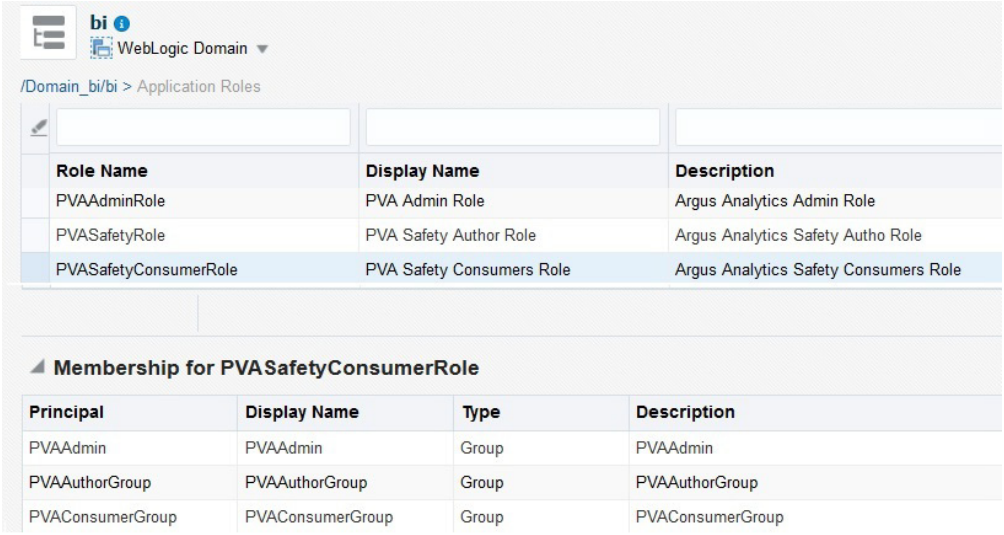
The Membership for **PVAAdminRole** appears as below:



9. To add **PVASafetyRole**, repeat from Step 4 to Step 8.



10. To add **PVASafetyConsumerRole**, repeat from Step 4 to Step 8.



Note: For more details, refer to *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition > Section 2.4.2.2 Creating an Application Role* in *https://docs.oracle.com/middleware/1221/biee/BIESC/authentication.htm#BIESC363*

To create new application policy:

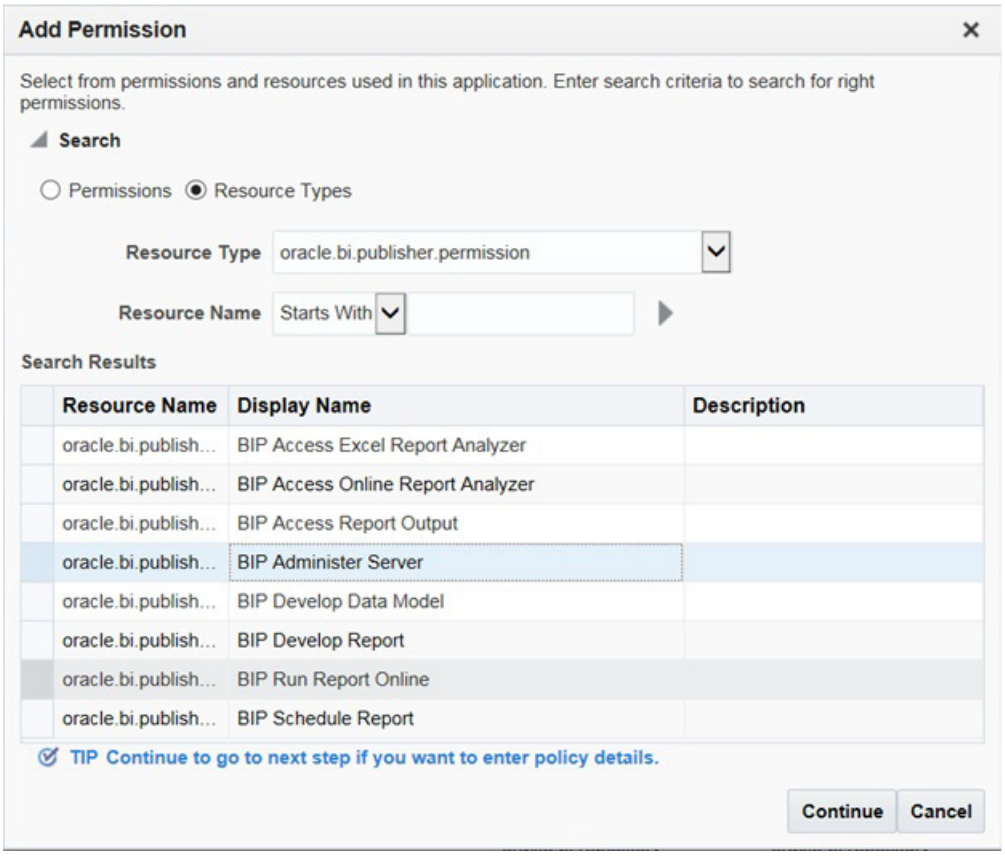
1. Login to Fusion Middleware Control Enterprise Manager.
2. Go to WebLogic Domain > Security > Application Policies.

   The Application Policies screen appears.
3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.
4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.
5. From the **Type** drop-down list, select **Application Role**, and click **Search** .
6. From the list of Searched Principals, select **PVAAdminRole**, and click **OK**.
7. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.



8. Select the **Resource Types** radio button.
9. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.
10. From the Search Results, select **oracle.bi.publisher.permission** (BIP Administer Server), and click **Continue**.

    The Add Permission dialog box appears.
11. For **Permission Actions**, select **All** (_all_), and click **Select**.
12. Repeat from Step 4 to Step 11, to add the following:

Policy Name/Principal	Resource Type	Resource Name	Permission Actions
PVAAdminRole	oracle.bi.catalog	*	manage
	oracle.bi.repository	oracle.bi.repository	manage
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanager.permission	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
	oracle.bi.server.permission	oracle.bi.server.manageRepositories	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
PVASafetyRole	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	schedule
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	*
PVASafetyConsumerRole	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	READ, EXECUTE
	oracle.bi.publisher.permission	BIP Access Excel Report Analyzer	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_

Note:

For more details, refer to *Oracle® Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition >Section 2.4.3 Creating Application Policies Using Fusion Middleware Control* from *http://docs.oracle.com/middleware/1221/biee/BIESC/authentication.htm#BIESC767*.

2.5.5 OBIEE Catalog Folder-level Permissions

1. Go to Catalog > Shared Folders > Tasks > Permissions.

   The Permissions dialog box appears.

2. Set the Permissions as follows:

Accounts	Permissions
PVA Administrator Role	Full Control
PVA Safety Author Role	Full Control
PVA Safety Consumers Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

   a. Select **Apply Permissions** to sub-folders.

   b. Select **Permissions** to items within folder.

   c. Click **OK**.

3. For each of the following folders, set the account permissions:

   - Shared Folders > Shared Folder > **Current** > Permissions
   - Shared Folders > Shared Folder > **Personal User** > Permissions
   - Shared Folders > Shared Folder > **Retrospective** > Permissions

Accounts	Permissions
PVA Administrator Role (Owner)	Full Control
PVA Safety Author Role	Full Control
PVA Safety Consumers Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

   a. Select **Apply Permissions** to sub-folders.

   b. Select **Permissions** to items within folder.

   c. Click **OK**.

2.5.6 OBIEE Default Application Roles

To view and administer privileges of Oracle Business Intelligence components:

1. Login to OBIEE Analytics with WebLogic user credentials.
2. Go to Security > Administration > Manage Privileges.

Note: Create these privileges only when you manually upload the RPD and Catalog.

You do not need to create these privileges when you import the BAR file.

You must NOT remove the privileges already present in the Manage Privileges tab for the various components. The below mentioned default role grants should only be appended to the existing grants in OBIEE components.

Component	Privilege	Default Role Granted
Access	Access to Dashboards	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Answers	PVA Safety Author Role, BI Service Administrator
Access	Access to BI Composer	PVA Safety Author Role, BI Service Administrator
Access	Access to Delivers	PVA Safety Author Role, BI Service Administrator
Access	Access to Briefing Books	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Mobile	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Administration	PVA Admin Role, BI Service Administrator
Access	Access to Segments	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Segment Trees	PVA Safety Author Role, BI Service Administrator
Access	Access to List Formats	PVA Safety Author Role, BI Service Administrator
Access	Access to Metadata Dictionary	PVA Safety Author Role, BI Service Administrator
Access	Access to Oracle BI for Microsoft Office	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Oracle BI Client Installer	PVASafetyConsumerRole, BI Service Administrator
Access	Catalog Preview Pane UI	PVASafetyConsumerRole, BI Service Administrator
Access	Access to Export	PVASafetyConsumerRole, BI Service Administrator
Access	Access to KPI Builder	PVA Safety Author Role, BI Service Administrator
Access	Access to Scorecard	PVASafetyConsumerRole, BI Service Administrator
Actions	Create Navigate Actions	PVASafetyConsumerRole, BI Service Administrator
Actions	Create Invoke Actions	PVA Safety Author Role, BI Service Administrator

Component	Privilege	Default Role Granted
Actions	Save Actions containing embedded HTML	PVA Admin Role, BI Service Administrator
Admin: Catalog	Change Permissions	PVA Safety Author Role, BI Service Administrator
Admin: Catalog	Toggle Maintenance Mode	PVA Admin Role, BI Service Administrator
Admin: General	Manage Sessions	PVA Admin Role, BI Service Administrator
Admin: General	Create Dashboards	PVA Safety Author Role, BI Service Administrator
Admin: General	See sessions IDs	PVA Admin Role, BI Service Administrator
Admin: General	Change Log Configuration	PVA Admin Role, BI Service Administrator
Admin: General	Issue SQL Directly	PVA Admin Role, BI Service Administrator
Admin: General	View System Information	PVA Admin Role, BI Service Administrator
Admin: General	Performance Monitor	PVA Admin Role, BI Service Administrator
Admin: General	Manage Agent Sessions	PVA Admin Role, BI Service Administrator
Admin: General	Manage Device Types	PVA Admin Role, BI Service Administrator
Admin: General	Manage Map Data	PVA Admin Role, BI Service Administrator
Admin: General	See privileged errors	PVA Admin Role, BI Service Administrator
Admin: General	See SQL issued in errors	PVASafetyConsumerRole, BI Service Administrator
Admin: General	Manage Global Variables	PVA Admin Role, BI Service Administrator
Admin: General	Diagnose BI Server Query	Denied: Authenticated User
Admin: General	Manage Marketing Jobs	PVA Safety Author Role, BI Service Administrator
Admin: General	Manage Marketing Defaults	PVA Admin Role, BI Service Administrator
Admin: Security	Manage Catalog Accounts	PVA Admin Role, BI Service Administrator
Admin: Security	Manage Privileges	PVA Admin Role, BI Service Administrator
Admin: Security	Set Ownership of Catalog Objects	PVA Admin Role, BI Service Administrator
Admin: Security	User Population - Can List Users	PVASafetyConsumerRole, BI Service Administrator, BI System
Admin: Security	User Population - Can List Catalog Groups	PVASafetyConsumerRole, BI Service Administrator, BI System
Admin: Security	User Population - Can List Application Roles	PVASafetyConsumerRole, BI Service Administrator, BI System
Admin: Security	Access to Permissions Dialog	PVASafetyConsumerRole, BI Service Administrator
Briefing Book	Add To or Edit a Briefing Book	PVA Safety Author Role, BI Service Administrator
Briefing Book	Download Briefing Book	PVASafetyConsumerRole, BI Service Administrator
Briefing Book	Add to Snapshot Briefing Book	PVASafetyConsumerRole, BI Service Administrator
Catalog	Personal Storage (My Folders and My Dashboard)	PVASafetyConsumerRole, BI Service Administrator
Catalog	Reload Metadata	PVA Admin Role, BI Service Administrator

Component	Privilege	Default Role Granted
Catalog	See Hidden Items	PVA Safety Author Role, BI Service Administrator
Catalog	Create Folders	PVA Safety Author Role, BI Service Administrator
Catalog	Archive Catalog	PVA Admin Role, BI Service Administrator
Catalog	Unarchive Catalog	PVA Admin Role, BI Service Administrator
Catalog	Upload Files	PVA Admin Role, BI Service Administrator
Catalog	Perform Global Search	PVA Safety Author Role, BI Service Administrator
Catalog	Perform Extended Search	PVA Safety Author Role, BI Service Administrator
Conditions	Create Conditions	PVA Safety Author Role, BI Service Administrator
Dashboards	Save Customizations	PVASafetyConsumerRole, BI Service Administrator
Dashboards	Assign Default Customizations	PVA Safety Author Role, BI Service Administrator
Dashboards	Create Bookmark Links	PVASafetyConsumerRole, BI Service Administrator
Dashboards	Create Prompted Links	PVASafetyConsumerRole, BI Service Administrator
Dashboards	Export Entire Dashboard To Excel	PVASafetyConsumerRole, BI Service Administrator
Dashboards	Export Single Dashboard Page To Excel	PVASafetyConsumerRole, BI Service Administrator
Formatting	Save System-Wide Column Formats	PVA Admin Role, BI Service Administrator
Home and Header	Access Home Page	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Access Catalog UI	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Access Catalog Search UI	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Access Rapid Search UI	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Simple Search Field	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Advanced Search Link	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Open Menu	PVASafetyConsumerRole, BI Service Administrator
Home and Header	New Menu	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Help Menu	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Dashboards Menu	PVASafetyConsumerRole, BI Service Administrator

Component	Privilege	Default Role Granted
Home and Header	Favorites Menu	PVASafetyConsumerRole, BI Service Administrator
Home and Header	My Account Link	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Custom Links	PVASafetyConsumerRole, BI Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Data Loader	Denied: Authenticated User
My Account	Access to My Account	PVASafetyConsumerRole, BI Service Administrator
My Account	Change Preferences	PVASafetyConsumerRole, BI Service Administrator
My Account	Change Delivery Options	PVASafetyConsumerRole, BI Service Administrator
Answers	Create Views	PVA Safety Author Role, BI Service Administrator
Answers	Create Prompts	PVA Safety Author Role, BI Service Administrator
Answers	Access Advanced Tab	PVA Safety Author Role, BI Service Administrator
Answers	Edit Column Formulas	PVA Safety Author Role, BI Service Administrator
Answers	Save Content with HTML Markup	PVA Admin Role, BI Service Administrator
Answers	Enter XML and Logical SQL	PVA Safety Author Role, BI Service Administrator
Answers	Edit Direct Database Analysis	PVA Admin Role, BI Service Administrator
Answers	Create Analysis From Simple SQL	PVA Admin Role, BI Service Administrator
Answers	Create Advanced Filters and Set Operations	PVA Safety Author Role, BI Service Administrator
Answers	Save Filters	PVA Safety Author Role, BI Service Administrator
Answers	Save Column	PVA Safety Author Role, BI Service Administrator
Answers	Add EVALUATE_PREDICATE Function	PVA Safety Author Role, BI Service Administrator
Answers	Execute Direct Database Analysis	PVA Admin Role, BI Service Administrator
Answers	Upload Images	PVA Safety Author Role, BI Service Administrator
Delivers	Create Agents	PVA Safety Author Role, BI Service Administrator
Delivers	Publish Agents for Subscription	PVA Safety Author Role, BI Service Administrator
Delivers	Deliver Agents to Specific or Dynamically Determined Users	PVA Admin Role, BI Service Administrator

Component	Privilege	Default Role Granted
Delivers	Chain Agents	PVA Safety Author Role, BI Service Administrator
Delivers	Modify Current Subscriptions for Agents	PVA Admin Role, BI Service Administrator
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	PVASafetyConsumerRole, BI Service Administrator
Scorecard	Create/Edit Scorecards	PVA Safety Author Role, BI Service Administrator
Scorecard	View Scorecards	PVASafetyConsumerRole, BI Service Administrator
Scorecard	Create/Edit Objectives	PVA Safety Author Role, BI Service Administrator
Scorecard	Create/Edit Initiatives	PVA Safety Author Role, BI Service Administrator
Scorecard	Create Views	PVA Safety Author Role, BI Service Administrator
Scorecard	Create/Edit Causes And Effects Linkages	PVA Safety Author Role, BI Service Administrator
Scorecard	Create/Edit Perspectives	PVA Safety Author Role, BI Service Administrator
Scorecard	Add Annotations	PVASafetyConsumerRole, BI Service Administrator
Scorecard	Override Status	PVASafetyConsumerRole, BI Service Administrator
Scorecard	Create/Edit KPIs	PVA Safety Author Role, BI Service Administrator
Scorecard	Write Back to Database for KPI	PVASafetyConsumerRole, BI Service Administrator
Scorecard	Add Scorecard Views To Dashboards	PVASafetyConsumerRole, BI Service Administrator
List Formats	Create List Formats	PVA Safety Author Role, BI Service Administrator
List Formats	Create Headers and Footers	PVA Safety Author Role, BI Service Administrator
List Formats	Access Options Tab	PVA Safety Author Role, BI Service Administrator
List Formats	Add/Remove List Format Columns	PVA Admin Role, BI Service Administrator
Segmentation	Create Segments	PVA Safety Author Role, BI Service Administrator
Segmentation	Create Segment Trees	PVA Safety Author Role, BI Service Administrator
Segmentation	Create/Purge Saved Result Sets	PVA Admin Role, BI Service Administrator
Segmentation	Access Segment Advanced Options Tab	PVA Admin Role, BI Service Administrator
Segmentation	Access Segment Tree Advanced Options Tab	PVA Admin Role, BI Service Administrator

Component	Privilege	Default Role Granted
Segmentation	Change Target Levels within Segment Designer	PVA Safety Author Role, BI Service Administrator
Mobile	Enable Local Content	PVASafetyConsumerRole, BI Service Administrator
Mobile	Enable Search	PVASafetyConsumerRole, BI Service Administrator
SOAP	Access SOAP	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Impersonate as system user	BI System
SOAP	Access MetadataService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access ScorecardAssessmentService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access MsgdbService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access ReportEditingService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access KPIAssessmentService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access ConditionEvaluationService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access SecurityService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access Tenant Information	BI System
SOAP	Access SchedulerService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access DashboardService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access ScorecardMetadataService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access JobManagementService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access CatalogIndexingService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access UserPersonalizationService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access AnalysisExportViewsService Service	PVASafetyConsumerRole, BI Service Administrator
SOAP	Access CatalogService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access AdministrationSOAPService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access HtmlViewService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
SOAP	Access XmlGenerationService Service	PVASafetyConsumerRole, BI Service Administrator, BI System

Component	Privilege	Default Role Granted
SOAP	Access IBotService Service	PVASafetyConsumerRole, BI Service Administrator, BI System
Subject Area: "Current"	Access within Oracle BI Answers	PVA Admin Role, BI Service Administrator
Subject Area: "Retrospective"	Access within Oracle BI Answers	PVA Admin Role, BI Service Administrator
View Canvas	Add/Edit Canvas View	PVA Safety Author Role, BI Service Administrator
View Column Selector	Add/Edit Column Selector View	PVA Safety Author Role, BI Service Administrator
View Compound Layout	Add/Edit Compound Layout View	PVA Safety Author Role, BI Service Administrator
View Contribution Wheel	Add/Edit Contribution Wheel View	PVA Safety Author Role, BI Service Administrator
View Graph	Add/Edit Graph View	PVA Safety Author Role, BI Service Administrator
View Funnel	Add/Edit Funnel View	PVA Safety Author Role, BI Service Administrator
View Gauge	Add/Edit Gauge View	PVA Safety Author Role, BI Service Administrator
View Micro Chart	Add/Edit Micro Chart View	PVA Safety Author Role, BI Service Administrator
View Filters	Add/Edit Filters View	PVA Safety Author Role, BI Service Administrator
View Dashboard Prompt	Add/Edit Dashboard Prompt View	PVA Safety Author Role, BI Service Administrator
View Performance Tile	Add/Edit Performance Tile View	PVA Safety Author Role, BI Service Administrator
View Heat Matrix	Add/Edit Heat Matrix View	PVA Safety Author Role, BI Service Administrator
View Static Text	Add/Edit Static Text View	PVA Safety Author Role, BI Service Administrator
View Javascript view	Edit Javascript View	PVA Safety Author Role, BI Service Administrator
View Legend	Add/Edit Legend View	PVA Safety Author Role, BI Service Administrator
View Map	Add/Edit Map View	PVA Safety Author Role, BI Service Administrator
View Narrative	Add/Edit Narrative View	PVA Safety Author Role, BI Service Administrator
View No Results	Add/Edit No Results View	PVA Safety Author Role, BI Service Administrator
View Pivot Table	Add/Edit Pivot Table View	PVA Safety Author Role, BI Service Administrator
View Generic Plugin View	Add/Edit Generic Plugin View View	PVA Safety Author Role, BI Service Administrator
View Report Prompt	Add/Edit Report Prompt View	PVA Safety Author Role, BI Service Administrator

Component	Privilege	Default Role Granted
View Create Segment	Add/Edit Create Segment View	PVA Safety Author Role, BI Service Administrator
View Selection Steps	Add/Edit Selection Steps View	PVA Safety Author Role, BI Service Administrator
View Logical SQL	Add/Edit Logical SQL View	PVA Safety Author Role, BI Service Administrator
View Table	Add/Edit Table View	PVA Safety Author Role, BI Service Administrator
View Create Target List	Add/Edit Create Target List View	PVA Safety Author Role, BI Service Administrator
View Ticker	Add/Edit Ticker View	PVA Safety Author Role, BI Service Administrator
View Title	Add/Edit Title View	PVA Safety Author Role, BI Service Administrator
View Treemap	Add/Edit Treemap View	PVA Safety Author Role, BI Service Administrator
View Trellis	Add/Edit Trellis View	PVA Safety Author Role, BI Service Administrator
View View Selector	Add/Edit View Selector View	PVA Safety Author Role, BI Service Administrator
Write Back	Manage Write Back	PVA Admin Role, BI Service Administrator
Write Back	Write Back to Database	Denied: Authenticated User

2.5.7 Changing the OBIEE RPD Password

To change the 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 password set in Section 2.5.2, "Deployment of OBIEE Repository and Catalog", as mentioned in the **Note** before Step 1.
4. Enter the new password and confirm by entering it again. You must remember this password, and use the same later in the installation process.

2.6 Configuring the OBIEE Help files

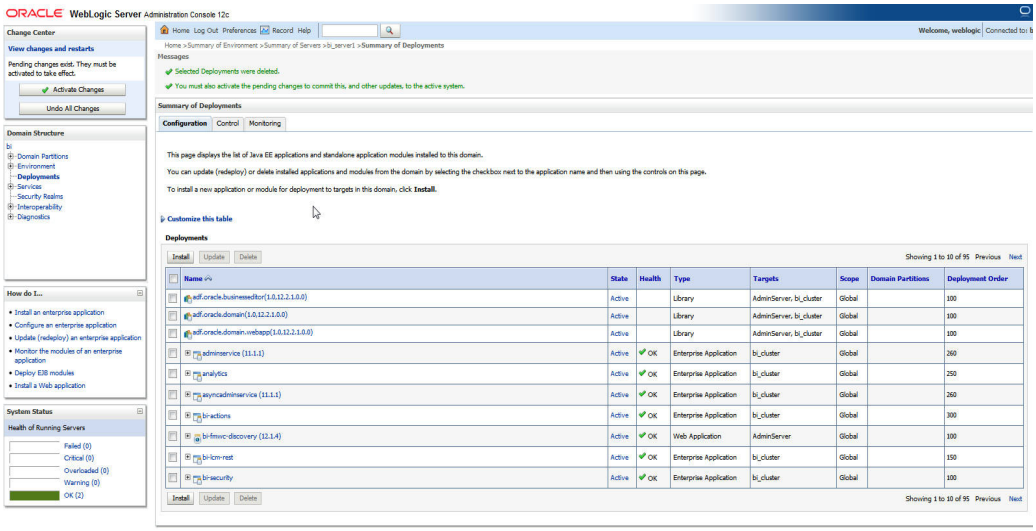
Note: If the OBIEE Server is not the same machine where the installer is run, then copy the opva_help.zip file into the machine where OBIEE server is installed.

2.6.1 Configuring the Help links in the Dashboards and Reports

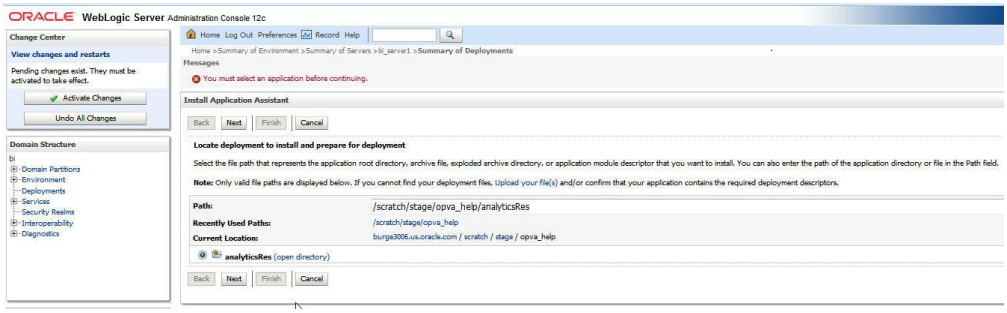
1. Extract the contents of the opva_help.zip file at any location on the OBIEE Server. For example, e.g */scratch/stage/opva_help*

   The opva_help folder contains analyticsRes folder.

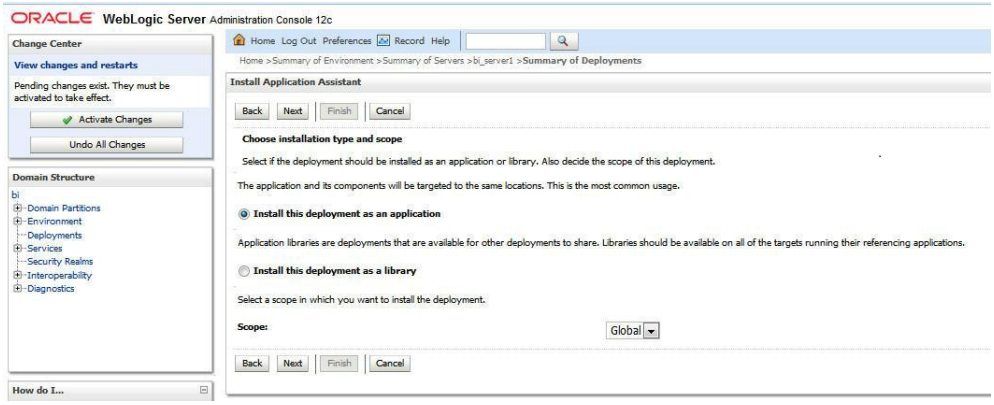
2. Log in to Console (Log in to the Weblogic Server).
3. Navigate to Deployments.
4. Click **Lock & Edit** in the left pane to enable the **Install** button.



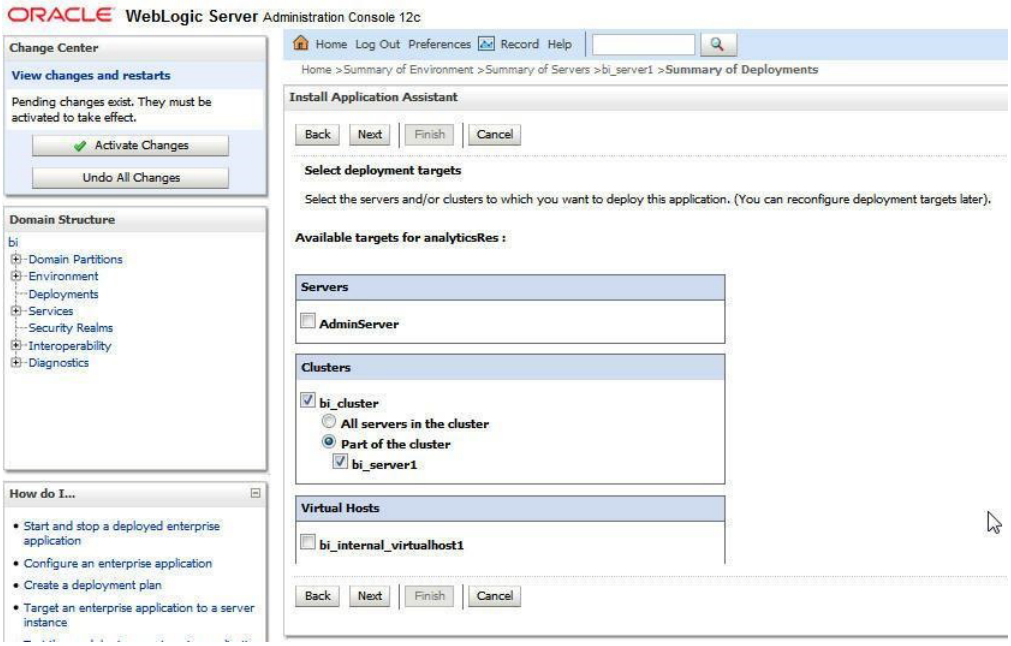
5. Click **Install**, and navigate to the location where opva_help.zip was extracted in Step 1.
6. Select **analyticsRes**, and click **Next**.



7. Select **Install this deployment as an application** (default), and click **Next**.



8. Select **Deployment targets**, choose **bi_server1**, and click **Next**.

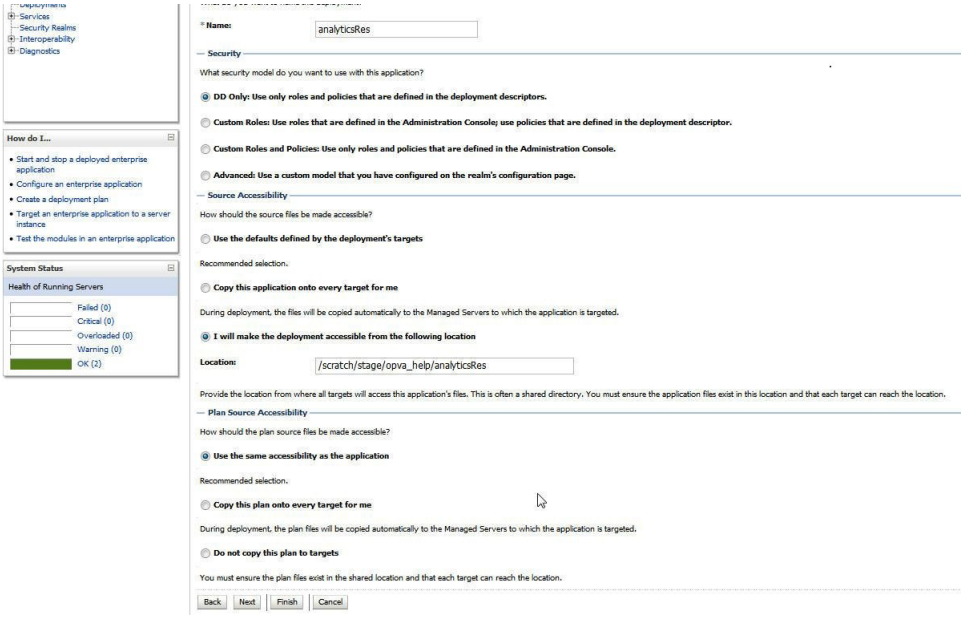


9. Under **Source accessibility:**

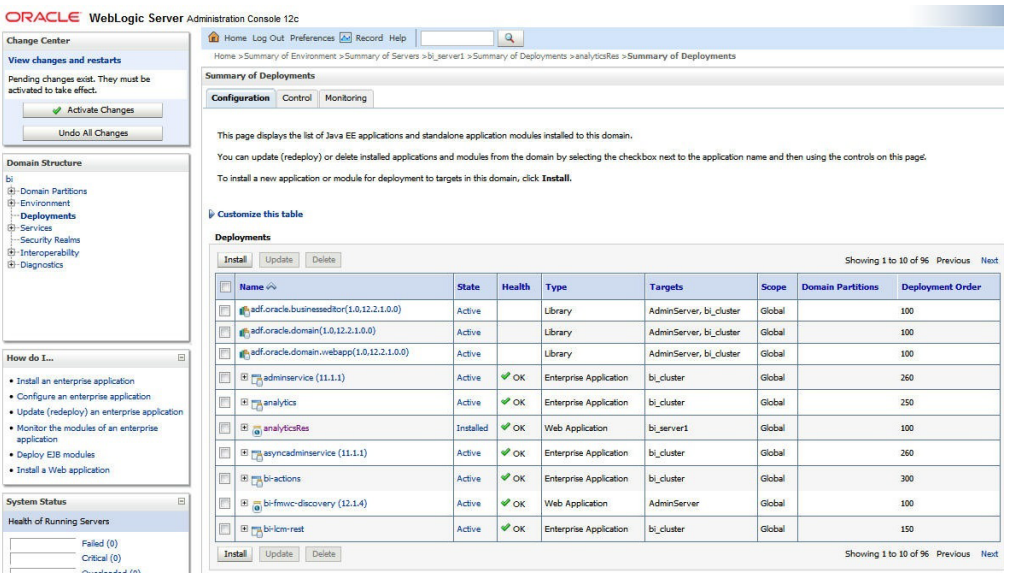
   Select **I will make the deployment accessible from the following location** option, and select the path for analyticsRes as selected in step 6.

   For example, */scratch/stage/opva_help/analyticsRes*

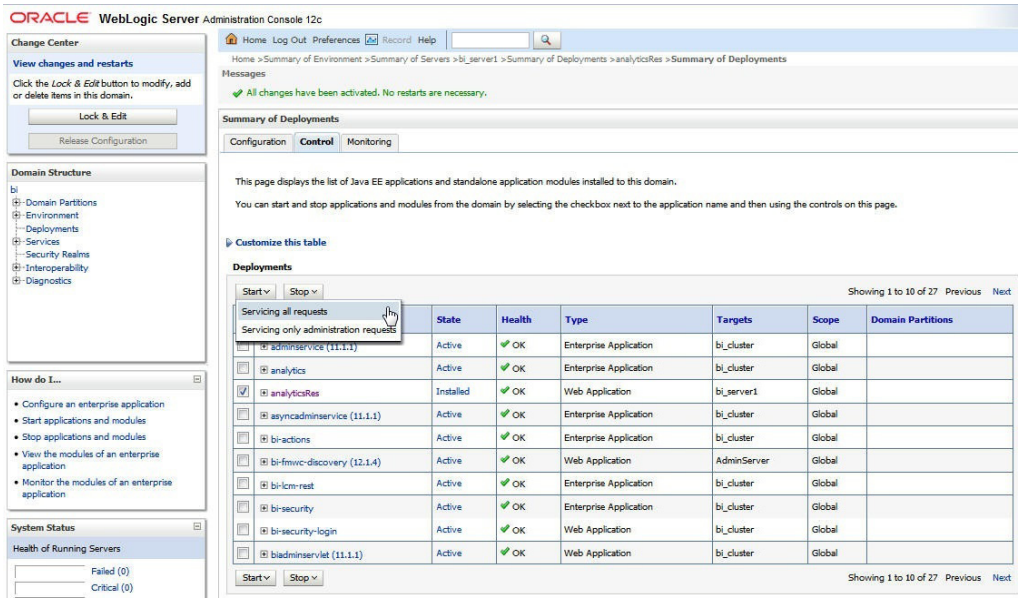
10. Click **Finish**.



The **analyticsRes** appears under Deployments.



11. Click **Active Changes**, and navigate to the Control tab.
12. Select **analyticsRes**, and click **Start**.



13. Start the Application Assistant, and click **Yes**.

The **analyticsRes State** is activated after starting the application assistant. Logout from the Console.

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

    When 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 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:

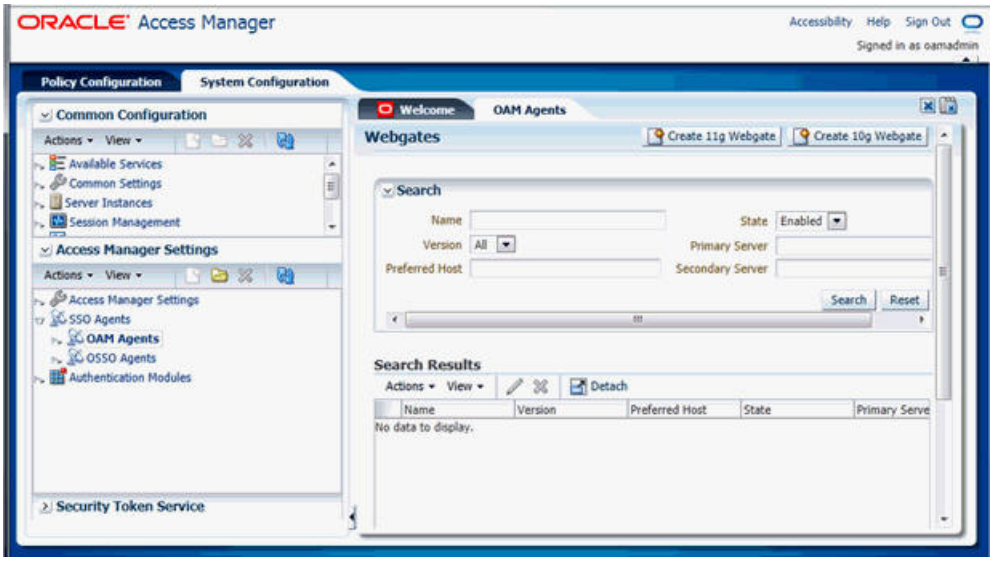
- There must be an OAM 11g installation configured to work with the desired LDAP (for example, OID), as the identity data-store.
- User profiles must exist in the LDAP server as well as in Argus Safety with the same credentials (login information).
- Oracle Web Tier 11.1.1.3 (or higher) must be installed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

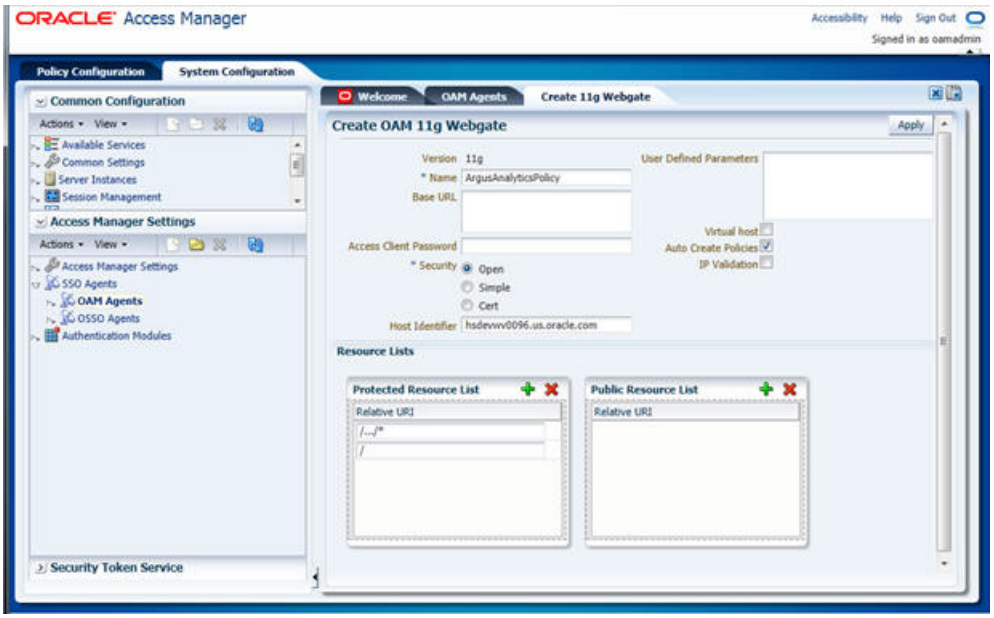
Figure 2–2 Viewing the OAM Agents Page



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

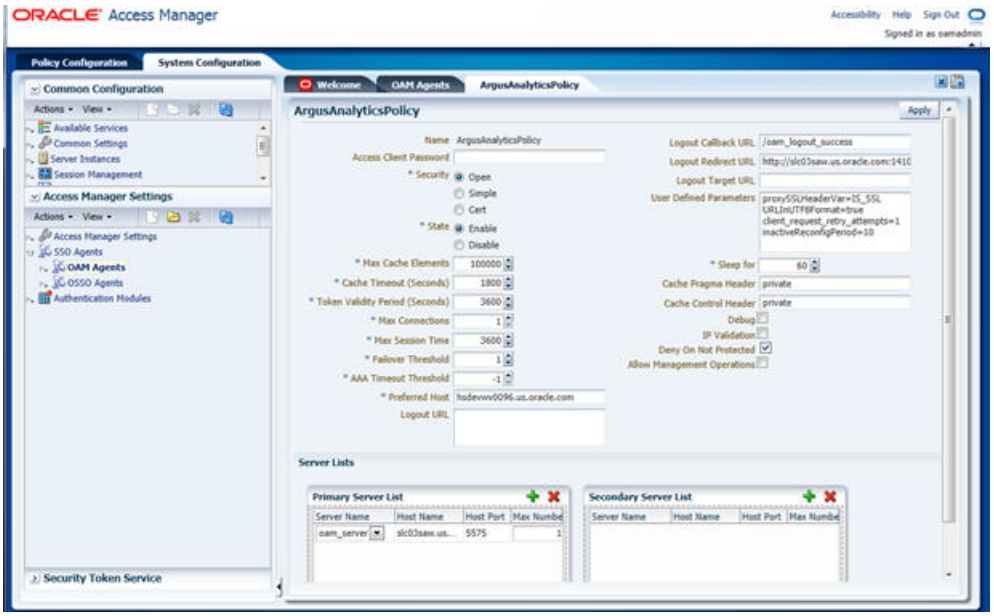
   Note: The <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate.

Figure 2–3 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 2–4 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.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.

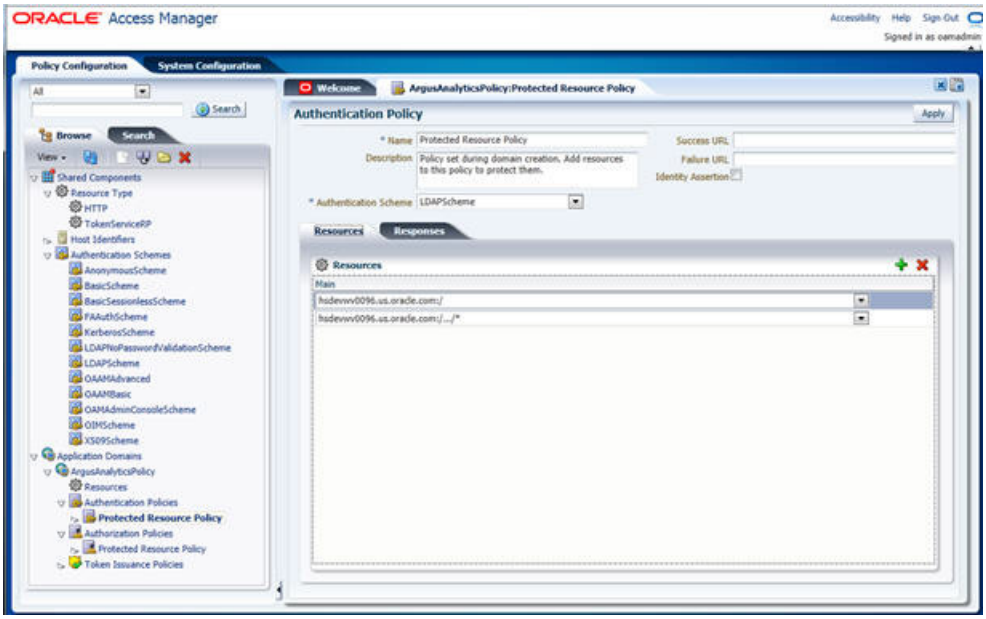
    Example:

Hostname	Port
obiee_server.oracle.com	
obiee_server.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:

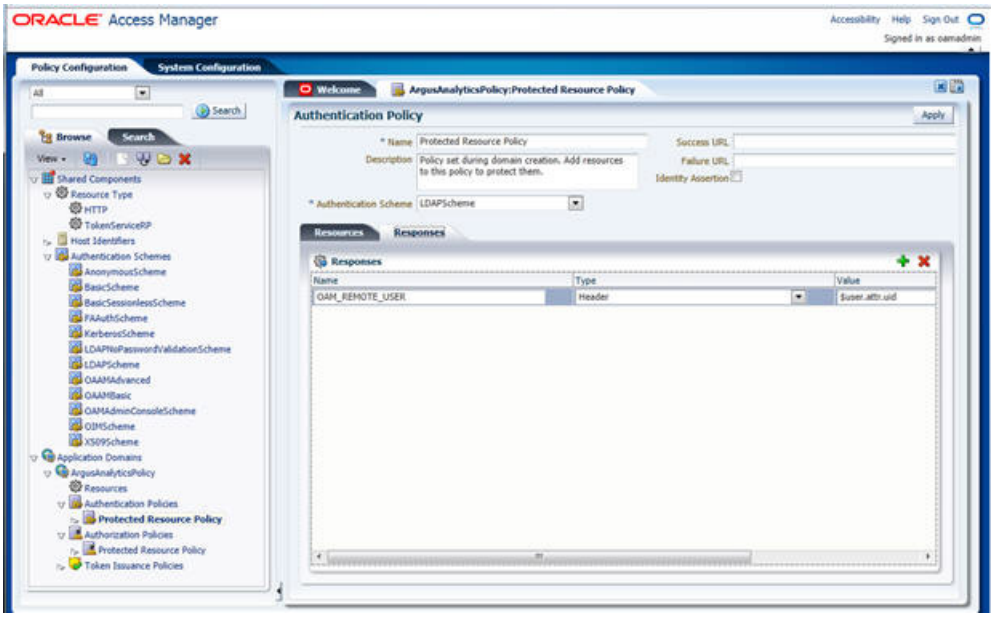
- /
- /…/*

Figure 2–5 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]

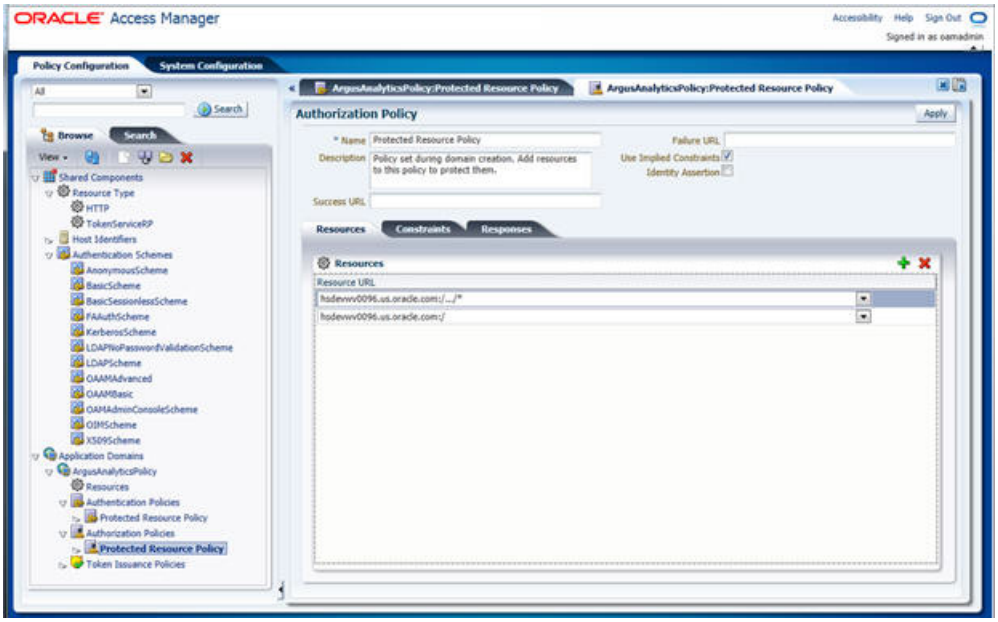
Figure 2–6 Adding the Response Variables to Authentication Protected Resource Policy



15. Click **Apply** and save the changes.

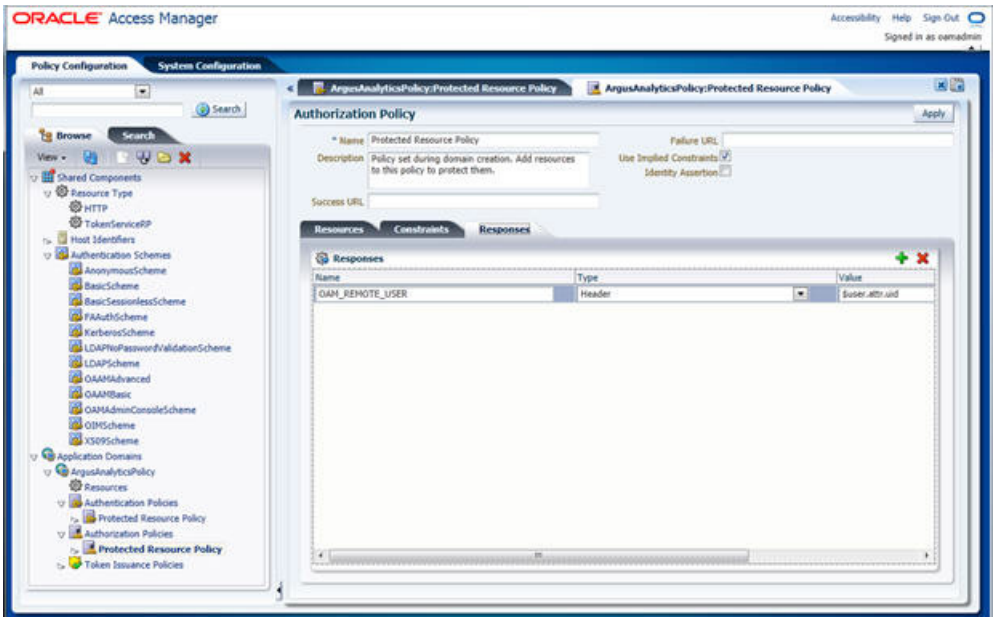
16. Expand and double-click **Application Domains** > **ArgusAnalyticsPolicy** > **Authorization Policies** > **Protected Resource Policy**
17. Ensure that the following resources are present:
    - /
    - /…/*

Figure 2–7 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 2–8 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.oracle.com
   WeblogicPort 7001
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>

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

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

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

<Location /xmlpserver>
   SetHandler weblogic-handler
   WebLogicHost hsdevwv0096.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.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.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.

2.8 Configuring SSL for Oracle Argus Analytics in OBIEE

To enable SSL in WebLogic 12c:

1. Open the following URL:

   https://docs.oracle.com/middleware/1221/biee/BIESC/ssl.htm#BIESC6414
2. Complete all the steps of the *Section 5.2.2 Configuring WebLogic SSL* including all the sub-sections:
    a. *Section 5.2.2.1, "Starting Only the Administration Server"*
    b. *Section 5.2.2.2, "Configuring HTTPS Ports"*
    c. *Section 5.2.2.3, "Configuring Internal WebLogic Server LDAP to Use LDAPs"*
    d. *Section 5.2.2.4, "Configuring Internal WebLogic Server LDAP Trust Store"*
    e. *Section 5.2.2.5, "Disable HTTP"*
    f. *Section 5.2.2.6, "Restart"*
    g. *Section 5.2.2.7, "Configure OWSM to Use t3s"*
    h. *Section 5.2.2.8, "Restart System"*
3. Complete all the steps of the *Section 5.3 Enabling BIEE Internal SSL*.
4. (Optional, not required for Argus Analytics)

   To further configure BI Publisher for SSL communication, follow the steps mentioned in the *Section 4.3.2 Add Virtualize Property to the Identity Store Configuration* from the following URL:

   https://docs.oracle.com/middleware/1221/bip/BIPAD/other_security.htm#CHDJEAFJ
5. Re-enable the Non-SSL ports, and disable the Non-SSL ports.

Note: You must perform this step or you will not be able to login to the OBIEE.

a. Login to WebLogic Admin console.

b. Click **Lock & Edit**.

c. Select environment, servers.

d. For each server:

i. Display the Configuration tab.

ii. To enable the Listen Port, click **Listen Port Enabled** check box.

iii. Click **Save.**

iv. To disable the listen Port, deselect the Listen Port Enabled check box.

v. Click **Save**.

2.9 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 Section 2.8, "Configuring SSL for Oracle Argus Analytics in OBIEE"
- Follow the steps as mentioned in the Part 2.7, "Configuring SSO Using Oracle Access Manager 11g", except for the deviations as mentioned here:

  Update/Create the Webgate Registration in OAM 11g, which you have created in the Section 2.7, "Configuring SSO Using Oracle Access Manager 11g".

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 Section 2.7, "Configuring SSO Using Oracle Access Manager 11g". 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.

2.10 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 2–3 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.

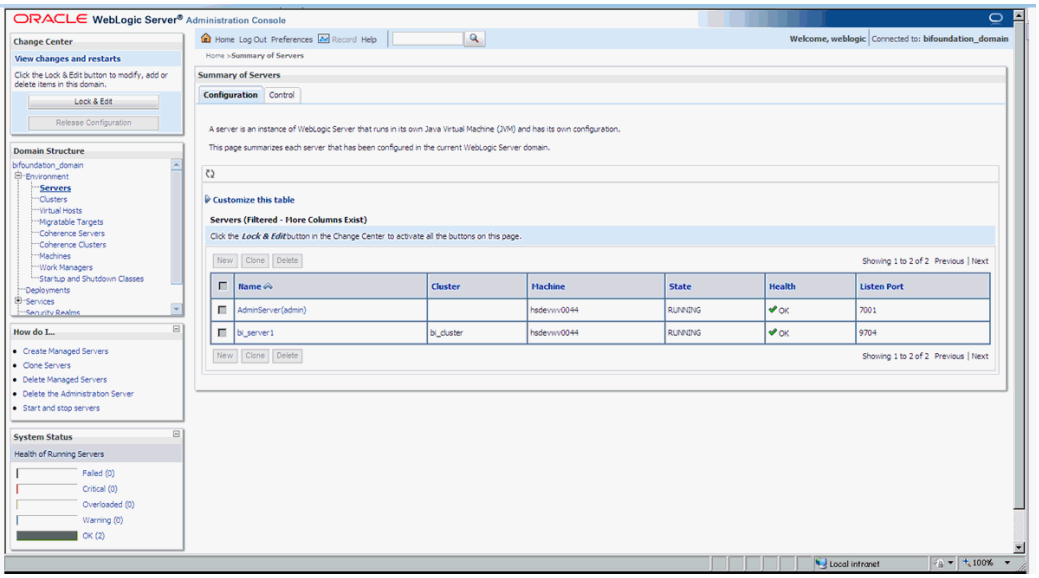
Note: It is recommended to create at least one user to be added with the Administrator Role in DAC to manage the DAC PVA metadata.

2.11 Configuring SSL for Oracle Argus Analytics in OBIEE

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

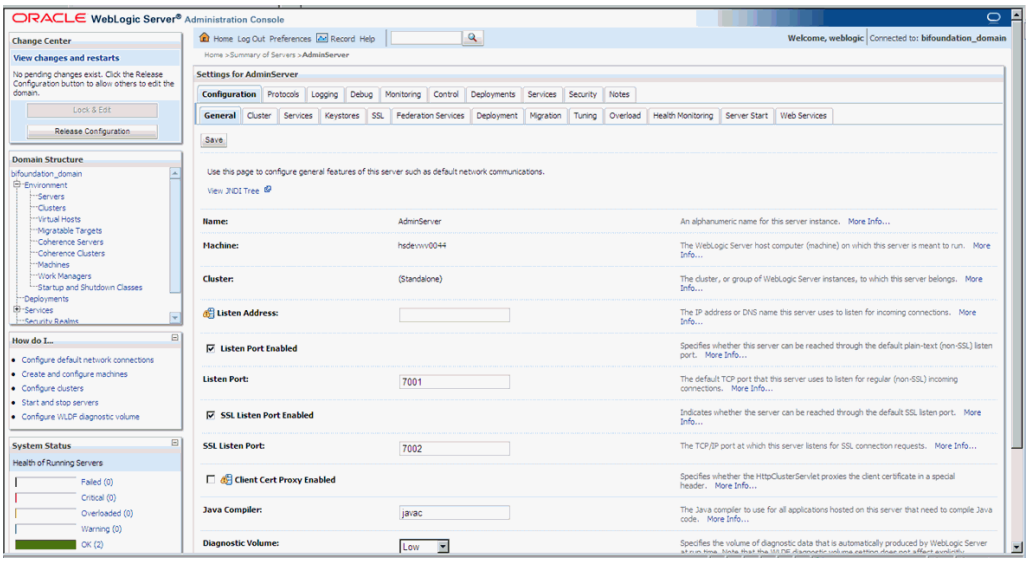
1. Open the WLS Administrator console for OBIEE.
2. Navigate to Environment -> Servers in the tree view displayed on the left side.

Figure 2–9 Servers: Configuration tab



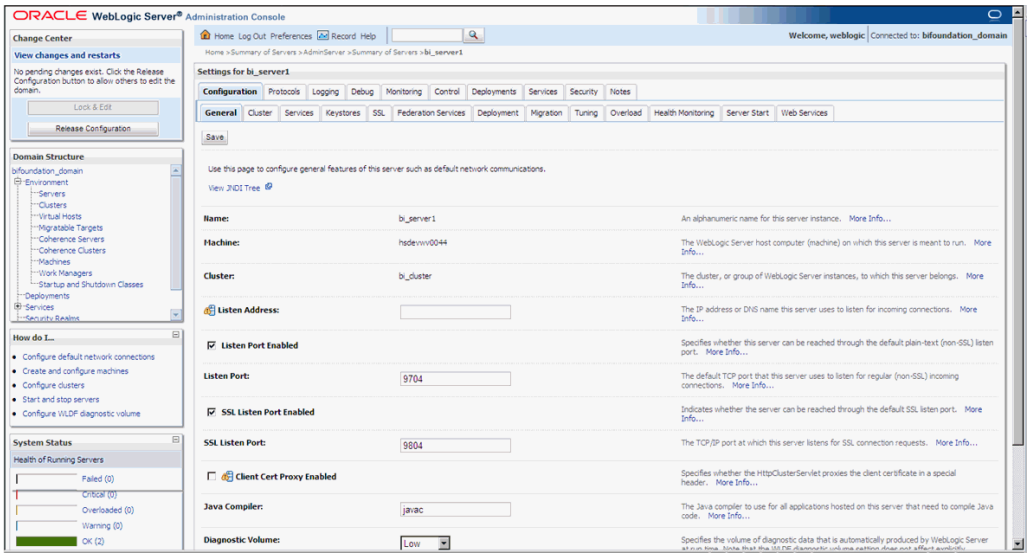
3. Click the Lock & Edit button to change the configuration.
4. Click the AdminServer(admin) link and in the General Tab, enable the SSL listen port, as displayed below:

Figure 2–10 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 2–11 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.

A

Creating ODBC Connection for OBIEE Administration Tool

This appendix comprises the steps to create ODBC connection for OBIEE Administration tool.

1. Navigate to Control Panel > All Control Panel Items > Administrative Tools.
2. Double-click Data Sources (ODBC) (64-bit).

   The ODBC Data Source Administrator (64-bit) dialog box appears.
3. From the System DSN tab, and click **Add**.

   The Create New Data Source dialog box appears.
4. From the list of the available drivers, select **Oracle BI Server**, and click **Finish**.

   The Oracle BI Server DSN Configuration dialog box appears.
5. Enter the following fields:
   a. **Name**—AN_DSN (or any name)
   b. **Description**
   c. **Server**—OBIEE Server Name (FQDN)
6. Click **Next**.
   a. **Login ID**—AN_DSN (or any name)
   b. **Password**
   c. **Port**—The port must be same as mentioned in the Managed Server port list for OBIEE BI Server.

      To retrieve this port, go to Enterprise Manager > BI Instance > Availability tab.
7. Click **Next**.
8. Click **Finish**.