

Oracle® Argus Analytics

Installation Guide

Release 8.1

E76205-01

September 2016

Oracle Argus Analytics Installation Guide, Release 8.1

E76205-01

Copyright © 2016, 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, 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	v
Audience	v
Documentation Accessibility	vi
Finding Information and Patches on My Oracle Support	vi
Related Documents	viii
Known Installation and Configuration Issues	viii
Conventions	viii
Part I Installing Oracle Argus Analytics	
1 Oracle Argus Analytics Requirements	
1.1 Requirements	1-1
1.1.1 Technology Stack and System Requirements	1-1
1.1.1.1 Server Components	1-1
1.1.1.2 Client Components	1-3
1.1.1.3 Supported Sources	1-4
1.1.1.4 Technology Stack Matrix	1-4
1.1.1.5 Typical Hardware Architecture	1-6
1.1.1.6 Installation Process Overview	1-7
1.1.2 Pre-requisites	1-7
1.1.2.1 Client Tools	1-8
2 Installing Oracle Argus Analytics	
2.1 Preinstallation Configuration	2-3
2.1.1 Configuring ETL Clients	2-5
2.1.1.1 Informatica	2-5
2.1.1.2 Installing ODI Studio and Creating Master and Work Repository	2-6
2.2 Running the Oracle Argus Analytics Installer	2-6
2.3 Preparing the DAC Repository (Informatica Only)	2-11
2.4 ODI Smart Import and Topology Configuration (ODI only)	2-15
2.4.1 Connecting to ODI Studio	2-15
2.4.2 ODI Smart Import	2-16
2.4.3 Configuring the Topology in ODI Studio	2-17
2.4.4 Configuring ODI Agent	2-18
2.4.5 Modifying ODI Java EE Agent Connection Pool Settings	2-21

2.5	Configuring the OBIEE Repository and Webcatalog	2-21
2.5.1	Prerequisites	2-22
2.5.1.1	Upgrading the AN RPD and Catalog (Upgrade Install Only).....	2-22
2.5.2	Deployment of OBIEE Repository and Catalog	2-23
2.5.2.1	Configuring the OBIEE Repository and Web Catalog using the BAR File	2-23
2.5.2.2	Configuring OBIEE Repository and Web Catalog Manually	2-27
2.5.2.3	Post-deployment of the Oracle Argus Analytics RPD	2-29
2.5.3	Creating Users and Groups in OBIEE.....	2-30
2.5.4	Creating Roles and Policies with Fusion Middleware Control.....	2-33
2.5.5	OBIEE Catalog Folder-level Permissions	2-37
2.5.6	OBIEE Default Application Roles.....	2-38
2.5.7	Changing the OBIEE RPD Password	2-44
2.6	Configuring the OBIEE Help files	2-44
2.6.1	Configuring the Help links in the Dashboards and Reports.....	2-45
2.7	Configuring SSO Using Oracle Access Manager 10g	2-48
2.8	Configuring SSO Using Oracle Access Manager 11g	2-63
2.9	Configuring SSL for Oracle Argus Analytics in OBIEE	2-75
2.10	Configuring SSL for SSO in Oracle Argus Analytics with OAM 11g	2-76
2.11	Creating Users for DAC	2-78
2.12	Configuring SSL for Oracle Argus Analytics in OBIEE	2-79

Part II Appendix

A Creating ODBC Connection for OBIEE Administration Tool

Preface

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

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

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

Audience

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

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

- Creating and managing user accounts, groups, and access
- Installation and maintenance of Oracle RDBMS
- Installation and maintenance of Informatica PowerCenter
- Installation and maintenance of Oracle Data Integrator
- Installation and maintenance of Oracle Business Intelligence Enterprise Edition 12c
- Installation and maintenance of Oracle Data Warehouse Administration Console 11g
- Installation and maintenance of Oracle Access Manager 11g
- Installation and maintenance of Oracle Weblogic
- Managing OS Environment, services, and network

Documentation Accessibility

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

Access to Oracle Support

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

Finding Information and Patches on My Oracle Support

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

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

Getting the Oracle Argus Analytics Standard Configuration Media Pack

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

To download the Oracle Argus Analytics media pack from eDelivery, do the following:

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

Creating a My Oracle Support Account

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

To register for My Oracle Support:

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

Signing In to My Oracle Support

To sign in to My Oracle Support:

1. Open a Web browser to <http://support.oracle.com>.

2. Click **Sign In**.
3. Enter your user name and password.
4. Click **Go** to open the My Oracle Support home page.

Searching for Knowledge Articles by ID Number or Text String

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

To search by the article ID number:

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

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

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

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

Finding Patches on My Oracle Support

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

To locate and download a patch:

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

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

- In the Patch ID or Number is field, enter the primary bug number of the patch you want. This option is useful if you already know the patch number.
 - To find a patch by product name, release, and platform, click the Product or Family link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.

4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download**. Follow the instructions on the screen to download, save, and install the patch files.

Finding Certification Information

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

1. Sign in to My Oracle Support at <http://support.oracle.com>.
2. Click the **Certifications** tab. The Certifications page opens and displays the Find Certifications region.
3. In Select Product, enter Oracle Argus Analytics.
4. Click the Go to Certifications icon.
The right pane displays the certification information.
5. Select a certification to view the certification details.

Related Documents

For more information, see the following documents:

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

- *Data Warehouse Administration Console User's Guide*
- *Oracle Business Intelligence Data Warehouse Administration Console Installation, Configuration, and Upgrade Guide*

For *Oracle Fusion Middleware* documentation set, refer to <http://docs.oracle.com/middleware/1221/biee/docs.htm>.

Known Installation and Configuration Issues

Oracle maintains a list of installation and configuration issues that you can download from My Oracle Support (MOS).

Conventions

The following text conventions are used in this document:

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

Part I

Installing Oracle Argus Analytics

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

Part I contains the following chapters:

- [Chapter 1, Oracle Argus Analytics Requirements](#)
- [Chapter 2, Installing Oracle Argus Analytics](#)

Oracle Argus Analytics Requirements

1.1 Requirements

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

1.1.1 Technology Stack and System Requirements

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

1.1.1.1 Server Components

1.1.1.1.1 Oracle Argus Analytics Database Server

Oracle Argus Analytics is certified for Oracle Database Enterprise Edition and Standard Edition 12.1.0.2.

Supported Operating System

- Oracle Enterprise Linux 6.7, or Linux 7.1
- Oracle Solaris 10 (64 Bit)
- Oracle Solaris 11
- 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

1.1.1.1.2 Oracle Argus Analytics ETL Server

This section comprises the following sub-sections:

1.1.1.1.3 Oracle Argus Analytics Informatica Server

Oracle Argus Analytics is certified against Informatica PowerCenter 9.0.1 with Hotfix2 and PowerCenter 9.6.1. Refer to the Informatica PowerCenter Installation Guide for recommended hardware and supported platforms.

Oracle Argus Analytics has got certified with the following:

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

1.1.1.1.4 Oracle Data Integrator (ODI) Server

Oracle Argus Analytics is certified against Oracle Data Integrator 12.1.3 or 12.2.1. Refer to the ODI Installation Guide for recommended hardware and supported platforms.

Oracle Argus Analytics has got certified with the following:

- Operating System: Microsoft Windows Server 2012 Standard (64 bit), Windows Server 2012 R2 Standard (64 bit), and Linux 6.6/6.7/7.1 (64 bit)
- Memory: At least 8 GB RAM. HDD – at least 250 GB free space
- CPU: At least 4 Dual Core CPUs

1.1.1.1.5 Oracle Argus Analytics OBIEE Server Oracle Argus Analytics is certified against Oracle Business Intelligence Enterprise Edition 12.2.1 with latest patch set (The following patch has been verified with AN 8.1: 12.2.1.160419 at the time of the release).

Refer to the installation manual of OBIEE for further hardware and software requirements Oracle Argus Analytics would recommend the following:

Operating System

- Microsoft Windows Server 2012 R2 Standard (64 bit)
- Oracle Enterprise Linux 6.6/6.7/7.1 (64 bit)
- 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.

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

1.1.1.1.6 Oracle Argus Analytics Data Warehouse Administration Console Server

Oracle Argus Analytics requires Oracle Data Warehouse Administration Console Server 11.1.1.6.4.

Supported Operating System

- Oracle Enterprise Linux 5 or above (32/64 bit)
- Oracle Solaris 10 and 11 (64 bit)
- Microsoft Windows Server 2008 or above (32/64 bit)
- Microsoft Windows Server 2012 or above (64 bit)

- Memory: RAM 4-16 GB (based on organization size), HDD – at least 500 GB free space
- CPU: At least 2 Dual Core CPUs

1.1.1.2 Client Components

1.1.1.2.1 Oracle Database Client

- Oracle Argus Analytics requires Oracle database client to connect to the database server. The supported client software version is 12.1.0.2.
- Supported Operating System:
 - Microsoft Windows Server 2012 Standard (64 bit)
 - Microsoft Windows Server 2012 R2 Standard (64 bit)

1.1.1.2.2 Oracle Data Warehouse Administration Console Client

- Oracle Data Warehouse Administration Console Client is required only when Informatica PowerCenter is used as an ETL Tool
- Oracle Argus Analytics requires Oracle Data Warehouse Administration Console Client 11.1.1.6.4
- Supported Operating System: Microsoft Windows Server 2012 or above (64 bit)

1.1.1.2.3 ETL Client

This section comprises the following sub-sections:

1.1.1.2.4 Informatica PowerCenter Client

- An Informatica PowerCenter Client 9.0.1 with Hotfix 2 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)

1.1.1.2.5 ODI Studio

- An ODI Studio 12.1.3 or 12.2.1 is required to connect to the ODI Repository.
- Supported Operating System:
 - Microsoft Windows Server 2012 Standard (64 bit)
 - Microsoft Windows Server 2012 R2 Standard (64 bit)
 - Linux 6.6/6.7/7.1

You can also refer to this link for supported platforms:

ODI 12.2.1:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/documentation/fmw-1221certmatrix-2739738.xlsx>

ODI 12.1.3:

<http://www.oracle.com/technetwork/middleware/fusion-middleware/documentation/fmw-1213certmatrix-2226694.xls>

1.1.1.2.6 Oracle Business Intelligence Developer Client Tool

- Oracle Business Intelligence Developer Client Tool 12.2.1 must be installed for configuring the repository file (RPD).
- Supported Operating System:
 - Microsoft Windows Server 2012 Standard (64 bit)
 - Microsoft Windows Server 2012 R2 Standard (64 bit)

1.1.1.2.7 Optional Security Component

You can also configure Single Sign On Support for your reports and dashboards using Oracle Access Manager 11g. For more information regarding the Oracle Access Manager installation and supported platforms, please refer the *Oracle Access Manager Installation Guide*.

1.1.1.2.8 Miscellaneous Components

- For running the reports and dashboards, your machine should have the Adobe Flash Player 10 or above installed.
- Although OBIEE 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.

1.1.1.3 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

The following table displays the technology stack matrix diagram of all the components of Oracle Argus Analytics.

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
Operating System	Windows Server 2012 Standard (64 Bit)	Windows Server 2012 R2 Standard (64 Bit)	Windows Server 2008 or above (32/64 Bit)	Windows Server 2012 Standard (64 Bit)	Windows Server 2012 Standard (64 Bit)
	Windows Server 2012 R2 Standard (64 Bit)	Oracle Enterprise Linux 6.6	Windows Server 2012 or above (64 Bit)	Windows Server 2012 R2 Standard (64 Bit)	Windows Server 2012 R2 Standard (64 Bit)
	Oracle Enterprise Linux 6.6	Oracle Enterprise Linux 6.7	Oracle Enterprise Linux X86 Version 5 or above (32/64 Bit)	Oracle Enterprise Linux 6.6	
	Oracle Enterprise Linux 6.7	Oracle Enterprise Linux 7.1	Oracle Solaris 10 (64 Bit)	Oracle Enterprise Linux 6.7	
	Oracle Enterprise Linux 7.1			Oracle Enterprise Linux 7.1	
Oracle Database	12.1.0.2 Client	12.1.0.2 (Enterprise) - AL32UTF8 character set (Supports both CDB-PDB/Non CDB)			

Specification	OBIEE Server	Database	Informatica Server	Oracle Data Integrator (ODI)	Client
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 11g				
Resolution					Minimal Resolution 1280x1024

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

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`.

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

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

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

1.1.1.5 Typical Hardware Architecture

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

- Servers:
 - An Oracle Database Server with Oracle Database 12.1.0.2
 - An OBIEE 12.2.1 Server with latest patch set
 - ETL Server
 - * Informatica: 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: The above three boxes can run on any of the supported platforms: Linux/Solaris/Windows.

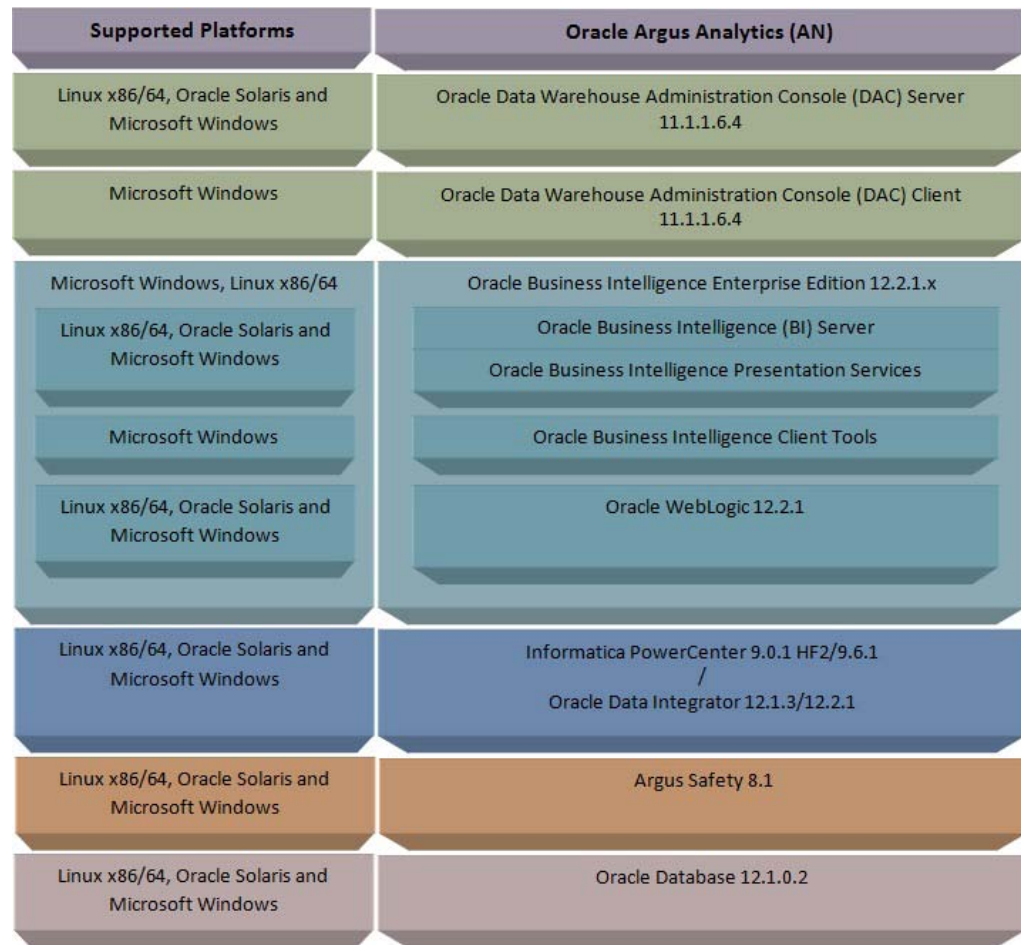
- Clients:
 - ETL Clients
 - * Informatica PowerCenter Client 9.0.1 + Hotfix 2 or Informatica PowerCenter Client 9.6.1
 - OR
 - * ODI Studio 12.1.3 or 12.2.1
 - Oracle Database Client 12.1.0.2
 - DAC Client 11.1.1.6.4
 - Oracle Business Intelligence Developer Client Tool (12.2.1.0.0)

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

1.1.1.6 Installation Process Overview

The following steps describes the overview of the installation process:

- Follow the steps described in [Section 1.1.2, "Pre-requisites"](#).
- Execute the installer – to create the data mart and Informatica ETLs.
- Follow the post-installation steps to configure DAC/ODI and OBIEE

For more information about certifications, refer to "[Finding Certification Information](#)".

1.1.2 Pre-requisites

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

- Oracle Database Server – An Oracle 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.

1.1.2.1 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.
-
-

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
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.
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.

Current Argus Analytics Version	Upgrade to Argus Analytics Version:				
	1.1	1.1.1	7.0.3	8.0	8.1
1.1.1	Not applicable	Not applicable	<p>Follow the steps given below:</p> <ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a) Extract the Argus Analytics 7.0.3 installer to any temporary folder. Example: C:\temp\AN80 b) Navigate to the folder <InstallerExtractionFolder>\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 Installing Oracle Argus Analytics opva_help_<Argus Analytics 	Use Argus Analytics 8.0 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
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.
8.0	Not applicable	Not applicable	Not applicable	Not applicable	Use Argus Analytics 8.1 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. This section includes the following topics:

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

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

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

1. The TNS entries for both the Data Mart Schema and the Argus Safety Database Schema should be present in the OBIEE 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 the SYSTEM or INSTALL(DBA) user:

- To setup a SYSTEM database user:

During the installation, either use in-built SYSTEM database user, or a custom INSTALL(DBA) database user.

a) Provide access rights to create a view over the V_\$SESSION view.

b) Execute privilege with the Grant option on DBMS_RLS in case of a multi-tenant system to run the installer.

c) Connect as SYS on both Argus Safety database instance, and Argus Analytics Data Mart database instance.

d) Execute the following script:

```
GRANT SELECT ON V_$SESSION TO SYSTEM WITH GRANT OPTION;
GRANT EXECUTE ON DBMS_RLS TO SYSTEM WITH GRANT OPTION;
```

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

- To setup an INSTALL(DBA) user:

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

b) Enter the following inputs:

- Log file name
- Argus Safety/Argus Analytics database connection string
- Password for the SYS user
- DBA or INSTALL user name to be created
- Password for the DBA or INSTALL user

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

Note:

- If the INSTALL(DBA) user already exists in the database, then the script provides the required additional grants to the user. If the user does not exist 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 '<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 '<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

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

1. The TNS entries for both the Data Mart Schema and the Argus Safety database Schema should be present in the Informatica Server as well so that the ETLs can

pick data from the Argus Safety Database and populate the same in the PVA Warehouse.

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

One can create the entry in the domains.infa file by configuring the Informatica Domain used for Argus Analytics in the Informatica Powercenter Repository Manager by navigating through the Repository > Configure Domains menu.

3. Setting up the Informatica environmental parameters:

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

4. Setting up the DAC Client:

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

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

2.1.1.2 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

Please choose appropriately in the installation process if Argus Analytics is a fresh installation or an upgrade installation which is supported from Argus Analytics 8.0 to 8.1.

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 8.0

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: Provide either the SYSTEM or the custom INSTALL(DBA) user name
- Argus Safety DBA Password: Password for SYSTEM or 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: <SYSYEM or INSTALL user name>
- AS DBA User Name: <SYSYEM or 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: Provide either the SYSTEM or the customer INSTALL(DBA) User Name
- DWH Data Mart DBA User Password: Password for SYSTEM/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: <SYSTEM or INSTALL user name>
- DW DBA User Password: <SYSTEM or 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\pvadrivercript<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
\$\$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 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**.

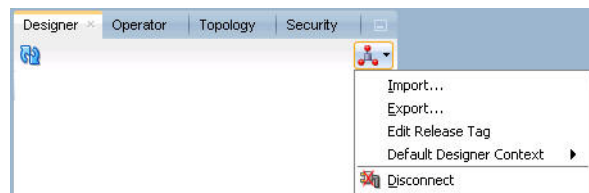
Refer to the *Oracle Data Integrator Install and Configuration Guide*:

- 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>

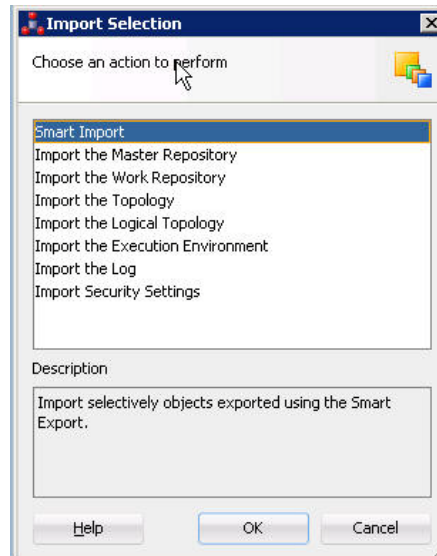
2.4.2 ODI Smart Import

Follow the steps listed below to execute ODI Smart Import:

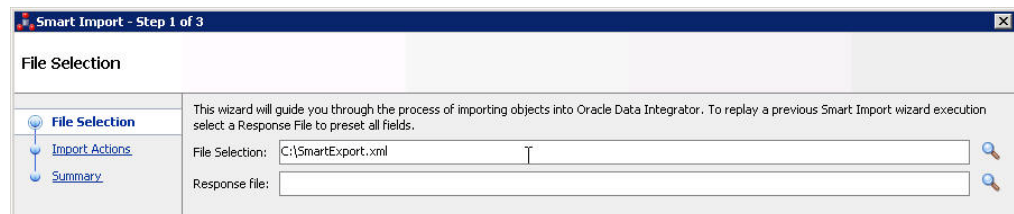
1. Log in to the work repository in ODI Studio by selecting the **AN Work Repository** connection.
2. Select the **Connect Navigator** drop-down list from the top right on the **Designer** tab and click **Import**.



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."](#)

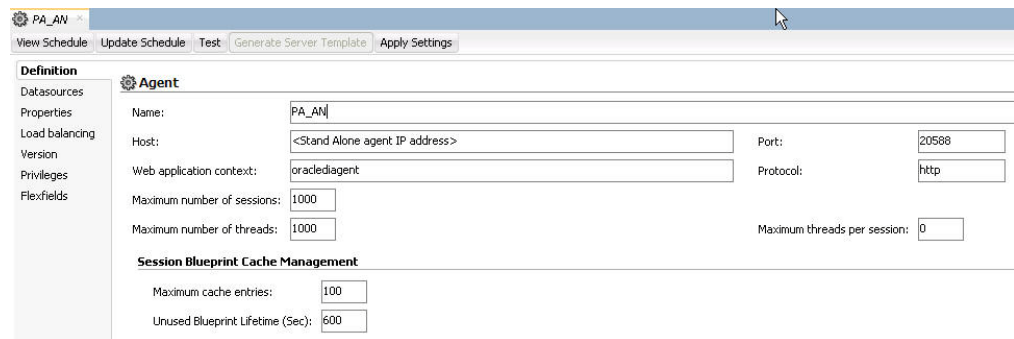
Note: Make sure to create the agent with name **PA_AN**, as the same is available in Argus Analytics ODI code.

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
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

Table 2–2 (Cont.) ODI Parameters

Parameters	Load Type	Description	Allowed Values
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'
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 upgrade from Argus Analytics 8.0 is not available. Use the latest catalog provided with the AN 8.1 installation (present at <AN_INSTALL_HOME>/catalog/opva.zip) for deployment.

2.5.1.1.1 Upgrading the RPD

The following steps will let you upgrade the AN 8.0 RPD to the latest code in AN 8.1.

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.

Steps to upgrade the AN RPD (if required):

1. Open the existing AN RPD file that you wish to upgrade to AN 8.1 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 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 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 is not available. Please use the latest catalog provided with the AN 8.1 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](#)

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

The following roles are imported as default application roles:

- PVAdminRole
- 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 bundler (.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 Mart Home>\report\opva.rpd and report\opva.rpd 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\biinstance\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."](#)

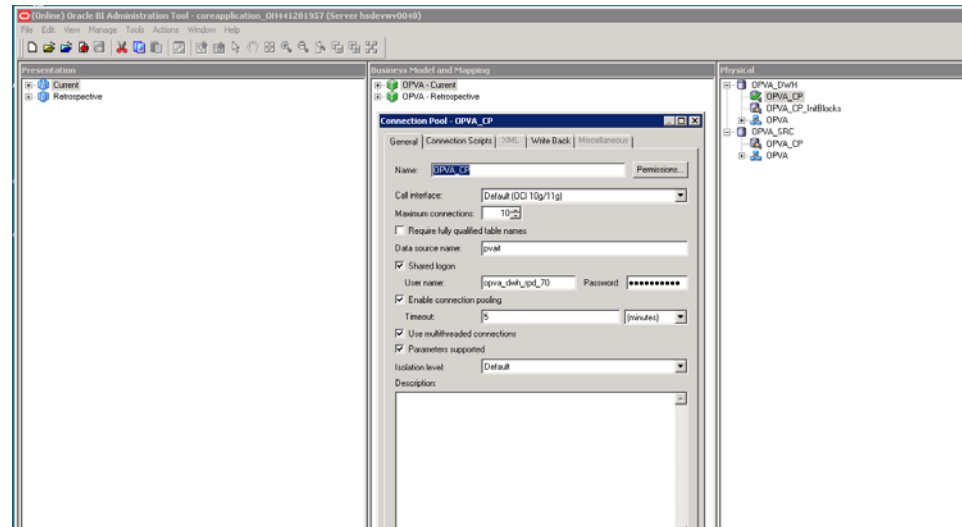
19. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See [Section 2.5.5, "OBIEE Catalog Folder-level Permissions"](#))

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 or BISystemUser
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 installation].
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

Create a New Group

OK Cancel

Group Properties

The following properties will be used to identify your new Group.

* Indicates required fields

What would you like to name your new Group?

* **Name:** PVAAdmin

How would you like to describe the new Group?

Description: PVA Administrators Group

Please choose a provider for the group.

Provider: DefaultAuthenticator

OK Cancel

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.

Create a New User

OK Cancel

User Properties

The following properties will be used to identify your new User.

* Indicates required fields

What would you like to name your new User?

* **Name:** Username

How would you like to describe the new User?

Description: User Description

Please choose a provider for the user.

Provider: DefaultAuthenticator

The password is associated with the login name for the new User.

* **Password:**

* **Confirm Password:**

OK Cancel

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**.

General Passwords Attributes **Groups**

Save

Use this page to configure group membership for this user.

Parent Groups:

Available:

- CrossDomainConnectors
- Deployers
- Monitors
- Operators
- OracleSystemGroup
- PVASafetyConsumersGr
- PVASafetyGroup

Chosen:

- PVAAdmin

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.

The screenshot shows the 'Application Roles' page in Fusion Middleware Control. The page title is 'Application Roles' and it is under the 'WebLogic Domain' context. Below the title, there is a search section with an 'Application Stripe' dropdown set to 'obi' and a 'Role Name' field set to 'Starts With'. Below the search section, there is a table with columns 'Role Name', 'Display Name', and 'Description'. The table contains one row: 'BIServiceAdministrator', 'BI Service Administrator', and 'This role confers privileges required to administer a service instance.'.

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

The screenshot shows the 'Create Application Role' dialog box. The 'General' section has the following fields: 'Application Stripe' (obi), 'Role Name' (PVAAdminRole), 'Display Name' (PVA Administrator Role), and 'Description' (PVA Administrator Role). The 'Members' section is empty, with a message: 'No groups or application roles added.'

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**.

Add Principal

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

Search

Type: Application Role

Principal Name: Starts With PVAAdmin

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
PVAAdminRole	PVA Administrator Role	PVA Administrator Role

OK Cancel

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

The Add Principal dialog box appears.

10. From the **Type** drop-down list, select **Application Role**, and click **Search**.

A list of principals appears.

11. From the list of Searched Principals, select **BIServiceAdministrator**, and click **OK**.

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

Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
PVAAdminRole	PVA Administrator Role	PVA Administrator Role
PVASafetyRole	PVA Safety Author Role	PVA Safety Author Role
PVASafetyConsumersRole	PVA Safety Consumers Role	PVA Safety Consumers Role

Membership for PVAAdminRole

Principal	Display Name	Type	Description
PVAAdmin	PVAAdmin	Group	PVAAdmin
BIServiceAdministrator	PVA Administrator Role	Application Role	PVA Administrator Role

12. To add **PVASafetyRole**, repeat from Step 4 to Step 11.

Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
PVAAdminRole	PVA Administrator Role	PVA Administrator Role
PVASafetyRole	PVA Safety Author Role	PVA Safety Author Role
PVASafetyConsumersRole	PVA Safety Consumers Role	PVA Safety Consumers Role

Principal	Display Name	Type	Description
PVAAdminRole	PVA Safety Author Role	Application Role	PVA Safety Author Role
PVASafetyGroup	PVASafetyGroup	Group	PVASafetyGroup

13. To add **PVASafetyConsumerRole**, repeat from Step 4 to Step 11, and add **authenticated-role** as a Member for this role.

Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
PVAAdminRole	PVA Administrator Role	PVA Administrator Role
PVASafetyRole	PVA Safety Author Role	PVA Safety Author Role
PVASafetyConsumersRole	PVA Safety Consumers Role	PVA Safety Consumers Role

Principal	Display Name	Type	Description
authenticated-role	Authenticated Role	Authenticated Role	
PVASafetyConsumersGroup	PVASafetyConsumersGroup	Group	PVASafetyConsumersGroup
PVASafetyRole	PVA Safety Consumers Role	Application Role	PVA Safety Consumers Role

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.

Select from permissions and resources used in this application. Enter search criteria to search for right permissions.

Search

Permissions Resource Types

Resource Type: oracle.bi.publisher.permission

Resource Name: Starts With

Search Results

Resource Name	Display Name	Description
oracle.bi.publish...	BIP Access Excel Report Analyzer	
oracle.bi.publish...	BIP Access Online Report Analyzer	
oracle.bi.publish...	BIP Access Report Output	
oracle.bi.publish...	BIP Administer Server	
oracle.bi.publish...	BIP Develop Data Model	
oracle.bi.publish...	BIP Develop Report	
oracle.bi.publish...	BIP Run Report Online	
oracle.bi.publish...	BIP Schedule Report	

TIP Continue to go to next step if you want to enter policy details.

Continue Cancel

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
PVAAdmin	oracle.bi.catalog	*	manage
	oracle.bi.server.permission	oracle.bi.server.permission	_all_
	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanager.permission	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
	oracle.bi.repository	oracle.bi.repository	manage
	oracle.bi.scheduler.permission	oracle.bi.scheduler.permission	_all_
PVASafetyRole	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	*
	oracle.bi.delivers.job	oracle.bi.delivers.job	schedule
PVASafetyConsumersRole	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	READ,EXECUTE
	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_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, and click **OK**.

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

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	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 (Owner)	Full Control

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.

Component	Privilege	Default Role Granted
Access	Access to Administration	PVA Administrator Role, BI Service Administrator
Access	Access to Answers	PVA Safety Author Role
Access	Access to BI Composer	PVA Safety Author Role
Access	Access to Briefing Books	PVA Safety Consumers Role
Access	Access to Dashboards	PVA Safety Consumers Role
Access	Access to Delivers	PVA Safety Author Role
Access	Access to Export	PVA Safety Consumers Role
Access	Access to KPI Builder	PVA Safety Author Role
Access	Access to List Formats	PVA Safety Author Role

Component	Privilege	Default Role Granted
Access	Access to Metadata Dictionary	PVA Safety Author Role
Access	Access to Mobile	PVA Safety Consumers Role
Access	Access to Oracle BI Client Installer	PVA Safety Consumers Role
Access	Access to Oracle BI for Microsoft Office	PVA Safety Consumers Role
Access	Access to Scorecard	PVA Safety Consumers Role
Access	Access to Segment Trees	PVA Safety Author Role
Access	Access to Segments	PVA Safety Consumers Role
Access	Catalog Preview Pane UI	PVA Safety Consumers Role
Actions	Create Invoke Actions	PVA Safety Author Role
Actions	Create Navigate Actions	PVA Safety Consumers Role
Actions	Save Actions containing embedded HTML	PVA Administrator Role, BI Service Administrator
Admin: Catalog	Change Permissions	PVA Safety Author Role
Admin: Catalog	Toggle Maintenance Mode	PVA Administrator Role, BI Service Administrator
Admin: General	Change Log Configuration	PVA Administrator Role, BI Service Administrator
Admin: General	Create Dashboards	PVA Safety Author Role
Admin: General	Diagnose BI Server Query	Denied: Authenticated User
Admin: General	Issue SQL Directly	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Agent Sessions	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Device Types	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Global Variables	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Map Data	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Marketing Defaults	PVA Administrator Role, BI Service Administrator
Admin: General	Manage Marketing Jobs	PVA Safety Author Role
Admin: General	Manage Sessions	PVA Administrator Role, BI Service Administrator
Admin: General	Performance Monitor	PVA Administrator Role, BI Service Administrator
Admin: General	See privileged errors	PVA Administrator Role, BI Service Administrator
Admin: General	See sessions IDs	PVA Administrator Role, BI Service Administrator
Admin: General	See SQL issued in errors	PVA Safety Consumers Role
Admin: General	View System Information	PVA Administrator Role, BI Service Administrator

Component	Privilege	Default Role Granted
Admin: Security	Access to Permissions Dialog	PVA Safety Consumers Role
Admin: Security	Manage Catalog Accounts	PVA Administrator Role, BI Service Administrator
Admin: Security	Manage Privileges	PVA Administrator Role, BI Service Administrator
Admin: Security	Set Ownership of Catalog Objects	PVA Administrator Role, BI Service Administrator
Admin: Security	User Population - Can List Application Roles	PVA Safety Consumers Role, BI System
Admin: Security	User Population - Can List Catalog Groups	PVA Safety Consumers Role, BI System
Admin: Security	User Population - Can List Users	PVA Safety Consumers Role, BI System
Answers	Access Advanced Tab	PVA Safety Author Role
Answers	Add EVALUATE_PREDICATE Function	PVA Safety Author Role
Answers	Create Advanced Filters and Set Operations	PVA Safety Author Role
Answers	Create Analysis From Simple SQL	PVA Administrator Role, BI Service Administrator
Answers	Create Prompts	PVA Safety Author Role
Answers	Create Views	PVA Safety Author Role
Answers	Edit Column Formulas	PVA Safety Author Role
Answers	Edit Direct Database Analysis	PVA Administrator Role, BI Service Administrator
Answers	Enter XML and Logical SQL	PVA Safety Author Role
Answers	Execute Direct Database Analysis	PVA Administrator Role, BI Service Administrator
Answers	Save Column	PVA Safety Author Role
Answers	Save Content with HTML Markup	PVA Administrator Role, BI Service Administrator
Answers	Save Filters	PVA Safety Author Role
Answers	Upload Images	PVA Safety Author Role
Briefing Book	Add To or Edit a Briefing Book	PVA Safety Author Role
Briefing Book	Add to Snapshot Briefing Book	PVA Safety Consumers Role
Briefing Book	Download Briefing Book	PVA Safety Consumers Role
Catalog	Archive Catalog	PVA Administrator Role, BI Service Administrator
Catalog	Create Folders	PVA Safety Author Role
Catalog	Perform Extended Search	PVA Safety Author Role
Catalog	Perform Global Search	PVA Safety Author Role
Catalog	Personal Storage (My Folders and My Dashboard)	PVA Safety Consumers Role
Catalog	Reload Metadata	PVA Administrator Role, BI Service Administrator
Catalog	See Hidden Items	PVA Safety Author Role

Component	Privilege	Default Role Granted
Catalog	Unarchive Catalog	PVA Administrator Role, BI Service Administrator
Catalog	Upload Files	PVA Administrator Role, BI Service Administrator
Conditions	Create Conditions	PVA Safety Author Role
Dashboards	Assign Default Customizations	PVA Safety Author Role
Dashboards	Create Bookmark Links	PVA Safety Consumers Role
Dashboards	Create Prompted Links	PVA Safety Consumers Role
Dashboards	Export Entire Dashboard To Excel	PVA Safety Consumers Role
Dashboards	Export Single Dashboard Page To Excel	PVA Safety Consumers Role
Dashboards	Save Customizations	PVA Safety Consumers Role
Delivers	Chain Agents	PVA Safety Author Role
Delivers	Create Agents	PVA Safety Author Role
Delivers	Deliver Agents to Specific or Dynamically Determined Users	PVA Administrator Role, BI Service Administrator
Delivers	Modify Current Subscriptions for Agents	PVA Administrator Role, BI Service Administrator
Delivers	Publish Agents for Subscription	PVA Safety Author Role
Formatting	Save System-Wide Column Formats	PVA Administrator Role, BI Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access Catalog Search UI	PVA Safety Consumers Role
Home and Header	Access Catalog UI	PVA Safety Consumers Role
Home and Header	Access Data Loader	Denied: Authenticated User
Home and Header	Access Home Page	PVA Safety Consumers Role
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Rapid Search UI	PVA Safety Consumers Role
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Advanced Search Link	PVA Safety Consumers Role
Home and Header	Custom Links	PVA Safety Consumers Role
Home and Header	Dashboards Menu	PVA Safety Consumers Role
Home and Header	Favorites Menu	PVA Safety Consumers Role
Home and Header	Help Menu	PVA Safety Consumers Role
Home and Header	My Account Link	PVA Safety Consumers Role
Home and Header	New Menu	PVA Safety Consumers Role
Home and Header	Open Menu	PVA Safety Consumers Role
Home and Header	Simple Search Field	PVA Safety Consumers Role
List Formats	Access Options Tab	PVA Safety Author Role
List Formats	Add/Remove List Format Columns	PVA Administrator Role, BI Service Administrator

Component	Privilege	Default Role Granted
List Formats	Create Headers and Footers	PVA Safety Author Role
List Formats	Create List Formats	PVA Safety Author Role
Mobile	Enable Local Content	PVA Safety Consumers Role
Mobile	Enable Search	PVA Safety Consumers Role
My Account	Access to My Account	PVA Safety Consumers Role
My Account	Change Delivery Options	PVA Safety Consumers Role
My Account	Change Preferences	PVA Safety Consumers Role
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	PVA Safety Consumers Role
Scorecard	Add Annotations	PVA Safety Consumers Role
Scorecard	Add Scorecard Views To Dashboards	PVA Safety Consumers Role
Scorecard	Create Views	PVA Safety Author Role
Scorecard	Create/Edit Causes And Effects Linkages	PVA Safety Author Role
Scorecard	Create/Edit Initiatives	PVA Safety Author Role
Scorecard	Create/Edit KPIs	PVA Safety Author Role
Scorecard	Create/Edit Objectives	PVA Safety Author Role
Scorecard	Create/Edit Perspectives	PVA Safety Author Role
Scorecard	Create/Edit Scorecards	PVA Safety Author Role
Scorecard	Override Status	PVA Safety Consumers Role
Scorecard	View Scorecards	PVA Safety Consumers Role
Scorecard	Write Back to Database for KPI	PVA Safety Consumers Role
Segmentation	Access Segment Advanced Options Tab	PVA Administrator Role, BI Service Administrator
Segmentation	Access Segment Tree Advanced Options Tab	PVA Administrator Role, BI Service Administrator
Segmentation	Change Target Levels within Segment Designer	PVA Safety Author Role
Segmentation	Create Segment Trees	PVA Safety Author Role
Segmentation	Create Segments	PVA Safety Author Role
Segmentation	Create/Purge Saved Result Sets	PVA Administrator Role, BI Service Administrator
SOAP	Access AdministrationSOAPSERVICE Service	PVA Safety Consumers Role, BI System
SOAP	Access AnalysisExportViewsService Service	PVA Safety Consumers Role
SOAP	Access CatalogIndexingService Service	PVA Safety Consumers Role, BI System
SOAP	Access CatalogService Service	PVA Safety Consumers Role, BI System
SOAP	Access ConditionEvaluationService Service	PVA Safety Consumers Role, BI System
SOAP	Access DashboardService Service	PVA Safety Consumers Role, BI System
SOAP	Access HtmlViewService Service	PVA Safety Consumers Role, BI System

Component	Privilege	Default Role Granted
SOAP	Access IBoTService Service	PVA Safety Consumers Role, BI System
SOAP	Access JobManagementService Service	PVA Safety Consumers Role, BI System
SOAP	Access KPIAssessmentService Service	PVA Safety Consumers Role, BI System
SOAP	Access MetadataService Service	PVA Safety Consumers Role, BI System
SOAP	Access MsgdbService Service	PVA Safety Consumers Role, BI System
SOAP	Access ReportEditingService Service	PVA Safety Consumers Role, BI System
SOAP	Access SchedulerService Service	PVA Safety Consumers Role
SOAP	Access ScorecardAssessmentService Service	PVA Safety Consumers Role, BI System
SOAP	Access ScorecardMetadataService Service	PVA Safety Consumers Role, BI System
SOAP	Access SecurityService Service	PVA Safety Consumers Role, BI System
SOAP	Access SOAP	PVA Safety Consumers Role, BI System
SOAP	Access Tenant Information	BI System
SOAP	Access UserPersonalizationService Service	PVA Safety Consumers Role
SOAP	Access XmlGenerationService Service	PVA Safety Consumers Role, BI System
SOAP	Impersonate as system user	BI System
Subject Area: "Current"	Access within Oracle BI Answers	PVA Administrator Role, PVA Safety Author Role, PVA Safety Consumers Role, BI Service Administrator
Subject Area: "Retrospective"	Access within Oracle BI Answers	PVA Administrator Role, PVA Safety Author Role, PVA Safety Consumers Role, BI Service Administrator
View Canvas	Add/Edit Canvas View	PVA Safety Author Role
View Column Selector	Add/Edit Column Selector View	PVA Safety Author Role
View Compound Layout	Add/Edit Compound Layout View	PVA Safety Author Role
View Contribution Wheel	Add/Edit Contribution Wheel View	PVA Safety Author Role
View Create Segment	Add/Edit Create Segment View	PVA Safety Author Role
View Create Target List	Add/Edit Create Target List View	PVA Safety Author Role
View Dashboard Prompt	Add/Edit Dashboard Prompt View	PVA Safety Author Role
View Filters	Add/Edit Filters View	PVA Safety Author Role
View Funnel	Add/Edit Funnel View	PVA Safety Author Role
View Gauge	Add/Edit Gauge View	PVA Safety Author Role
View Generic Plugin View	Add/Edit Generic Plugin View View	PVA Safety Author Role
View Graph	Add/Edit Graph View	PVA Safety Author Role
View Heat Matrix	Add/Edit Heat Matrix View	PVA Safety Author Role
View Javascript view	Edit Javascript View	PVA Safety Author Role

Component	Privilege	Default Role Granted
View Legend	Add/Edit Legend View	PVA Safety Author Role
View Logical SQL	Add/Edit Logical SQL View	PVA Safety Author Role
View Map	Add/Edit Map View	PVA Safety Author Role
View Micro Chart	Add/Edit Micro Chart View	PVA Safety Author Role
View Narrative	Add/Edit Narrative View	PVA Safety Author Role
View No Results	Add/Edit No Results View	PVA Safety Author Role
View Performance Tile	Add/Edit Performance Tile View	PVA Safety Author Role
View Pivot Table	Add/Edit Pivot Table View	PVA Safety Author Role
View Report Prompt	Add/Edit Report Prompt View	PVA Safety Author Role
View Selection Steps	Add/Edit Selection Steps View	PVA Safety Author Role
View Static Text	Add/Edit Static Text View	PVA Safety Author Role
View Table	Add/Edit Table View	PVA Safety Author Role
View Ticker	Add/Edit Ticker View	PVA Safety Author Role
View Title	Add/Edit Title View	PVA Safety Author Role
View Treemap	Add/Edit Treemap View	PVA Safety Author Role
View Trellis	Add/Edit Trellis View	PVA Safety Author Role
View View Selector	Add/Edit View Selector View	PVA Safety Author Role
Write Back	Manage Write Back	PVA Administrator 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.

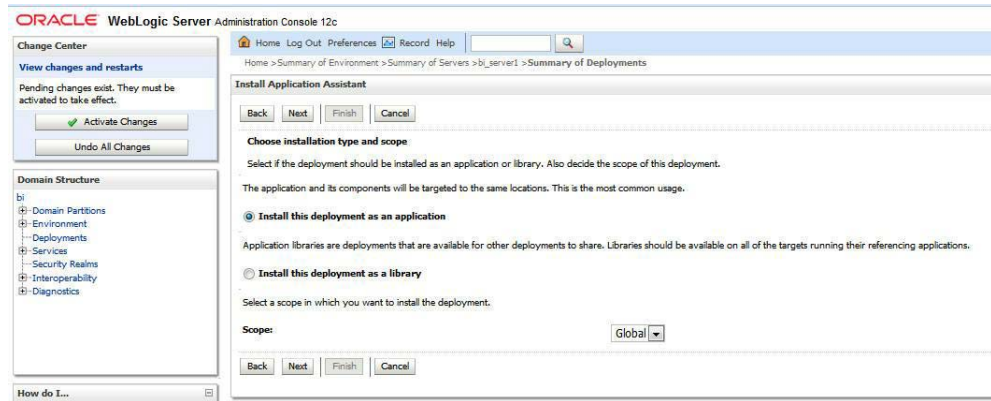
The screenshot shows the Oracle WebLogic Server Administration Console. The left pane shows the Domain Structure with 'Deployments' selected. The main area displays a table of installed applications and modules. The 'Install' button is visible for the selected application.

Name	State	Health	Type	Targets	Scope	Domain Partitions	Deployment Order
oracle.wls.welcome(1.0.12.1.0.0)	Active		Library	AdminServer, ls_cluster	Global		100
oracle.wls.domain(1.0.12.1.0.0)	Active		Library	AdminServer, ls_cluster	Global		100
oracle.wls.domain-webapp(1.0.12.1.0.0)	Active		Library	AdminServer, ls_cluster	Global		100
myadminservice (11.1.1)	Active	OK	Enterprise Application	ls_cluster	Global		200
myanalytics	Active	OK	Enterprise Application	ls_cluster	Global		250
myapplicationmodule (11.1.1)	Active	OK	Enterprise Application	ls_cluster	Global		260
myfactors	Active	OK	Enterprise Application	ls_cluster	Global		300
myhttp-discovery (12.1.4)	Active	OK	Web Application	AdminServer	Global		100
myhttp-mat	Active	OK	Enterprise Application	ls_cluster	Global		190
mysecurity	Active	OK	Enterprise Application	ls_cluster	Global		100

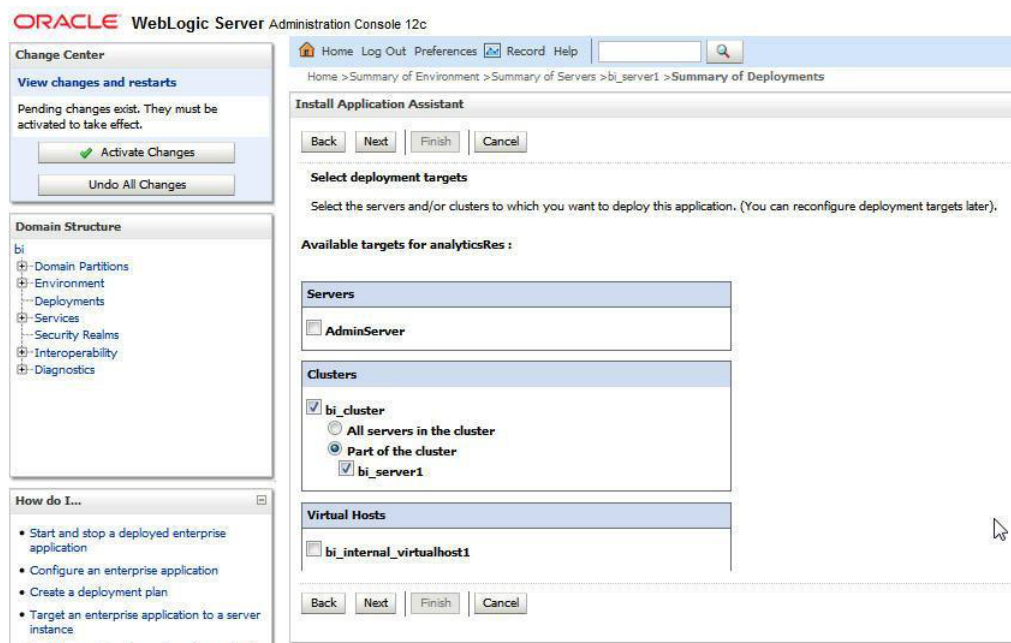
5. Click **Install**, and navigate to the location where opva_help.zip was extracted in Step 1.
6. Select **analyticsRes**, and click **Next**.

The screenshot shows the Install Application Assistant dialog. The 'Path' field is filled with `/scratch/stage/opva_help/analyticsRes`. The 'Recently Used Path' field shows `/scratch/stage/opva_help` and `burg000.us.oracle.com / scratch / stage / opva_help`. The 'Current Location' is `analyticsRes (open directory)`.

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



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

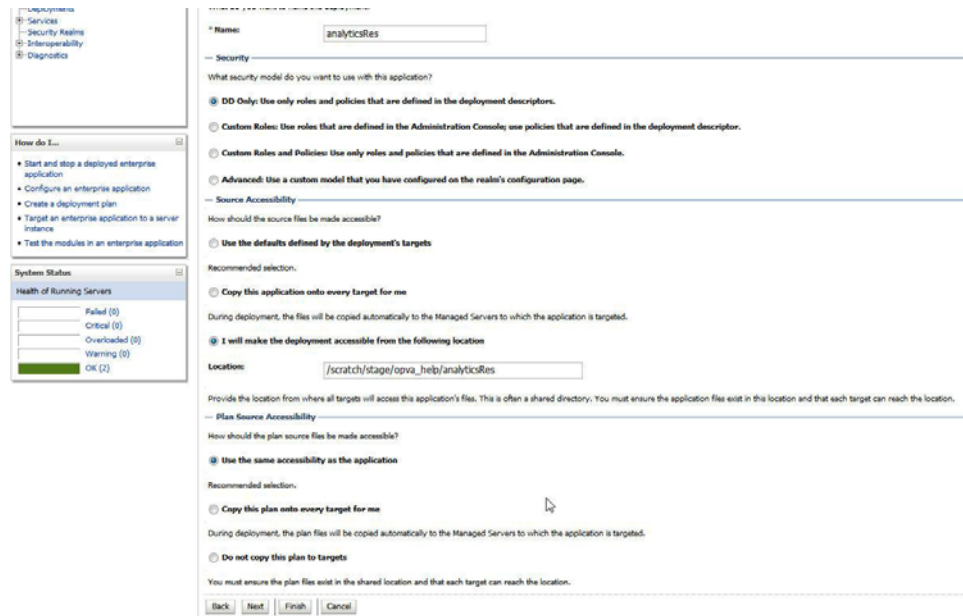


9. Under Source accessibility:

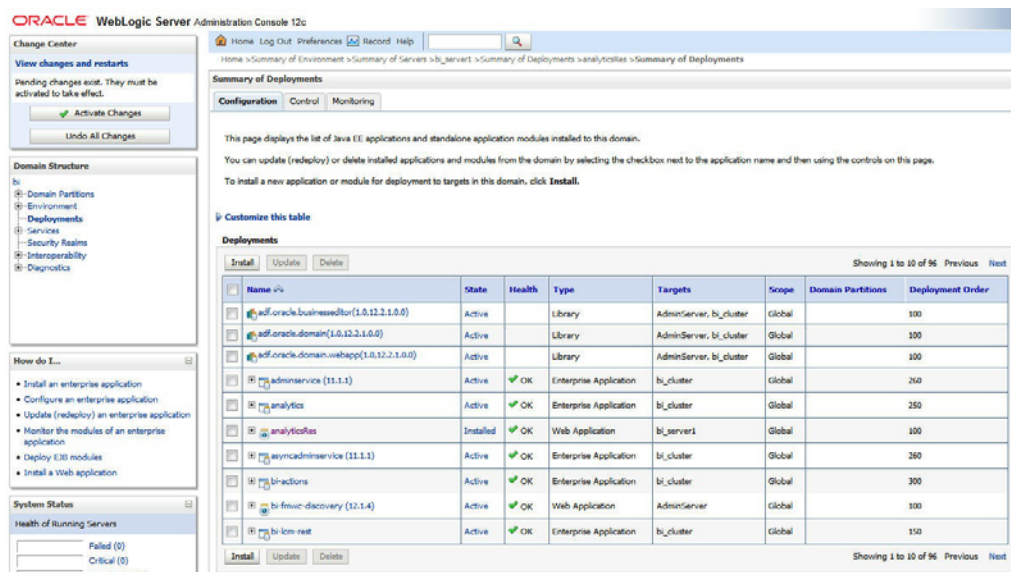
Select **I will make the deployment accessible from the following location** option, and select the path for `analyticsRes` as selected in step 6.

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

10. Click Finish.

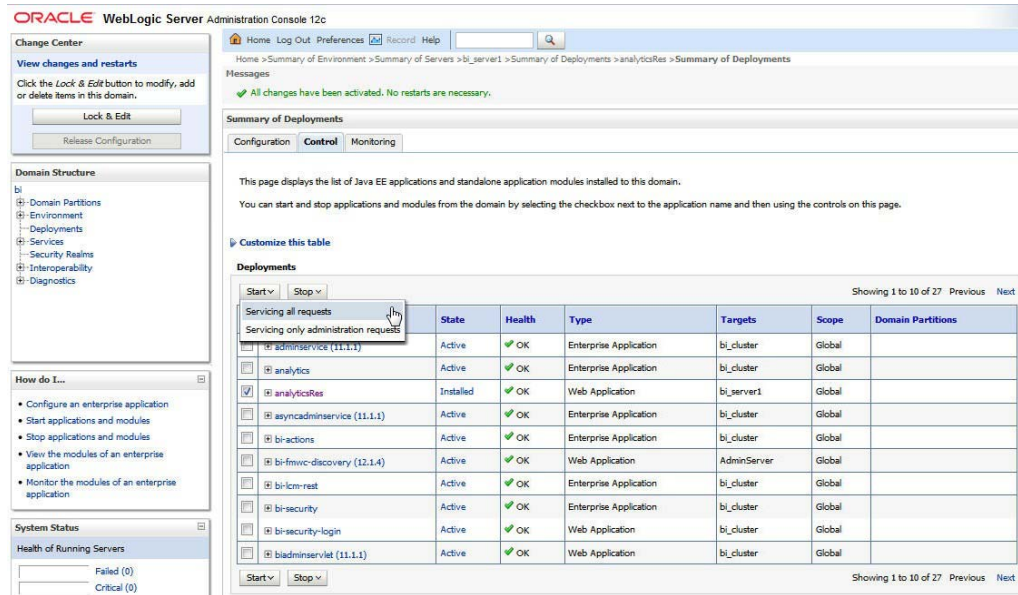


The analyticsRes appears under Deployments.



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 10g

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

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

The following are the pre-requisites for this configuration:

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

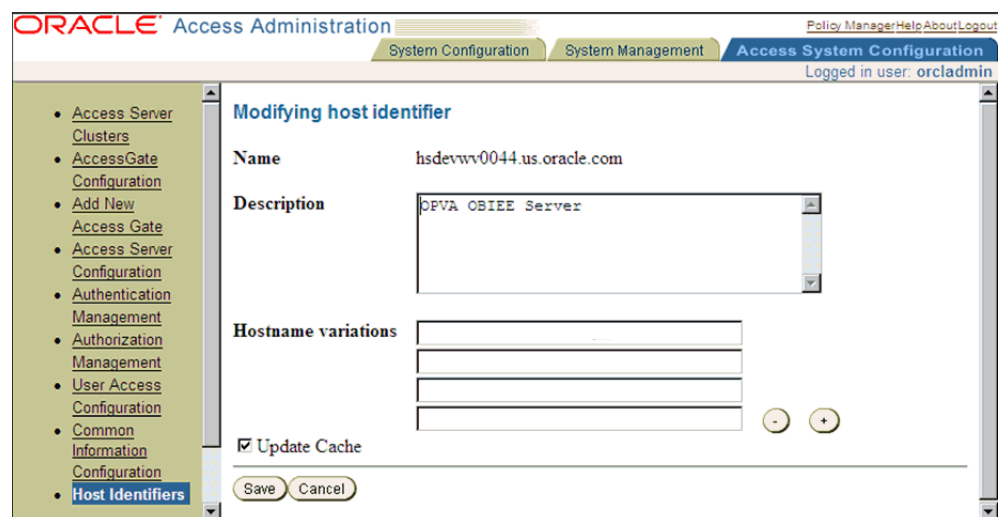
Perform the following steps to install SSO on the OAM:

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

For example:

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



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



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

Figure 2-3 The Host Identifiers Screen with Entered Information



Modify AccessGate

AccessGate Name	AccessGateOPVA	
Description	Access Gate for OPVA Web Server	
State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Hostname**		
Port**	7777	
New Access Gate Password	*****	
Re-type New Access Gate Password	*****	
Debug	<input checked="" type="radio"/> Off <input type="radio"/> On	
Maximum user session time (seconds)*	3600	
Idle Session Time (seconds)	3600	
Maximum Connections	1	
Transport Security	<input checked="" type="radio"/> Open <input type="radio"/> Simple <input type="radio"/> Cert	
IPValidation	<input type="radio"/> Off <input checked="" type="radio"/> On	
IPValidationException		 
Maximum Client Session Time (hours)	24	
Failover threshold	1	
Access server timeout threshold*		
Sleep For (seconds)	60	
Maximum elements in cache*	100000	
Cache timeout (seconds)*	1800	
Impersonation username		
Impersonation password		
Re-type impersonation password		



ASDK Client

Access Management Service	<input type="radio"/> Off <input checked="" type="radio"/> On	
---------------------------	---	--

Web Server Client

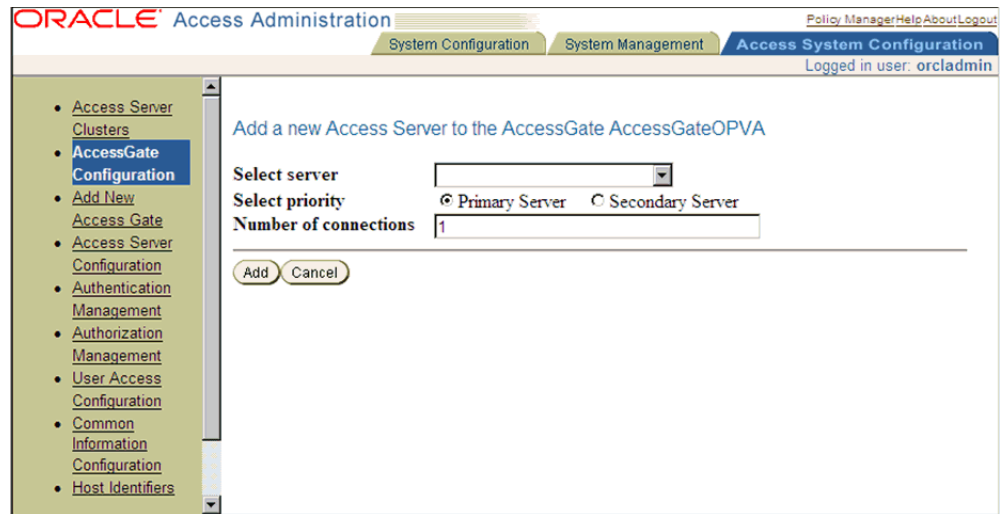
Primary HTTP Cookie Domain*	.us.oracle.com	
Preferred HTTP Host		
Deny On Not Protected	<input checked="" type="radio"/> Off <input type="radio"/> On	
CachePragmaHeader	private	
CacheControlHeader	private	
LogOutURLs		 

User Defined Parameters

Parameters	Values	
		 

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

Figure 2-4 The Access System Configuration: Access Gate Configuration Screen



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

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

Figure 2-5 Authentication Management: General tab

General Plugins Steps Authentication Flow

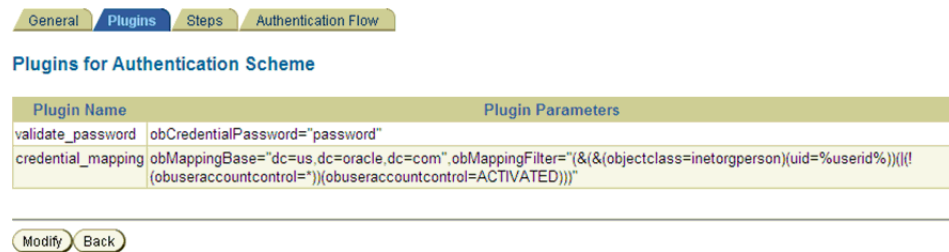
Details for Authentication Scheme

Name	Oracle Access and Identity Basic Over LDAP
Description	Used in protecting Oracle Access Manager related URLs
Level	1
Challenge Method	Basic
Challenge Parameter	realm:Oracle Access and Identity
SSL Required	No
Challenge Redirect	
Enabled	Yes

Modify Back

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

Figure 2–6 Authentication Management: Plugins tab



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

Note: The order of Plugins added is important.

Figure 2–7 Authentication Management: Steps tab



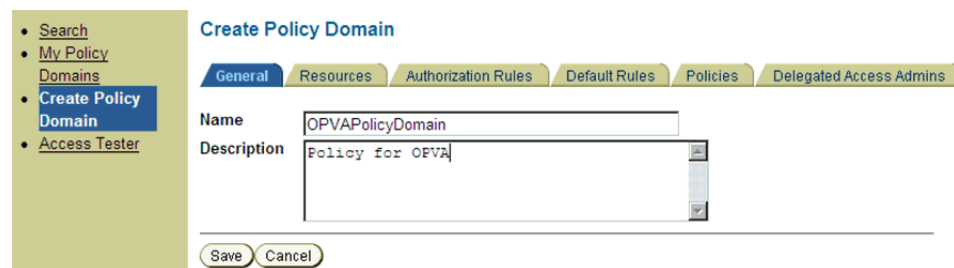
- Click on Save.
- Choose the Authentication Flow Tab and configure as shown below:

Figure 2–8 Authentication Management: Authentication Flow tab



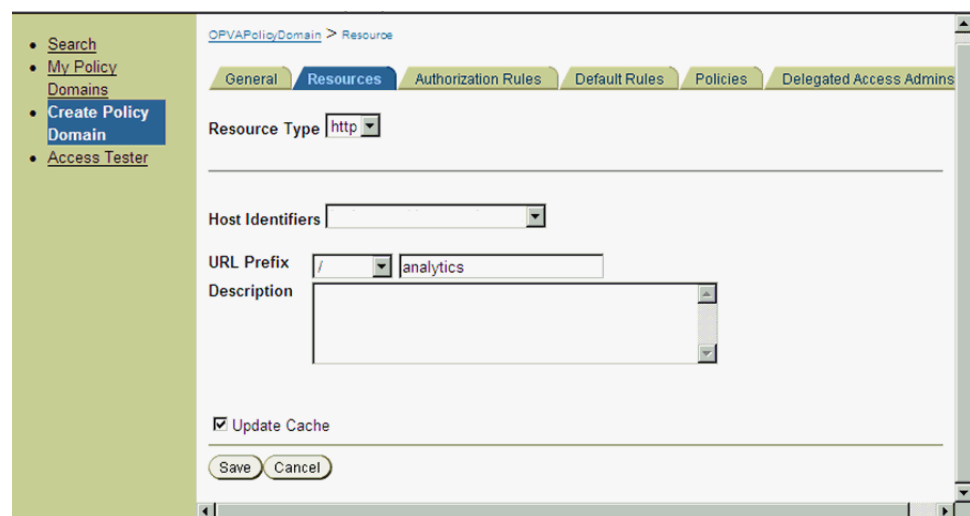
9. Click on Policy Manager to setup the rules for protecting the Oracle Argus Analytics Application URL as follows:
 - Click on Create Policy Domain.
 - Enter the details as given below:

Figure 2–9 Create Policy Domain: General tab



- Click on Save, and then choose 'Modify' set enabled to Yes.
- Navigate to the 'Resources' tab and click on Add and enter details as shown here and click on Save:

Figure 2–10 Create Policy Domain: Resources tab



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

Figure 2–11 My Policy Domains: Authorization Rules tab

OPVAPolicyDomain > Authorization Rules

General Resources **Authorization Rules** Default Rules Policies Delegated Access Admins

General Timing Conditions Actions Allow Access Deny Access

Name: Default_Authorization

Description: Default Authorization

Enabled: Yes

Allow takes precedence: Yes

Update Cache

Save Cancel

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

Figure 2–12 My Policy Domains: Authorization Rules tab: Actions sub-tab

General Resources **Authorization Rules** Default Rules Policies Delegated Access Admins

General Timing Conditions **Actions** Allow Access Deny Access

Authorization Success

Redirection URL: []

Return	Type	Name	Return Value
	[]	[]	[]
	HeaderVar	OAM_REMOTE_USER	uid
	HeaderVar	REMOTE_USER	uid

Authorization Failure

Redirection URL: []

Return	Type	Name	Return Value
	[]	[]	[]
	[]	[]	[]

Update Cache

Save Cancel

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

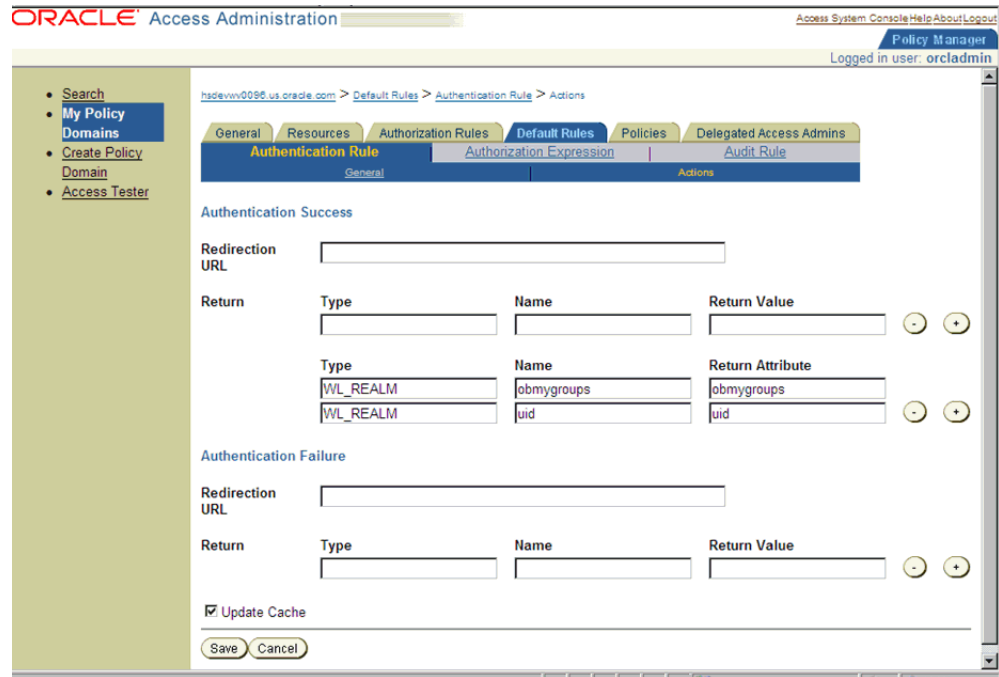
Figure 2–13 My Policy Domains: Authorization Rules tab: Allow Access sub-tab

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

Figure 2–14 My Policy Domains: Default Rules tab: General sub-tab

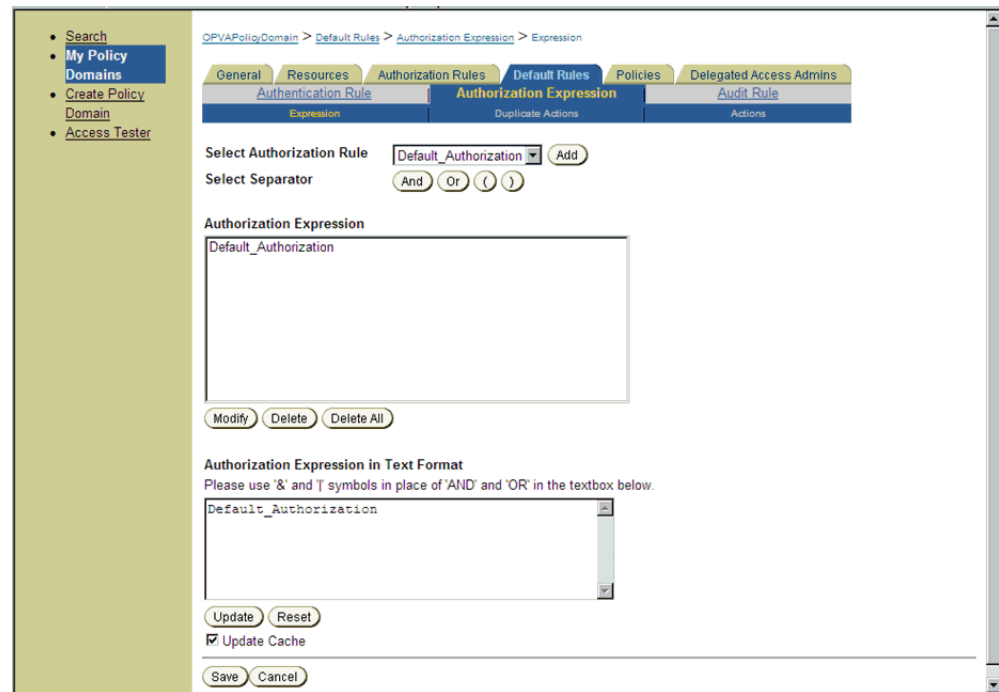
- Save the details in the General sub tab, and choose the Actions sub-tab.
- Click on Add and enter the details as shown here and save the details:

Figure 2–15 My Policy Domains: Default Rules tab: Actions sub-tab



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

Figure 2–16 My Policy Domains: Default Rules tab: Expression sub-tab



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

Figure 2–17 My Policy Domains: Default Rules tab: Actions sub-tab

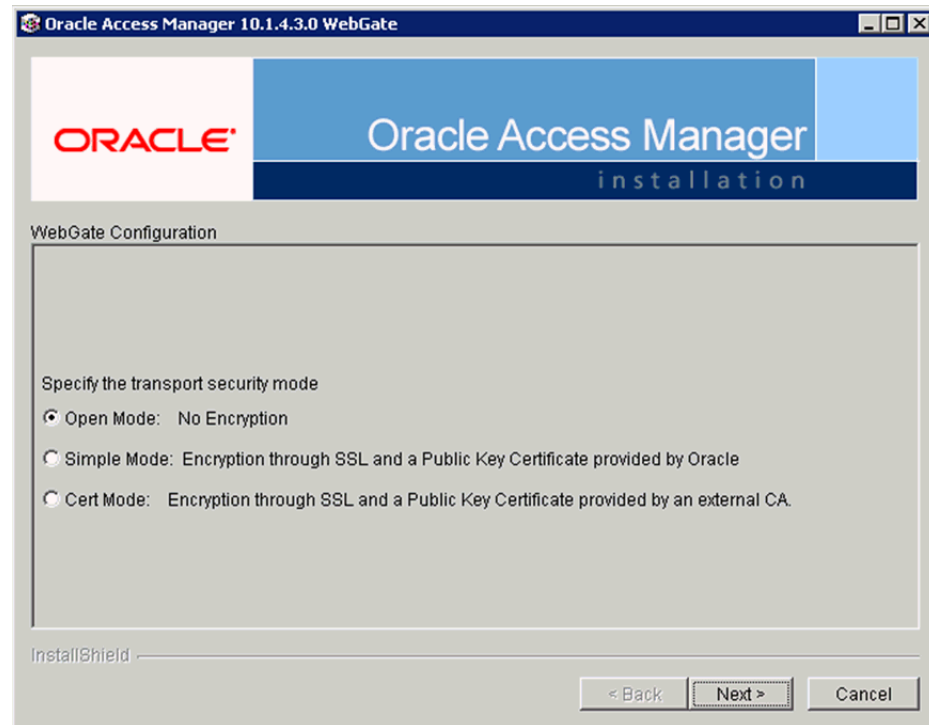
- Click on Save.
- Click on the Policies tab and choose the Add button, enter details as given here:

Figure 2–18 My Policy Domains: Policies tab

10. Navigate to the Oracle Argus Analytics Web Tier Machine, which is the machine where you have installed Oracle Argus Analytics OBIEE Server and run the installer for Webgate (OFM Webgate 11g for OAM 10.1.4.3.0).
 - Once the installer launches, click Next on the initial two information screens

- Choose the install directory for the webgate and click Next for the information on the installation.
- Click Next to begin the installation of webgate, once completed it starts the configuration, where in enter the details as given here below:

Figure 2–19 Oracle Access Manager Installation Screen



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


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

11. Configure the HTTP Server as a reverse proxy for the WebLogic Server

- Modify the file `mod_wl_ohs.conf` present in the location to reflect as shown below: Location:
OracleWebTierHome\instances\instance2\config\OHS\ohs1

Note: This is a template to configure `mod_weblogic`.

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

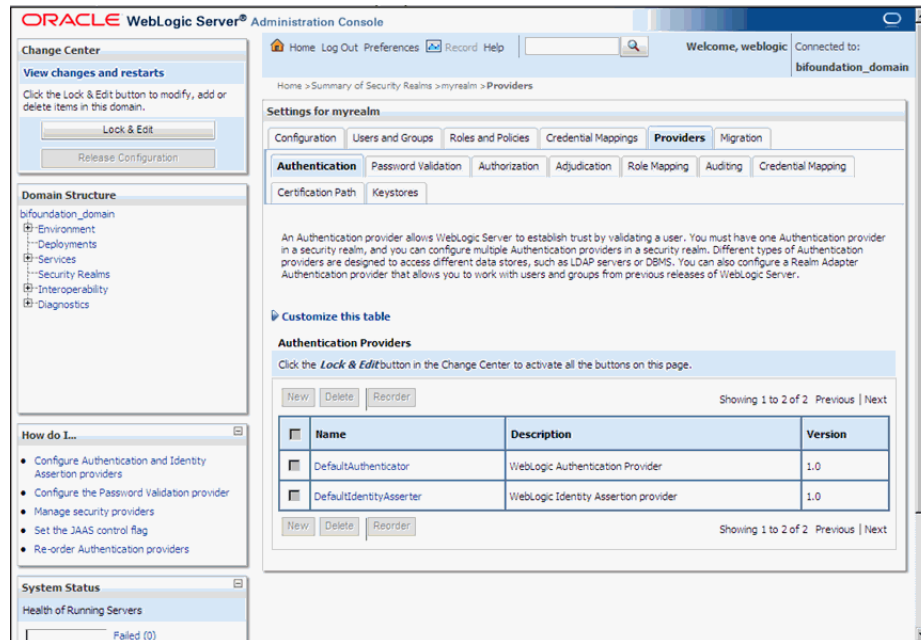
# This empty block is needed to save mod_wl related configuration from EM
to this file when changes are made at the Base Virtual Host Level

<IfModule weblogic_module>
# WebLogicHost <WEBLOGIC_HOST>
# WebLogicPort <WEBLOGIC_PORT>
# Debug ON
# WLLogFile /tmp/weblogic.log
# MatchExpression *.jsp
WebLogicHost hsdevwv0044.us.oracle.com
WLTmpDir <MIDDLEWARE_HOME>\Oracle_WT1\error_Logs
WLLogFile <MIDDLEWARE_HOME>\Oracle_WT1\error_Logs\ohs1_error.log
Debug ON
DynamicServerList Off
WebLogicPort 7001
<Location /analytics>
SetHandler weblogic-handler
WebLogicHost hsdevwv0044.us.oracle.com
WebLogicPort 9704
</Location>
</IfModule>
# <Location /weblogic>
# SetHandler weblogic-handler
# PathTrim /weblogic
# ErrorPage http://WEBLOGIC_HOME:WEBLOGIC_PORT/
# </Location>
```

12. Restart the Web Tier Instance in WebLogic EM

- Configure a new Authenticator for Oracle WebLogic Server
- Log in to the WebLogic Server Administrator Console and navigate the Security Realms-> myrealm and click on the Providers tab

Figure 2–20 myrealm Settings: Providers tab



- Click on Lock & Edit in the right-hand corner of the web page, highlighted as Change Center
- Click New to create a new Authentication Provider and add the details as given here:
 - Name: OPVAOIDAuthenticator, or a name of your choosing
 - Type: OracleInternetDirectoryAuthenticator
 - After saving the details, click on the new Authenticator created and enter details as given here:
 - In the Common sub tab change the Control Flag as SUFFICIENT
 - Click on Save
 - Click the Provider Specific tab and enter the following required settings using values for your environment:
 - Host: Your LDAP host.
For example: hsdevlv0016.us.oracle.com
 - Port: Your LDAP host listening port.
For example: 389
 - Principal: LDAP administrative user.
For example: cn=orcladmin,cn=Users,dc=us,dc=oracle,dc=com
 - Credential: LDAP administrative user password
 - User Base DN: Same searchbase as in Oracle Access Manager.
For example: cn=Users,dc=us,dc=oracle,dc=com
 - All Users Filter:
For example: (&(uid=*) (objectclass=person))

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

For example: uid

Group Base DN: The group searchbase

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

Leave the other defaults as is

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

For example: uid

Click Save.

13. Configuring a new Identity asserter for WebLogic Server

- In Oracle WebLogic Server Administration Console, select Security Realms from the left pane and click the realm you are configuring. For example, myrealm. Select Providers.
- Click New. Complete the fields as follows:
 - Name: OPVAOAMIdentityAsserter, or a name of your choosing
 - Type: OAMIdentityAsserter
 - Click OK
 - Click on the newly created Asserter and set the Control Flag to REQUIRED
 - Click Save
 - Navigate the Provider Specific tab and enter details as given here:
 - Transport Security: open
 - Application Domain: OPVAPolicyDomain, as set in the OAM Policy Manager
 - Access Gate Password: the password for the access gate
 - Access Gate Name: AccessGateOPVA, as specified in the OAM Access Console
 - Primary Access Server: hsdevlv0016.us.oracle.com:8000, OAM server with port
 - Click on Save
- In the Providers tab, perform the following steps to reorder Providers:
 - Click Reorder
 - On the Reorder Authentication Providers page, select a provider name and use the arrows beside the list to order the providers as follows:
 - OPVAOAMIdentityAsserter
 - OPVAOIDAuthenticator
 - DefaultAuthenticator
 - DefaultIdentityAsserter
 - Click OK to save your changes

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

- Check Enable SSO this makes the SSO provider list becomes active.
- Select the configured SSO provider from the list.
- Click Apply, then Activate Changes.
- Manually edit each instanceconfig.xml file for every Oracle BI Presentation Services process to configure the login and logout information. Inside the <Authentication> section, add the following:


```
<SchemaExtensions>
<Schema name="SSO" logonURL="{your SSO logon URL}" logoffURL="{your
logoff
URL}"/>
</SchemaExtensions>
```

For e.g.-

```
<SchemaExtensions>
<Schema name="SSO" logonURL="http://<machinename>.<port>
/analytics/saw.dll?bieehome&startPage=1"
logoffURL="http://<machinename>.<port>
/access/oblix/lang/en-us/logout.html"/>
</SchemaExtensions>
```
- Restart the Oracle Business Intelligence components using Fusion Middleware Control

2.8 Configuring SSO Using Oracle Access Manager 11g

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

Pre-requisites

The following are the pre-requisites to this task:

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

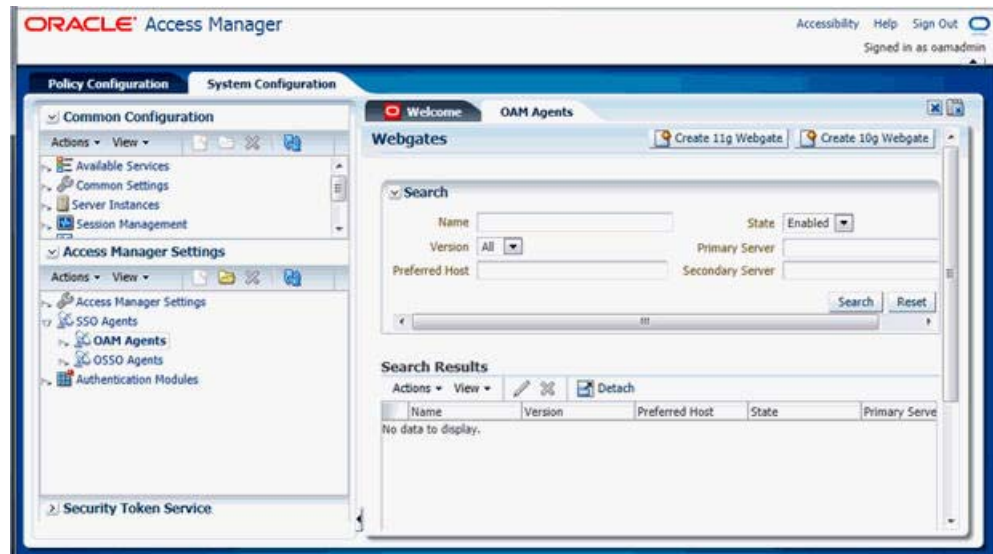
Installing SSO on OAM 11g

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

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

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

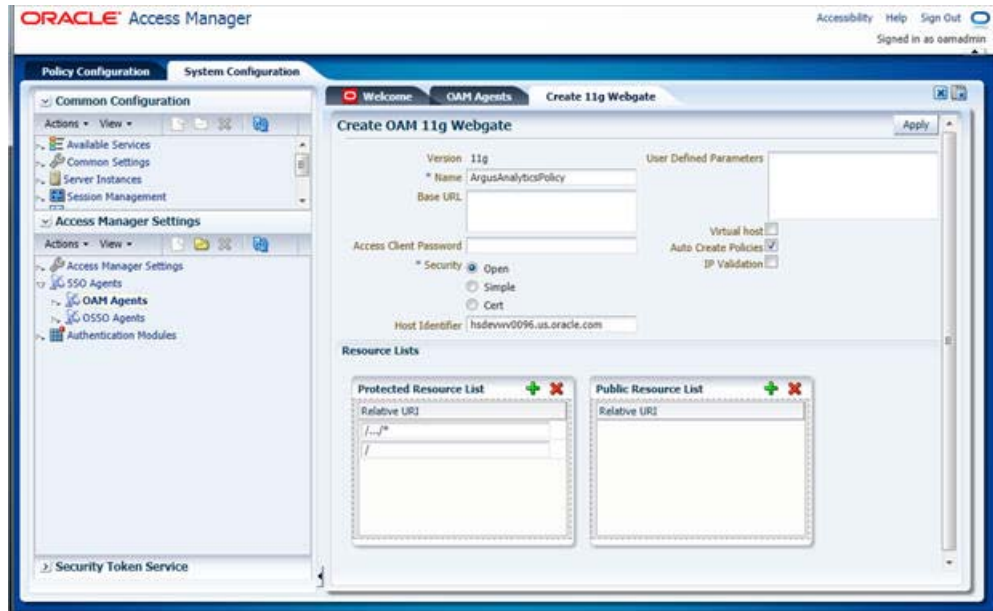
Figure 2–21 Viewing the OAM Agents Page



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

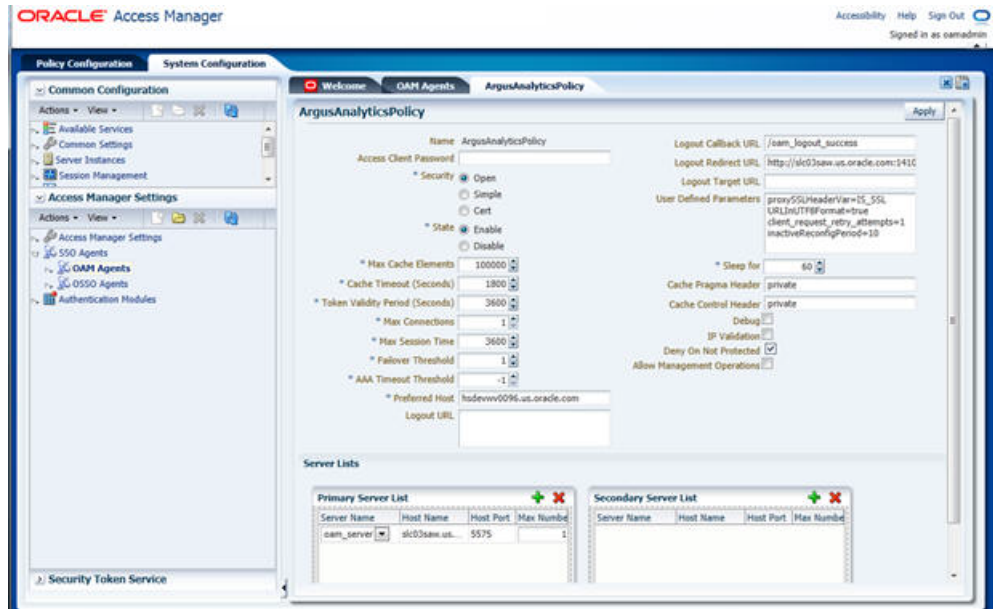
Note: The <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate.

Figure 2–22 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 2–23 Updating Details for ArgusAnalyticsPolicy



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

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

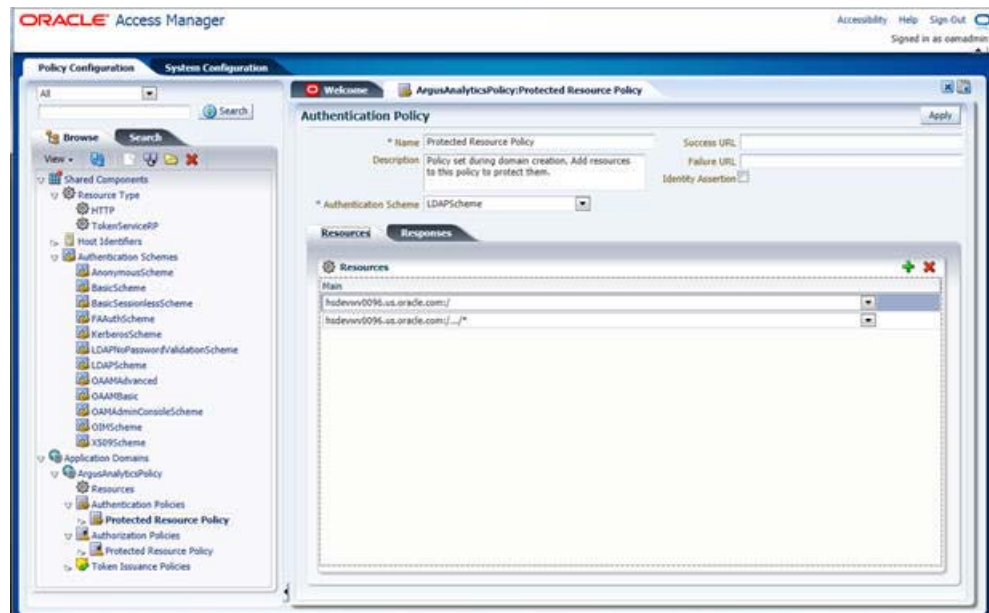
Note: <obiee_server> refers to the server where the OBIEE 11g is installed along with Oracle Web Tier and Oracle Webgate. The port refers to the Oracle Web Tier Port.

Example:

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

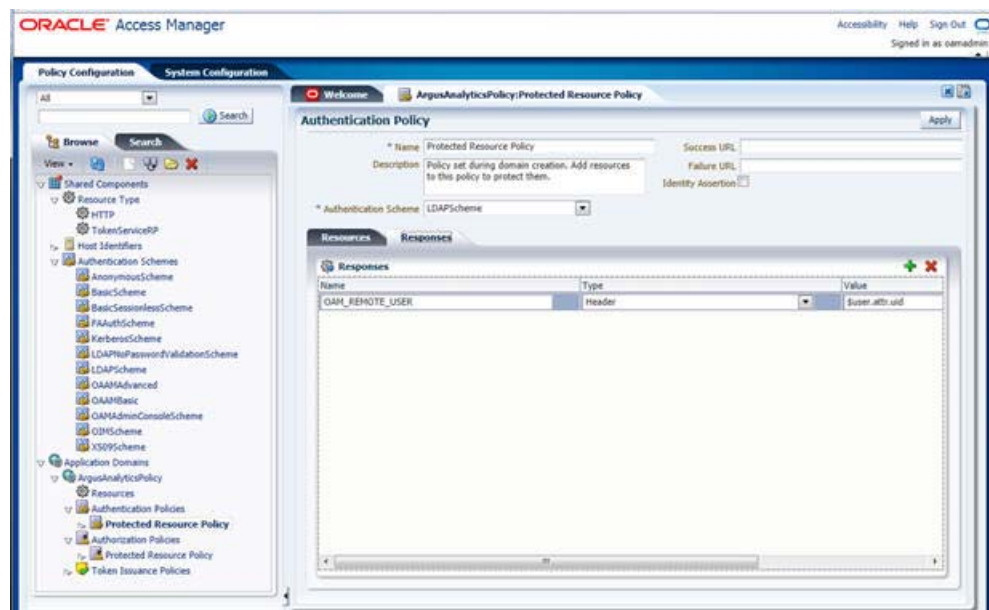
11. Expand and double-click **Application Domains > ArgusAnalyticsPolicy > Authentication Policies > Protected Resource Policy**.
12. Ensure that the Authentication Scheme is set as **LDAPScheme**.
13. Ensure that the following resources are present:
 - /
 - /.../*

Figure 2–24 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 2–25 Adding the Response Variables to Authentication Protected Resource Policy

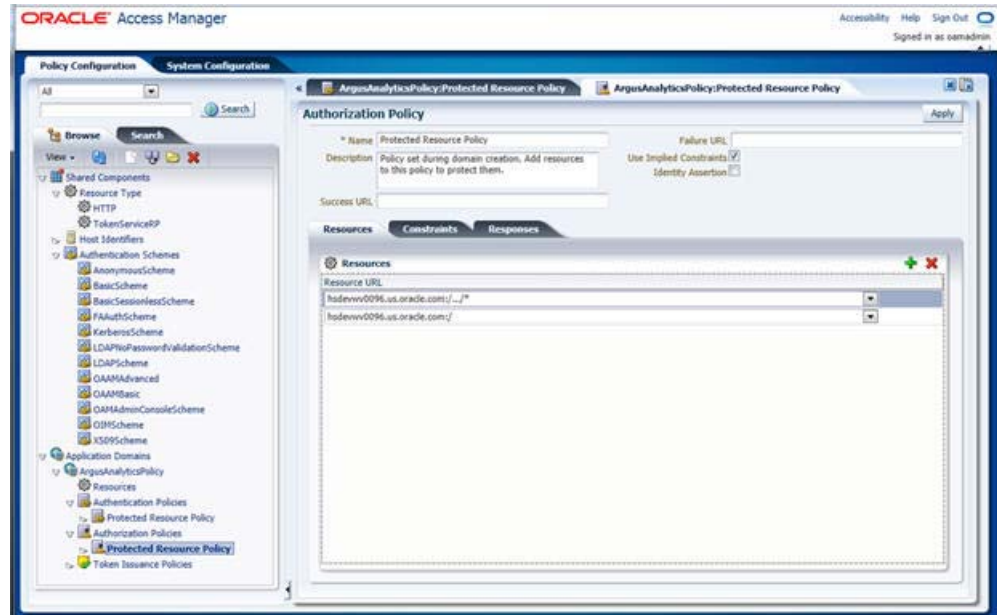


15. Click **Apply** and save the changes.
16. Expand and double-click **Application Domains > ArgusAnalyticsPolicy > Authorization Policies > Protected Resource Policy**

17. Ensure that the following resources are present:

- /
- /.../*

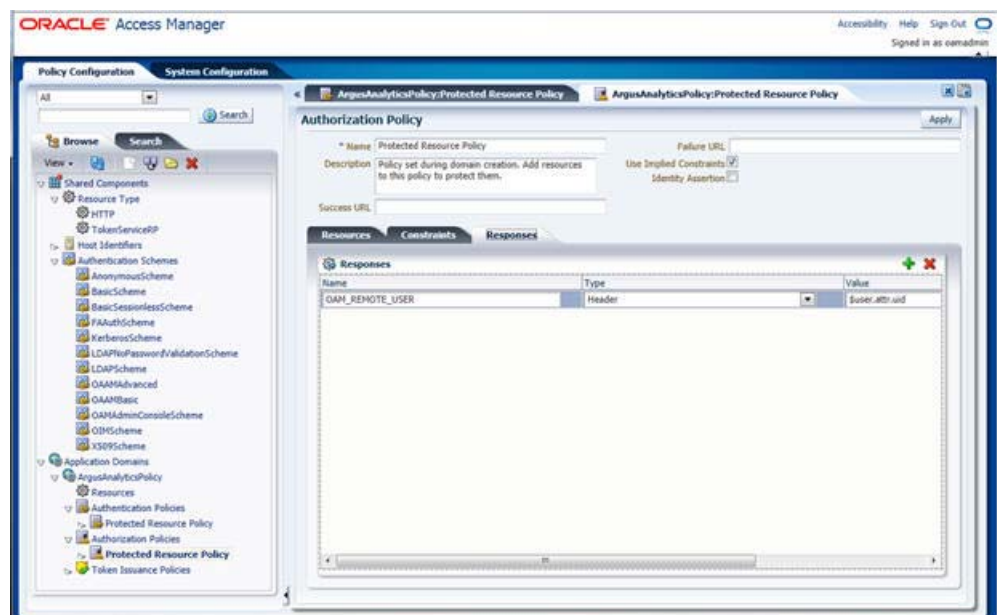
Figure 2–26 Viewing the Authorization Protected Resource Policy



18. Add the following Response variables:

- **Name:** OAM_REMOTE_USER
- **Type:** Header
- **Value:** \$user.attr.uid [as based on the LDAP schema setup]

Figure 2–27 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
```

```
# WLogFile /tmp/weblogic.log
```

```
# MatchExpression *.jsp
```

```
<Location /console>
```

```
SetHandler weblogic-handler
```

```
WebLogicHost hsdevwv0096.us.oracle.com
```

```
WeblogicPort 7001
```

```
WLProxySSL ON
```

```
WLProxySSLPassThrough ON
```

```
</Location>
```

```
<Location /em>
```

```
SetHandler weblogic-handler
```

```
WebLogicHost hsdevwv0096.us.oracle.com
```

```
WeblogicPort 7001
```

```
WLProxySSL ON
```

```
WLProxySSLPassThrough ON
```

```
</Location>
```

```
<Location /analytics>
```

```

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

```

```

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

```

```

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

```

```
</IfModule>
```

```

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

```

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

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

- d. Click **New** to create a new Authentication Provider and add the following details:
 - Name:** OPVАОIDAuthenticator, or a name of your choice
 - Type:** OracleInternetDirectoryAuthenticator
 - e. After saving the details, click the new Authenticator that you have created and enter the following details:
 - In the sub tab change the Control Flag as **SUFFICIENT**
 - f. Click **Save**.
 - g. Click the **Provider Specific** tab and enter the following required settings using values for your environment:
 - **Host:** Your LDAP host.
For example: oid_server.us.oracle.com
 - **Port:** Your LDAP host listening port.
For example: 3060
 - **Principal:** LDAP administrative user.
For example: cn=orcladmin,cn=Users,dc=us,dc=oracle,dc=com
 - **Credential:** LDAP administrative user password
 - **User Base DN:** Same searchbase as in Oracle Access Manager.
For example: cn=Users,dc=us,dc=oracle,dc=com
 - All Users Filter:
For example: (&(uid=*) (objectclass=person))
 - **User Name Attribute:** Set as the default attribute for username in the directory server.
For example: uid
 - **Group Base DN:** The group searchbase
For example: cn=Groups,dc=us,dc=oracle,dc=com
 - Leave the other defaults as is.
 - **GUID Attribute:** The GUID attribute defined in the OID LDAP Server
For example: uid
 - Click **Save**.
- 24.** Configure a new Identity Asserter for WebLogic Server using the following steps:
- a. In the Oracle WebLogic Server Administration Console, select **Security Realms** from the left pane and click the realm which you want to configure. For example, myrealm. Select Providers.
 - b. Click **New** and enter the following values in the fields:
 - Name:** OPVАОAMIdentityAsserter, or a name of your choice
 - Type:** OAMIdentityAsserter
 - c. Click **OK**.
 - d. Click on the newly created Asserter and set the Control Flag to **REQUIRED**.

- e. Ensure that the Active Types that you have selected is **OAM_REMOTE_USER**.
 - f. Click **Save**.
 - g. Navigate to the **Provider Specific** tab and enter the following details:
 - **Transport Security:** open
 - **Application Domain:** ArgusAnalyticsPolicy, as set in the OAM 11g Console
 - **Access Gate Name:** ArgusAnalyticsPolicy, as specified in the OAM 11g Console
 - **Primary Access Server:** oam_server.us.oracle.com:5575, OAM 11g server with port
 - Click **Save**.
 - h. In the **Providers** tab, perform the following steps to reorder Providers:
 - Click **Reorder**.
 - On the **Reorder Authentication Providers** page, select a Provider Name and use the arrows besides the list to order the following providers:
 - OPVAOAMIdentityAsserter
 - OPVAOIDAuthenticator
 - DefaultAuthenticator
 - DefaultIdentityAsserter
 - Click **OK** to save your changes.
 - i. In the **Providers** tab, click **Default Authenticator** and change the Control Flag to **Sufficient**.
 - j. In the Change Center, click **Activate Changes**.
 - k. Restart Oracle WebLogic Server
- 25.** The **BISystemUser** present in the default embedded LDAP must be deleted (using Security Realms in the **Administration Console** Link of the WebLogic Server) and the same/another user must be added in the newly added OID. This user also needs to be added to the BI Application Roles using the following steps:
- a. Navigate to **Administration Console > Security Realms > myrealm > Users and Groups > Users** and select the checkbox against **BISystemUser** (from Provider: Default Authenticator)
 - b. Click **Delete**.
 - c. Navigate to **Security Realms > myrealm > Roles and Policies > Realm Roles**.
 - d. In the tree structure, expand **Global Roles** node and select the **Roles** link.
 - e. In the subsequent screen, click the **Admin Role** link
 - f. Click the **Add Conditions** button.
 - g. In the next screen, select the Predicate List as **User** and click **Next**.
 - h. In the **User Argument Name**, enter **BISystemUser** and click **ADD**.
 - i. Click **Finish**.
 - j. In the **Role Conditions** screen, ensure that the set operator is set to **Or**.

- k. Save the configuration.
 - l. Navigate to the Enterprise Manager of OBIEE or the Fusion Middleware Control page and navigate in the tree structure to the **Business Intelligence > coreapplication** node.
 - m. In the Business Intelligence drop-down menu, select **Security > Application Roles**.
 - n. In the Roles displayed, select **BISystem** and in the next screen remove the old **BISystemUser** (from the Default Provider) and add the newly created **BISystemUser** user in OID.
 - o. Add the trusted user's credentials to the oracle.bi.system credential map.
 - p. Using Fusion Middleware Control target navigation pane, navigate to **farm > WebLogic Domain**, and select **bifoundation_domain**.
 - Using the WebLogic Domain menu, select **Security > Credentials**.
 - Open the oracle.bi.system credential map, and select **system.user**.
 - Click **Edit**.
 - In the **Edit Key** dialog box, enter **BISystemUser** (or the name that you have selected) in the **User Name** field.
 - In the **Password** field, enter the trusted user's password that is contained in Oracle Internet Directory.
 - Click **OK**.
 - q. Restart the Managed Servers.
26. Enable the SSO Authentication in the Weblogic Server for OBIEE using the following steps:
- a. Login to Fusion Middleware Control (EM) of the WebLogic Server.
 - b. Go to the **Business Intelligence Overview** page.
 - c. Go to the **Security** page.
 - d. Click **Lock and Edit Configuration**.
 - e. Check **Enable SSO**, this makes the SSO provider list active.
 - f. Select the configured SSO provider from the list, as **Oracle Access Manager**.
 - g. In **The SSO Provider Logoff URL**, specify the following URL:
 http://<oam_server>:14100/oam/server/logout
 - h. Click **Apply**.
 - i. Click **Activate Changes**.
 - j. Restart the Oracle Business Intelligence components using Fusion Middleware Control.

2.9 Configuring SSL for Oracle Argus Analytics in OBIEE

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**.

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

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

- Configure OBIEE in SSL mode as given in the [Section 2.9, "Configuring SSL for Oracle Argus Analytics in OBIEE"](#)
- Follow the steps as mentioned in the [Part 2.8, "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 2.8, "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 2.8, "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.

2.11 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.

Table 2–3 (Cont.) Creating Users for DAC

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

d. Click on Save.

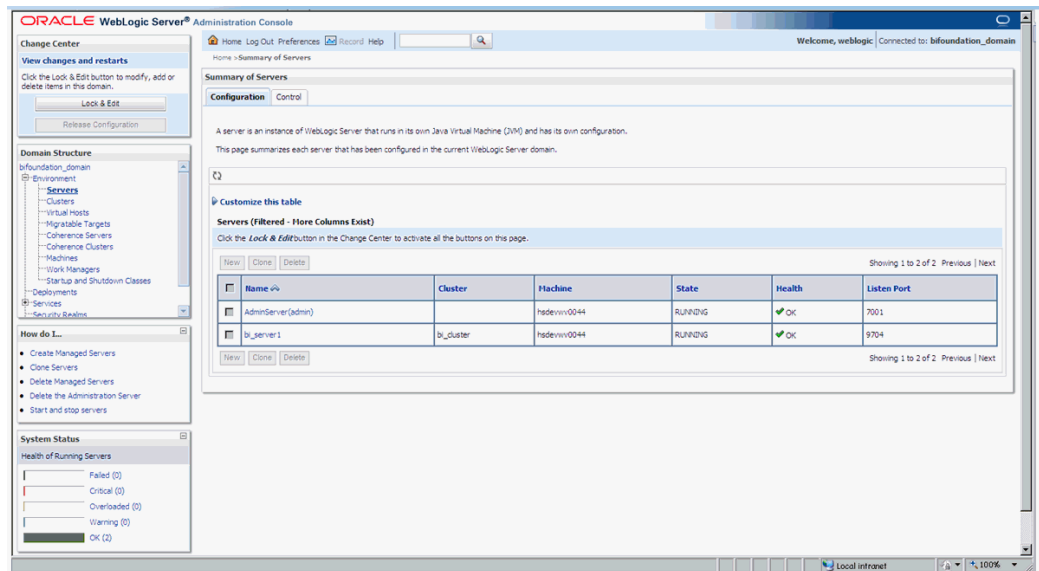
Note: It is recommended to create at least one user to be added with the Administrator Role in DAC to manage the DAC PVA metadata.

2.12 Configuring SSL for Oracle Argus Analytics in OBIEE

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

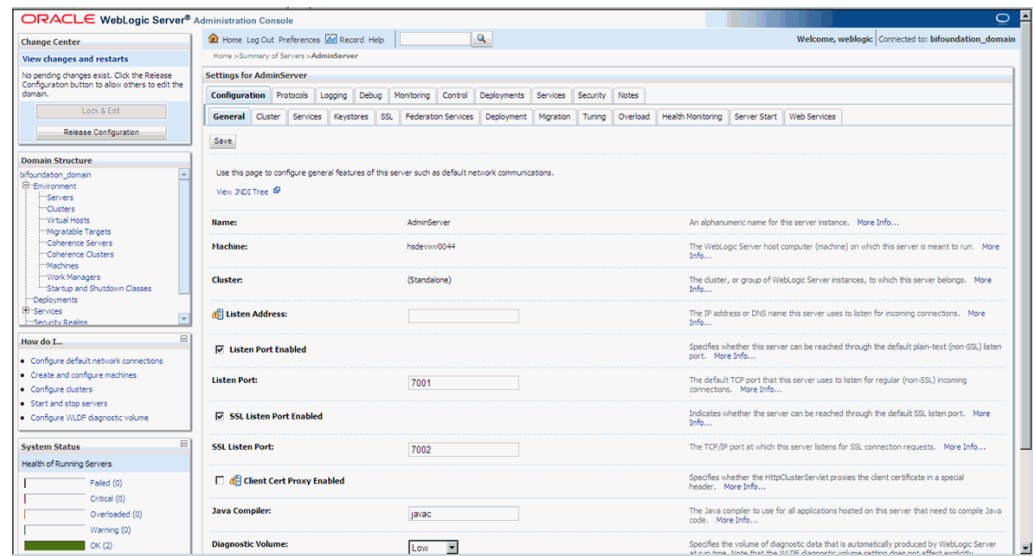
1. Open the WLS Administrator console for OBIEE.
2. Navigate to Environment -> Servers in the tree view displayed on the left side.

Figure 2–28 Servers: Configuration tab



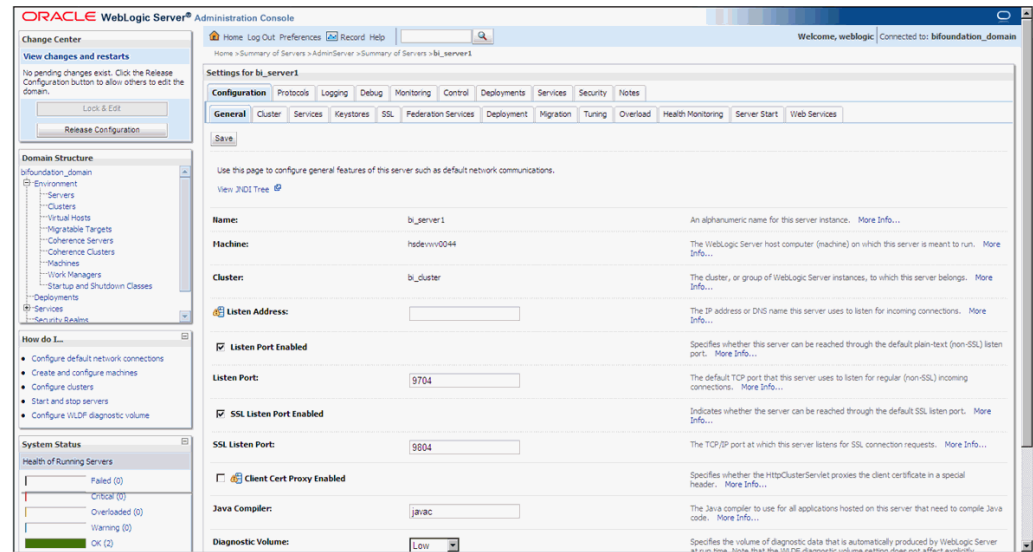
3. Click the Lock & Edit button to change the configuration.
4. Click the AdminServer(admin) link and in the General Tab, enable the SSL listen port, as displayed below:

Figure 2–29 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 2–30 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.

Part II

Appendix

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

Part II contains the following chapter:

- [Chapter A, Creating ODBC Connection for OBIEE Administration Tool](#)

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**.

