Oracle Argus Analytics

Installation Guide

Release 8.4.4
G33670-01
February 2025

Oracle Argus Analytics Installation Guide, Release 8.4.4

G33670-01

Copyright © 2019, 2025, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

Documentation accessibility vi
Diversity and Inclusion vi
Related resources vi
Access to Oracle Support vi

1 Oracle Argus Analytics Requirements

Technology Stack and System Requirements 1-1
- Server Components 1-1
- Client Components 1-2
- Supported Sources 1-3
- Technology Stack Matrix 1-3
  - Supported Security Configuration (Optional) 1-4
- Typical Hardware Architecture 1-4
- Installation Process Overview 1-5

Prerequisites 1-5
- Client Tools 1-5

2 Install Oracle Argus Analytics

Oracle Argus Analytics Upgrade Matrix 2-1
Preinstallation Configuration 2-1
- Configure ETL Client on Oracle Data Integrator 2-3

Run the Oracle Argus Analytics Installer 2-4
- Launch the Universal Installer 2-4
- Complete the Oracle Argus Analytics Installer Process 2-4

3 Oracle Data Integrator Smart Import and Topology Configuration (Oracle Data Integrator only)

Connect to Oracle Data Integrator Studio 3-1
Execute the Oracle Data Integrator Smart Import 3-1
Configure the Topology in Oracle Data Integrator Studio 3-2

Configure the Oracle Data Integrator Agent 3-4
Configure the Standalone Oracle Data Integrator Agent 3-4
Modify Oracle Data Integrator Java EE Agent Connection Pool Settings 3-7

4 Configure Oracle Analytics Server Repository and Webcatalog

Prerequisites 4-1
Upgrade the Oracle Argus Analytics RPD and Catalog (Upgrade Install Only) 4-1
Upgrade RPD 4-2
Upgrade the Oracle Argus Analytics Catalog 4-2
Deploy Oracle Analytics Server Repository and Catalog 4-3
Configure the Oracle Analytics Server Repository and Web Catalog using the BAR File 4-3
Import the BAR file in an existing Oracle Analytics Server instance 4-4
Check if the BAR file has imported RPD, Catalog, and the Security Mode 4-5
Import the BAR file when creating a new Oracle Analytics Server Instance 4-7
Configure Oracle Analytics Server Repository and Web Catalog Manually 4-8
Post-deployment of the Oracle Argus Analytics RPD 4-10
Create Users and Groups in Oracle Analytics Server 4-11
Create groups in Oracle Fusion Middleware Control 4-11
Create users in the Oracle Fusion Middleware Control 4-12
Create Roles and Policies with Oracle Fusion Middleware Control 4-14
Create new application roles 4-14
Create new application policy 4-17
Oracle Analytics Server Catalog Folder-level Permissions 4-19
Oracle Analytics Server Default Application Roles 4-20
Change the Oracle Analytics Server RPD Password 4-29

5 Configure Oracle Analytics Server Help Files

Configure the Help links in the Dashboards and Reports 5-1

6 Configure SSO using the Oracle Access Manager 12c

Prerequisites 6-1
Install SSO on Oracle Access Manager 12c 6-1

7 Enable SSL

Enable SSL in Oracle WebLogic Server 7-1
Configure SSL for SSO with Oracle Access Manager 12c 7-2
Enable default SSL Configuration in OAS 7-3

A Create ODBC Connection for Oracle Analytics Server Administration Tool

Preface

This preface contains the following sections:

- Documentation accessibility
- Diversity and Inclusion
- Related resources
- Access to Oracle Support

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.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related resources

For information about Oracle Argus patches, see My Oracle Support.

All documentation and other supporting materials are available on the Oracle Help Center.

Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

Cloud customers receive support assistance through Support Cloud

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Life Sciences Support Cloud (https://hsgbu.custhelp.com/)

- Japanese interface of Oracle Life Sciences Support Cloud へようこそ (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit Life Sciences Support | Oracle or visit Oracle Accessibility Learning and Support if you are hearing impaired.

On-premises customers receive support assistance through My Oracle Support

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

1
Oracle Argus Analytics Requirements

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.

In this chapter:

- Technology Stack and System Requirements
- Prerequisites

Technology Stack and System Requirements

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

For more information, see:

- Server Components
- Client Components
- Supported Sources
- Technology Stack Matrix
- Typical Hardware Architecture
- Installation Process Overview

Server Components

- **Oracle Argus Analytics Database Server**

  (Enterprise Edition or Standard Edition 19c (19.3+))

  - Operating System as certified by the database
  - Microsoft Windows Server 2022 (64 bit)
  - Microsoft Windows Server 2019 (64 bit)
  - Microsoft Windows Server 2016
  - Memory: RAM 4-16 GB (based on organization size), HDD – at least 500 GB free space
  - CPU: At least 4 Dual Core CPUs
- **Oracle Argus Analytics ETL Server**
  - **Oracle Data Integrator (ODI) Server**
    - Oracle Data Integrator 12.2.1.4

Refer to the *Oracle Data Integrator Installation Guide* for recommended hardware and supported platforms.

  * Operating System: As certified by Oracle Data Integrator
  * Memory: At least 8 GB RAM. HDD – at least 250 GB free space
  * CPU: At least 4 Dual Core CPUs

- **Oracle Analytics Server (OAS)**
  - Oracle Analytics Server 6.4 or 2023

    Refer to the *Installating and Configuring Oracle Analytics Server guide* for further hardware and software requirements.
  - Operating System: As certified by Oracle Analytics Server
  - 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 Oracle Analytics Server, then the Oracle Analytics Developer Client Tool must be installed separately on a Microsoft Windows box.
>
> Refer to the version-specific certification matrix for detailed information on OS certification.

Client Components

- **Oracle Database Client**

  Oracle Argus Analytics requires Oracle database client to connect to the database server. The supported client software version is 19c (19.3+).
- **ETL Client**
  - **Oracle Data Integrator (ODI) Studio**

    An Oracle Data Integrator Studio 12.2.1.4 is required to connect to the Oracle Data Integrator Repository.
- **Oracle Analytics Developer Client Tool**

  Oracle Analytics Developer Client Tool 12.2.1.4 must be installed for configuring the repository file (RPD).
- **Security Component** (Optional)

  You can also configure Single Sign On Support for your reports and dashboards using Oracle Access Manager 12c with latest patch. For more information regarding the Oracle Access Manager installation and supported platforms, refer to the *Oracle Access Manager Installation Guide*.
- **Miscellaneous Components**
  - For running the reports and dashboards, your machine should have the Adobe Flash Player 10 or above installed.

Supported Sources

Oracle Argus Analytics, by default, supports only Oracle Argus Safety. It supports Oracle Argus Safety 8.4.4.

Technology Stack Matrix

Specification	Oracle Analytics Server(OAS)	Database	Oracle Data Integrator (ODI)	Client
Operating System	As certified by Oracle Analytics Server	As certified by Oracle Database	As certified by Oracle Data Integrator	—
Oracle Database	19c (19.3+) Client	19c (19.3+) (Enterprise) - AL32UTF8 character set (Supports both CDB-PDB/Non CDB)	—	—
Oracle Analytics Server	Oracle Analytics Server 6.4 or 2023 (with the latest patch set)	—	—	—
Browser	Google Chrome version 116.0.5845.97 or above Microsoft Edge (Chromium based) version 116.0.1938.54 or above (Official build) (64 bit)	—	—	Google Chrome version 116.0.5845.97 or above Microsoft Edge (Chromium based) version 116.0.1938.54 or above (Official build) (64 bit)
Adobe Reader	Acrobat Reader DC Acrobat Reader XI	—	—	Acrobat Reader DC Acrobat Reader XI
Single Sign On Solution (Optional)	Oracle Access Manager 12.2.1.4	—	—	--
Resolution	—	—	—	1280 x 1024

> **Note:**
>
> Oracle Analytics Developer Client Tool can be installed along with the Oracle Analytics Server, provided the Operating System is Microsoft Windows.

For more information, see:

- Supported Security Configuration (Optional)

Supported Security Configuration (Optional)

- LDAP/LDAPS 3.0
- Single Sign On Solution through Oracle Access Manager 12c

> **Note:**
>
> If Oracle Access Manager is used, then the Oracle Analytics Server must have Oracle Web Tier 19c with in-built WebGate.

Typical Hardware Architecture

- **Servers**:
  - An Oracle Database Server with Oracle Database 19c (19.3+)
  - An Oracle Analytics Server 6.4 or 2023 with latest patch set
  - ETL Server—Oracle Data Integrator Studio 12.2.1.4

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

- **Clients**:
  - ETL Client—Oracle Data Integrator Studio 12.2.1.4
  - Oracle Database Client 19c (19.3+)
  - Oracle Analytics Developer Client Tool (6.4 or 2023)

> **Note:**
>
> All tools can be installed in a single Microsoft Windows box.
>
> If the Oracle Analytics Server server mentioned under the "Servers" section is a Windows Server, then all the clients can be installed in the same box itself.

> **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.

Installation Process Overview

The following steps describes the overview of the installation process:

- Follow the steps described in Section 1.2, Prerequisites.
- Execute the installer – to create the data mart.
- Follow the post-installation steps to configure Oracle Data Integrator and Oracle Analytics Server.

For more information about certifications, go to **My Oracle Support** > **Certifications**.

Prerequisites

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

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

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

- ETL Server—Oracle Data Integrator Studio should be installed on the server machine where ETLs have to be configured.

  > **Note:**
  >
  > Oracle Data Integrator Server needs Master and Work Repository Database, which can be created on the same Data Warehousing Oracle Database Server created above.

- OAS—An Oracle Analytics Server must be installed before the Oracle Argus Analytics Installation. Follow platform-specific Oracle Analytics Server Installation Guide for installation instructions.

For more information, see:

- Client Tools

Client Tools

- ETL Client Tools—Oracle Data Integrator Studio installation mentioned in the sever section above can be used as an ETL client to administer/manage ETL metadata.

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

2
Install Oracle Argus Analytics

> **Note:**
>
> This installation assumes the typical hardware configuration with an Oracle Database server, an ODI Studio, and a Windows Server 2019 (64 bit) or 2016 with Oracle Analytics Server (OAS), ODI Studio, and an Oracle Database Client.
>
> All installation and configuration actions must be performed as an administrator or root user.

In this chapter:

- Oracle Argus Analytics Upgrade Matrix
- Preinstallation Configuration
- Run the Oracle Argus Analytics Installer

Oracle Argus Analytics Upgrade Matrix

You can upgrade Oracle Argus Analytics from version 8.2, 8.2.1, or 8.4 to Oracle Argus Analytics 8.4.4.

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

> **Note:**
>
> To connect to SQLPLUS, execute the following steps:
>
> 1. Open a command window in Windows. Alternatively, in Unix, type at the shell prompt.
> 2. Enter the sqlplus `<dbuser>@<tnsnames_entry>` command and press Enter.
> 3. Enter the password when prompted by the SQLPLUS program.

Preinstallation Configuration

1. The TNS entries for both the Data Mart Schema and the Oracle Argus Safety Database Schema should be present in the Oracle Analytics Server 19c 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 Oracle Argus Analytics data mart and the Oracle Argus Safety Source system should be configured here:

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

3. Configuring the TNS for Oracle Database Servers:

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

   a. Oracle Argus Safety DB Server: `<Oracle Client Home>\network\admin\tnsnames.ora`

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

   b. Oracle Argus Analytics DB Server: `<Oracle DB Home>\network\admin\tnsnames.ora`

      This should contain the TNS entry for Oracle Argus Analytics Data DB Server.

4. Set up the Oracle Client Home in the PATH variable.

5. Set up an INSTALL (DBA) user:

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

      A prompt appears as `Do you want to use SYSDBA to run the script? (Y/N):`. Enter **Y** to run as SYSDBA.

   b. Enter the following inputs:

      - Database Connection String for Oracle Argus Safety or Oracle Argus Analytics DB
      - Enter the user with SYSDBA privileges in <Argus Analytics/Argus Safety> database
      - Enter password for <SYSDBA user> in <Argus Analytics/Argus Safety> database
      - Enter DBA User to be created in <Argus Analytics/Argus Safety> database
      - Enter password for <DBA user> in <Argus Analytics/Argus Safety> database

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

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

6. Set 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 Oracle Argus Analytics DB Instance and the Oracle Argus Safety DB Instance.

You can choose to create tablespaces either by executing a batch file or manually.

- To create tablespace from a **batch** file:
  a. Execute the **ancreatetablespace.bat** file from `<Argus Analytics Installer directory>\install\utils\an_tablespace`.
     A prompt appears as `Do you want to use SYSDBA to run the script? (Y/N):`.
     Enter **Y** to run as SYSDBA.
  b. Enter the following parameters:
     – Database Connection String for Oracle Argus Safety or Oracle Argus Analytics DB
     – Enter the user with SYSDBA privileges in &db_mart. database
     – Enter password for &sysdba_user in &db_mart. Database
     – Enter the DATA Tablespace Name [e.g. AN_DATA_TS]
     – Enter the TEMP Tablespace Name [e.g. AN_TEMP_TS]
     – Enter the complete data file path
     – Tablespace Encryption Required [0 - No, 1 - Yes]
     – Tablespace Encryption Algorithm [e.g AES256]

  Repeat the procedure to create tablespaces for Oracle Argus Safety database and Oracle Argus Analytics database.
- To **manually** create the tablespaces, see the following examples:
  Default TABLESPACE [one each needed at the Oracle Argus Analytics DWH DB Server and Oracle Argus Safety DB Server]:

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

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

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

Next:

- Configure ETL Client on Oracle Data Integrator

Configure ETL Client on Oracle Data Integrator

This section lists steps to configure ETL Client on Oracle Data Integrator and install ODI Studio and create 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).

Oracle Data Integrator 12c has the following types of installation:

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

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

When installing the Oracle Data Integrator, 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 Oracle Data Integrator 12.2.1.4.

Run 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, 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 is installed.

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

For more information, see:

- Launch the Universal Installer
- Complete the Oracle Argus Analytics Installer Process

Launch the Universal Installer

1. Extract the contents of the media pack into a temporary directory (for example, `C:\argus_analytics_temp`).
2. Set the Java install path in the server system's environment variables.
3. Open the command prompt as an administrator, and navigate to the directory where you extracted the contents in step 1.
4. Execute `runSetup.bat`.
5. Continue with the steps in the next topic, Complete the Oracle Argus Analytics Installer Process.

Complete the Oracle Argus Analytics Installer Process

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

1. **Choice of New Install / Upgrade from Previous Versions**

   Select if Oracle Argus Analytics is a fresh installation or an upgrade installation, which is supported from Oracle Argus Analytics 8.2, 8.2.1, 8.4, or 8.4.1.

> **Note:**
>
> For an upgrade installation, you need to provide information about the previous Oracle Argus Analytics installation.

2. **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 scripts.

   Home Name: ANHome1

   Path: C:\argus_analytics

   Click **Next**.

> **Note:**
>
> If this is an upgrade installation, provide the Home Name and path for the previously installed version of Oracle Argus Analytics.

3. **Oracle Argus Analytics (File Drop/Database Upgrade)**

   Do you want to just drop files?

   - **Yes:**This option does not install or upgrade the database. Instead it only copies the files from the installer location to Oracle Argus Analytics Home, and jumps to Step 8 Summary Screen.
   - **No:** This option copies the files from the installer location to Oracle Argus Analytics Home and database install or upgrade is executed simultaneously. The installer continues to Step 4 to prompt for necessary details.

4. **Select the Choice of New Install / Upgrade from Oracle Argus Analytics 8.2, 8.2.1, 8.4, or 8.4.1.**

   The sections below explain the details you provide for both new installations and upgrades.

5. **Oracle Argus Safety Database Details**

   This screen collects all information about the source Oracle Argus Safety database.

   Supply the values for:

   - Oracle Argus Safety Database Connect String
   - Oracle Argus Safety Schema, Password
   - Oracle Argus Safety DBA User: Enter the custom INSTALL(DBA) user name (created in Preinstallation Configuration> Step 5).
   - Oracle Argus Safety DBA Password: Password of the INSTALL(DBA) user
   - VPD Schema Name
   - ESM Schema Owner
   - ESM Schema Password
   - Oracle Argus Analytics Source Schema and Password
   - Oracle Argus Analytics Source RPD Schema and Password

- Oracle Argus Analytics Source Work Schema and Password
- Oracle Argus Analytics Source Default Tablespace [<AN_DATA_TS>]
- Oracle Argus Analytics Source Temp Tablespace [<AN_TEMP_TS>]

> **Note:**
>
> Oracle Argus Analytics Source schema, Oracle Argus Analytics Source RPD schema, and Oracle Argus Analytics Source Work schema are the new schemas which would get created by the installer to store the views for all Oracle Argus Safety 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 details of the existing Oracle Argus Analytics Schemas.

For example:

- Oracle Argus Safety Database Connect String: AS70X_SID
- Oracle Argus Safety Schema: ARGUS_APP
- Oracle Argus Safety Password: <ARGUS_APP user's password>
- Oracle Argus Safety DBA User Name: <INSTALL user name>
- Oracle Argus Safety DBA User Name: <INSTALL user's password>
- VPD Schema: VPD_ADMIN
- ESM Schema Owner: ESM_OWNER
- ESM Schema Password: < ESM_OWNER's password>

Click **Next**

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

6. **Oracle Argus Analytics Data Mart Details**

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

   The following are the details of the data mart:

   - DWH Data Mart DB Connect String
   - DWH Data Mart DBA User name: Enter the customer INSTALL(DBA) User Name (created in Preinstallation Configuration> Step 5).
   - DWH Data Mart DBA User Password: Password of the INSTALL(DBA) user

- DWH Schema and Password
- DWH RPD Schema and Password
- DWH Work Schema and Password
- DWH Default Tablespace
- DWH Temporary Tablespace

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

For example:

- DW Database Connect String: ANDWH_SID
- DW DBA User Name: <INSTALL user name>
- DW DBA User Password: <INSTALL user's password>
- Oracle Argus Analytics DW Schema: AN_DWH
- Oracle Argus Analytics DW Password: <password for AN_DWH schema>
- Oracle Argus Analytics RPD Schema: AN_DWH_RPD
- Oracle Argus Analytics RPD Password: <password for AN_DWH_RPD schema>
- Oracle Argus Analytics Work Schema: AN_DWH_WRK
- Oracle Argus Analytics Work Password: <password for AN_DWH_WRK schema>
- DW Default table space: <AN_DATA_TS>
- DW Temporary tablespace: <AN_TEMP_TS>

Click **Next**.

7. **Exadata Database**

   If the Datawarehouse DB Server is Exadata, select **Yes**.

8. **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 Oracle Argus Safety installation is a multitenant application.

   After the installation has been completed, the install log can be verified from the following path or from your local Oracle Inventory logs folder.

   ```
   <Argus Analytics Home>\install\pvadriverscript<timestamp>.log
   ```

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

3

Oracle Data Integrator Smart Import and Topology Configuration (Oracle Data Integrator only)

In this chapter:

- Connect to Oracle Data Integrator Studio
- Execute the Oracle Data Integrator Smart Import
- Configure the Topology in Oracle Data Integrator Studio
- Configure the Oracle Data Integrator Agent
- Modify Oracle Data Integrator Java EE Agent Connection Pool Settings

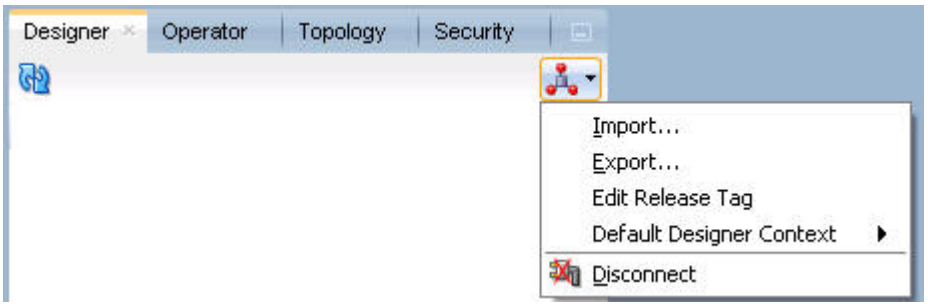
Connect to Oracle Data Integrator Studio

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`.

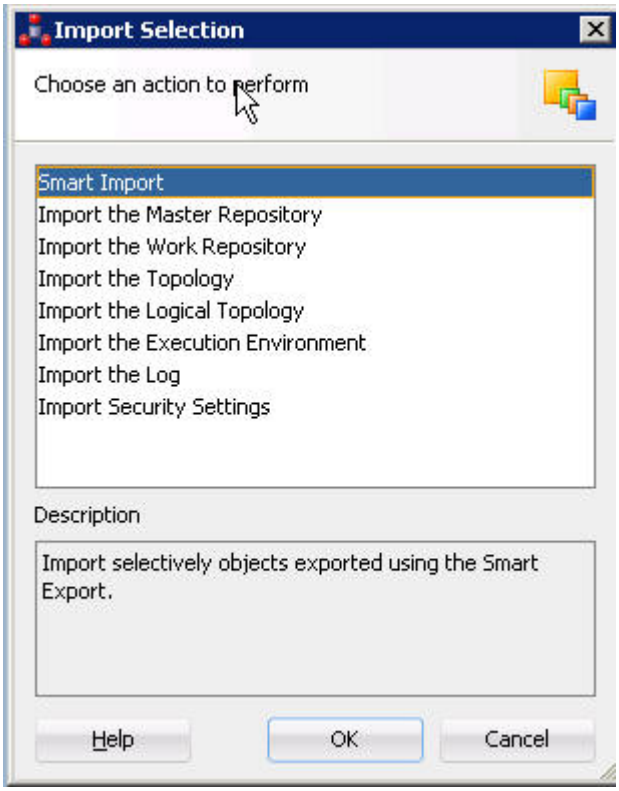
Refer to the `Oracle Data Integrator Installing and Configuring Guide` for 12.2.1.4.

Execute the Oracle Data Integrator Smart Import

1. Log in to the work repository in Oracle Data Integrator 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**.

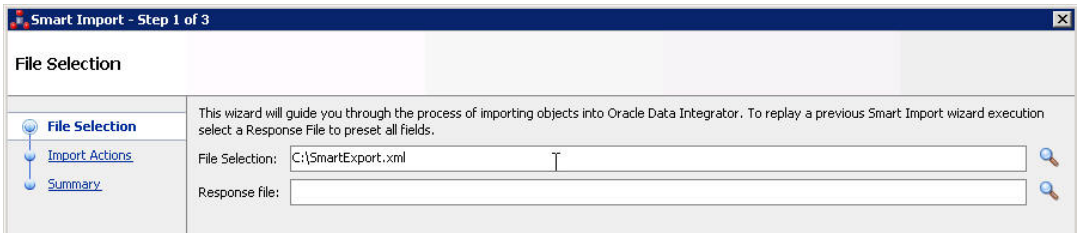


3. Select **Smart Import** from the **Import Selection** menu and click **OK**.



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. Oracle Data Integrator imports the file and checks for any issues that can occur while importing Oracle Data Integrator 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 Oracle Argus Analytics objects in Oracle Data Integrator repository and makes them visible in the Oracle Data Integrator Studio Console.

Configure the Topology in Oracle Data Integrator Studio

1. Open the Oracle Data Integrator Studio and connect as Oracle Argus Analytics 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 one of the following fields:
   - JDBC URL: jdbc:oracle:thin: <DWH_DB_SERVER>:<DWH_DB_LISTENER_PORT>:<DWH_DB_SID>
   - jdbc:oracle:thin: <DWH_DB_SERVER>:<DWH_DB_LISTENER_PORT>/ <DWH_DB_SERVICE_NAME>

   Use the jdbc connection string with database SERVICE_NAME in case the Oracle Database version is 19c.
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 Oracle 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 one of the following fields:
    - JDBC URL: jdbc:oracle:thin: <AS_DB_SERVER>:<AS_DB_LISTENER_PORT>:<AS_DB_SID>
    - jdbc:oracle:thin: <AS_DB_SERVER>:<AS_DB_LISTENER_PORT>/ <AS_DB_SERVICE_NAME>

    Use the jdbc connection string with database SERVICE_NAME in case the Oracle Database version is 19c.
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.

Configure the Oracle Data Integrator 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 *Oracle Data Integrator Install and Configuration Guide > Planning the Oracle Data Integrator Installation section*.

When installing the Oracle Data Integrator, use SUPERVISOR credentials, and Master and Work Repository credentials as created in the Configure ETL Client on Oracle Data Integrator.

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

Refer to the `Oracle Data Integrator Installing and Configuring Guide` for 12.2.1.4.

For topics with further information, see:

- Configure the Standalone Oracle Data Integrator Agent

Configure the Standalone Oracle Data Integrator Agent

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

> **Note:**
>
> The Host field contains the Host name where the Oracle Data Integrator 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 Oracle Argus Analytics Oracle Analytics Server URL available to the end users, the Initial/Full load ETL (LP_FL_AN) in Oracle Data Integrator should be successfully run.
>
> To run the ETLs in Oracle Data Integrator 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. In Oracle Data Integrator, 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 3-1 Oracle Data Integrator 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 Oracle Argus Safety DB support	Valid values:0: Does not truncate Stage table1: Truncate Stage tableShould be specified as 1 always in case of Single Oracle 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

Table 3-1 (Cont.) Oracle Data Integrator Parameters

Parameters	Load Type	Description	Allowed Values
VAR_ALN_ENTERPRISE	Both	The specific Enterprise ID to run the ETL for.	-1: Runs the ETL for the entire Warehouse 0: Runs the ETL for all the enterprises the user ($$p_user_name) has access to Integer Value [1,2,3, etc]: Runs the Incremental ETL for the specified Enterprise only. **Note:** For Full Load, this value has to be -1.
VAR_ALN_ERROR_REJECT_LIMIT	Both	This variable is used to set the number of rows that will be tracked in the respective error tables prior to aborting the ETL in case of errors.	Valid Values: Positive Integer numbers: (E.g. 0, 100, 1000, etc.) UNLIMITED: All the error records are logged Recommended Value: UNLIMITED
VAR_ALN_USER_NAME	Both	The user name for which the ETL shall use to set the VPD Context for the specified enterprise in the parameter: VAR_ALN_ENTERPRISE. This value should be passed inside single quotes: such as 'username'.	Default value: 'admin'
VAR_INT_RAISE_ERROR	Both	Setting this variable to 0 or 1 will appropriately either stop a Load Plan/Interface or continue the same when data errors are encountered during the load.	0: Do not raise data error when encountered during ETLs 1: Raise data error when encountered during ETLs Recommended Value: 1
VAR_INT_CONFIG_DAYS	Incremental Load	Reduces the incremental extract window by the specified number of days. For example: Extract all changed rows between LAST_EXTRACT_DATE and (SYSDATE - $$p_config_days)	Integers Recommended Value: 0

Modify Oracle Data Integrator Java EE Agent Connection Pool Settings

> **Note:**
>
> This section is applicable only if you are using Oracle Data Integrator Java EE Agent.

After configuring the Oracle Data Integrator 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 Oracle Data Integrator 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.

   Without increasing the connection pool size the Oracle Argus Analytics ETLs will fail.

4

Configure Oracle Analytics Server Repository and Webcatalog

In this chapter:

- Prerequisites
- Deploy Oracle Analytics Server Repository and Catalog
- Create Users and Groups in Oracle Analytics Server
- Create Roles and Policies with Oracle Fusion Middleware Control
- Oracle Analytics Server Catalog Folder-level Permissions
- Oracle Analytics Server Default Application Roles
- Change the Oracle Analytics Server RPD Password

Prerequisites

Make sure Oracle Analytics Server 6.4 with latest patch set is installed and the Administrator Console and the Oracle Enterprise Manager (Oracle 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. Check with your Oracle WebLogic Server administrator for the correct port number if the above port does not work as expected.

For more information, see:

- Upgrade the Oracle Argus Analytics RPD and Catalog (Upgrade Install Only)

Upgrade the Oracle Argus Analytics RPD and Catalog (Upgrade Install Only)

> **Note:**
>
> Catalog and RPD upgrade are not available from Oracle Argus Analytics 1.1/1.1.1/7.0.3/8.0/8.1/8.1.1/8.2/8.2.1/8.4/8.4.1. Use the latest catalog provided with the AN 8.4.4 installation (present at `<AN_INSTALL_HOME>/catalog/opva.zip`) for deployment.

For more information, see:

- Upgrade RPD
- Upgrade the Oracle Argus Analytics Catalog

Upgrade RPD

The following steps upgrades the Oracle Argus Analytics 8.2.1 RPD to the latest code in Oracle Argus Analytics 8.4.4.

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

To upgrade the Oracle Argus Analytics RPD (if required):

1. Open the existing Oracle Argus Analytics RPD file that you wish to upgrade to Oracle Argus Analytics 8.4.4 in the Oracle Analytics 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 Oracle Argus Analytics 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 Oracle Argus Analytics 8.4.4 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 Oracle Argus Analytics 8.4.4 release.
14. Copy this file to another location and rename it back to `opva.rpd`, which will later be used to deploy on the Oracle Analytics Server.

Upgrade the Oracle Argus Analytics Catalog

Catalog upgrade from Oracle Argus Analytics 8.2 or 8.2.1 is not available. Use the latest catalog provided with the Oracle Argus Analytics 8.4.4 installation (present at `<AN_INSTALL_HOME>/catalog/opva.zip`) for deployment.

Deploy Oracle Analytics Server Repository and Catalog

In this section:

- Configure the Oracle Analytics Server Repository and Web Catalog using the BAR File
- Import the BAR file when creating a new Oracle Analytics Server Instance
- Configure Oracle Analytics Server Repository and Web Catalog Manually
- Post-deployment of the Oracle Argus Analytics RPD

Configure the Oracle Analytics Server 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 Oracle Analytics Server, using the Oracle Analytics Server Administrator Tool. You must remember to use this password in the steps mentioned below.

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

```
<Argus Analytics Home>\report\ssi.bar
```

A BAR file contains the following Oracle Analytics application module artifacts:

- Data model metadata for the Oracle Analytics Server. This metadata is xml-based but functionally equivalent to an .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.

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

For more information, see:

- Import the BAR file in an existing Oracle Analytics Server instance
- Check if the BAR file has imported RPD, Catalog, and the Security Mode

Import the BAR file in an existing Oracle Analytics Server instance

Before importing the BAR file, make sure:

- Oracle Analytics Server 6.4 is installed.
- The Administrator Console is up and running.
  (validate it from `http://<machinename>.<port>/console`)
- The Oracle Enterprise Manager (Oracle 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 Oracle Analytics Server is installed.
2. Login to the Oracle 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:

   `<oas_home>/user_projects/domains/bi`

   The Key appears at the end of the command.

> **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.
>
> While executing the WLST on Windows server, you must use forward slash (/) to avoid any error messages.

9. Exit WLST using the **exit ()** command.
10. To import the BAR file, Go to the Domain Home path `<oas_home>/user_projects/domains/bi/bitools/bin` and execute the command, importarchive.cmd Oracle Analytics Service Instance key `<Complete path of Bar file to import>`

    BI Service Instance Key: `ssi` (This key must be **ssi** for Oracle Argus Analytics deployment). For example,

    ```
    importarchive.cmd ssi C:\an844\ssi.bar
    ```
11. Go to Oracle 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.

Check if the BAR file has imported RPD, Catalog, and the Security Mode

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

   The following roles are imported as deafult 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 Analytics Tool opens.

      > **Note:**
      >
      > If Oracle Analytics Server is installed on Unix or Linux machine, then you must setup the Oracle Analytics Developer Client tool on any windows machine to access Oracle Analytics Administration Tool.
      > See Create ODBC Connection for Oracle Analytics Server Administration Tool.

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

> **Note:**
>
> You must set the Open Database Connectivity (ODBC).
>
> To open the RPD in the online mode on Unix or Linux, set the ODBC on a Windows machine where Oracle Analytics Server 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--Oracle Argus Analytics database TNS Name
       * User name--Oracle Argus Analytics DWH RPD schema <AN_DWH_RPD>
       * Pasword--Password for Oracle Argus Analytics DWH RPD schema
     - OPVA_CP_InitBlocks:
       * Data Source Name--Oracle Argus Analytics database TNS Name
       * User name--Oracle Argus Analytics DWH RPD schema <AN_DWH_RPD>
       * Password--Password for Oracle Argus Analytics DWH RPD schema
   - Under OPVA_SRC database:
     - OPVA_CP:
       * Data Source Name--Oracle Argus Safety database TNS Name
       * User name--Oracle Argus Analytics SRC RPD schema <AN_SRC_RPD>
       * Password--Password for Oracle Argus Analytics SRC RPD schema

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

   Ignore the warning message that appear during the consistency check.

4. To view and administer privileges for the Oracle Analytics components, login to Oracle Analytics Server Analytics (`http://oasset.com:port/analytics`) with WebLogic user credentials.

5. Go to **Security** > **Administration** > **Manage Privileges**.

   For a list of privileges assigned to the Oracle Analytics Application roles, refer to Oracle Analytics Server Default Application Roles.

6. Go to **Catalog**, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)

7. Create Oracle Analytics Server Groups and Users. (See Create Users and Groups in Oracle Analytics Server)

Import the BAR file when creating a new Oracle Analytics Server Instance

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

   When creating an instance in Oracle Analytics Server 6.4, on the Oracle Analytics Server Initial Application wizard screen, select **Your own existing BI Application from export bunder (.jar file)** option, and enter the **Path** of the `Argus Analytics ssi.bar` file.

2. To modify the Connection Pool Settings:

   a. From the following path, `<MiddlewareHome>\user_projects\domains\bi\bitools\bin`, right click the `admintool.cmd` file, and click **Run as Administrator**.

      The Oracle Analytics Administration Tool opens.

      > **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 Oracle Analytics Server client is installed, and open the RPD.

   b. To open the RPD, select the online mode, and enter the Oracle WebLogic Server 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 Oracle Analytics Server 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 Analytics components, login to Oracle Analytics Server Analytics (`http://oasser.com:port/analytics`) with WebLogic user credentials.

5. Go to **Security** > **Administration** > **Manage Privileges**.

   For a list of privileges assigned to the Oracle Analytics Application roles, refer to Oracle Analytics Server Default Application Roles.

6. Go to Catalog, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)

7. Create Oracle Analytics Server Groups and Users. (See Create Users and Groups in Oracle Analytics Server)

Configure Oracle Analytics Server Repository and Web Catalog Manually

1. Copy the RPD, and Catalog files from `<Argus Analytics Home>\report\opva.rpd and report\catalog\opva.zip folders` to a machine where the Oracle Analytics Server 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:

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

For example,
datamodel.cmd uploadrpd -I C:\temp\opva.rpd -W opva1234 -U <username> -P
<password> -SI ssi
```

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

7. Login to the Oracle Enterprise Manager with the WebLogic credentials.
8. Click **Target Navigation**.

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

   The Oracle Analytics 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 Oracle Argus Analytics catalog **opva.zip** into a local folder, and navigate to `\opva\root\shared` folder.
    a. Copy the following folders and files:
       - current
       - current.atr
       - personal+user
       - personal+user.atr
       - retrospective
       - retrospective.atr

   b. Paste in `<Oracle_Home>\user_projects\domains\bi\bidata\service_instances\ssi\metadata\content\catalog\root\shared` folder.

13. Go to Oracle 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 Create Users and Groups in Oracle Analytics Server.)

16. Create Roles and policies manually in Enterprise Manager. (See Create Roles and Policies with Oracle Fusion Middleware Control.)

17. To view and administer privileges for the Oracle Analytics components, login to Oracle Analytics Server Analytics (`http://oasser.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 Oracle Analytics Server Default Application Roles.

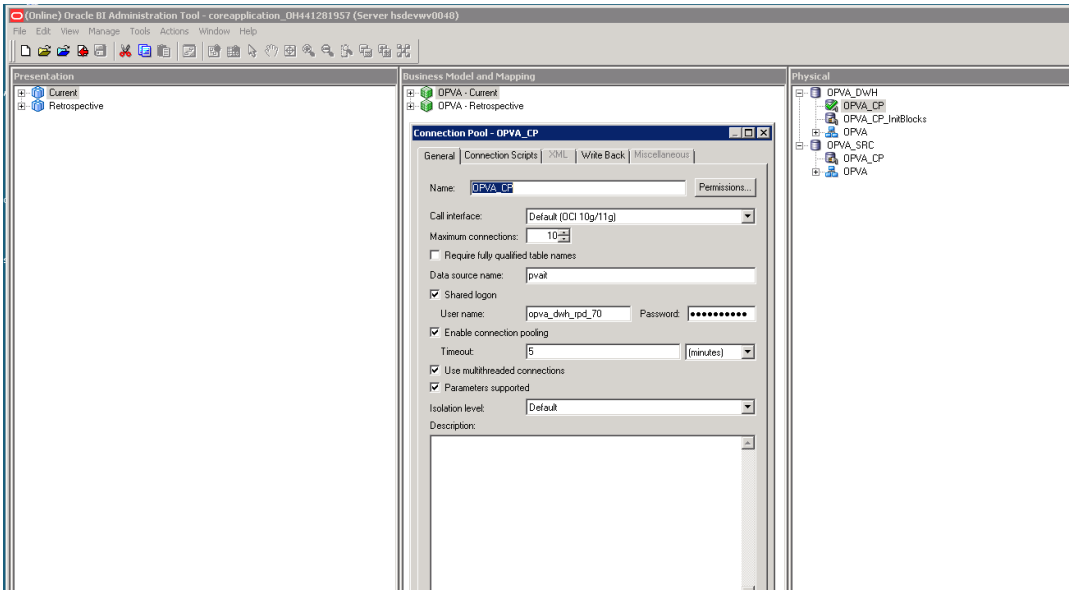
19. Go to Catalog, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)

Post-deployment of the Oracle Argus Analytics RPD

The Oracle Argus Analytics RPD Screen

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 Deploy Oracle Analytics Server Repository and Catalog, as mentioned in the **Note** before Step 1.
2. User: weblogic
3. Password: Password for the user mentioned above



Change the Connection Pool Settings

Once the Oracle 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 Oracle Argus Analytics DWH RPD Schema <AN_DWH_RPD>, created during installation, on the Oracle Argus Analytics DB Instance.
2. Data Source Name: TNS name entry for Oracle Argus Analytics DB Instance.
3. User Name: <AN_DWH_RPD> [the schema name specified for the Oracle Argus Analytics 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 Oracle Argus Safety Source RPD schema <AN_SRC_RPD>, created during installation, on the Oracle Argus Safety Instance.
6. Data Source Name: TNS name entry for Oracle Argus Safety DB Instance.
7. User Name: <AN_SRC_RPD> [the schema name specified for the Oracle Argus Analytics Source RPD schema during installation].
8. Password: The password specified for the <AN_SRC_RPD> schema.
9. Save the RPD.

Create Users and Groups in Oracle Analytics Server

In this section:

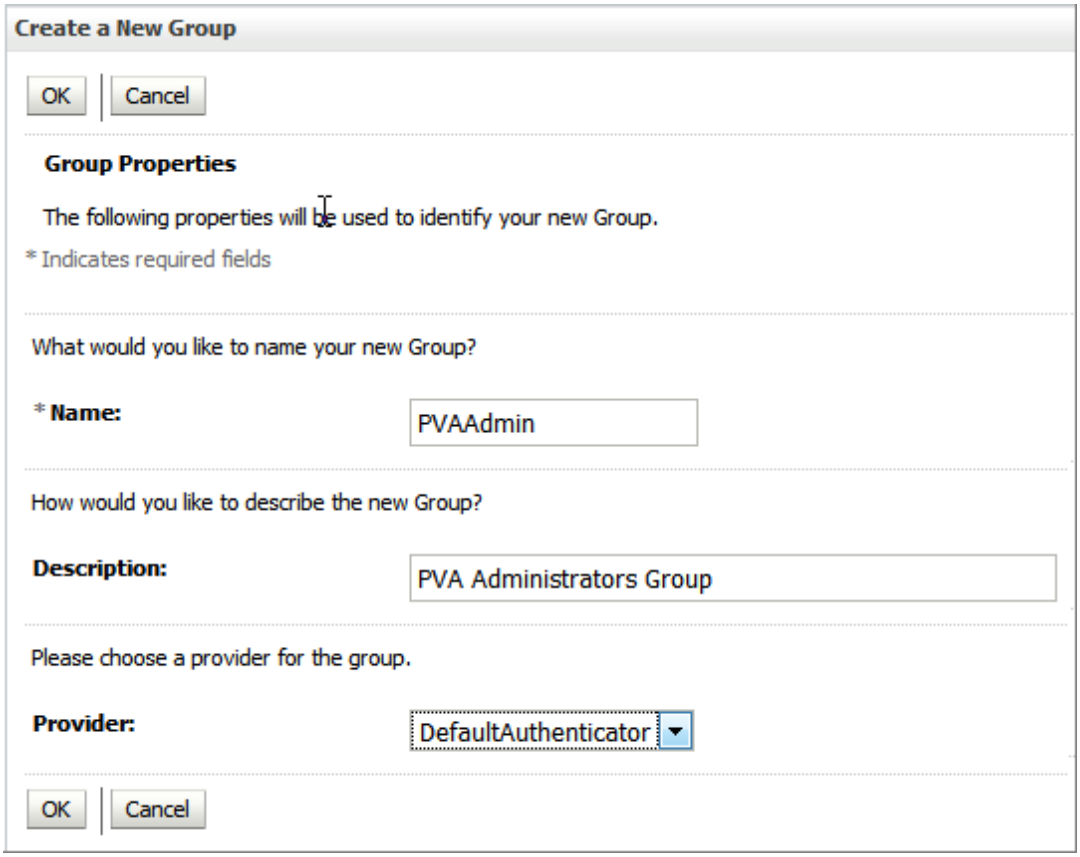
- Create groups in Oracle Fusion Middleware Control
- Create users in the Oracle Fusion Middleware Control

Create groups in Oracle Fusion Middleware Control

1. Open the Oracle WebLogic Server 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.

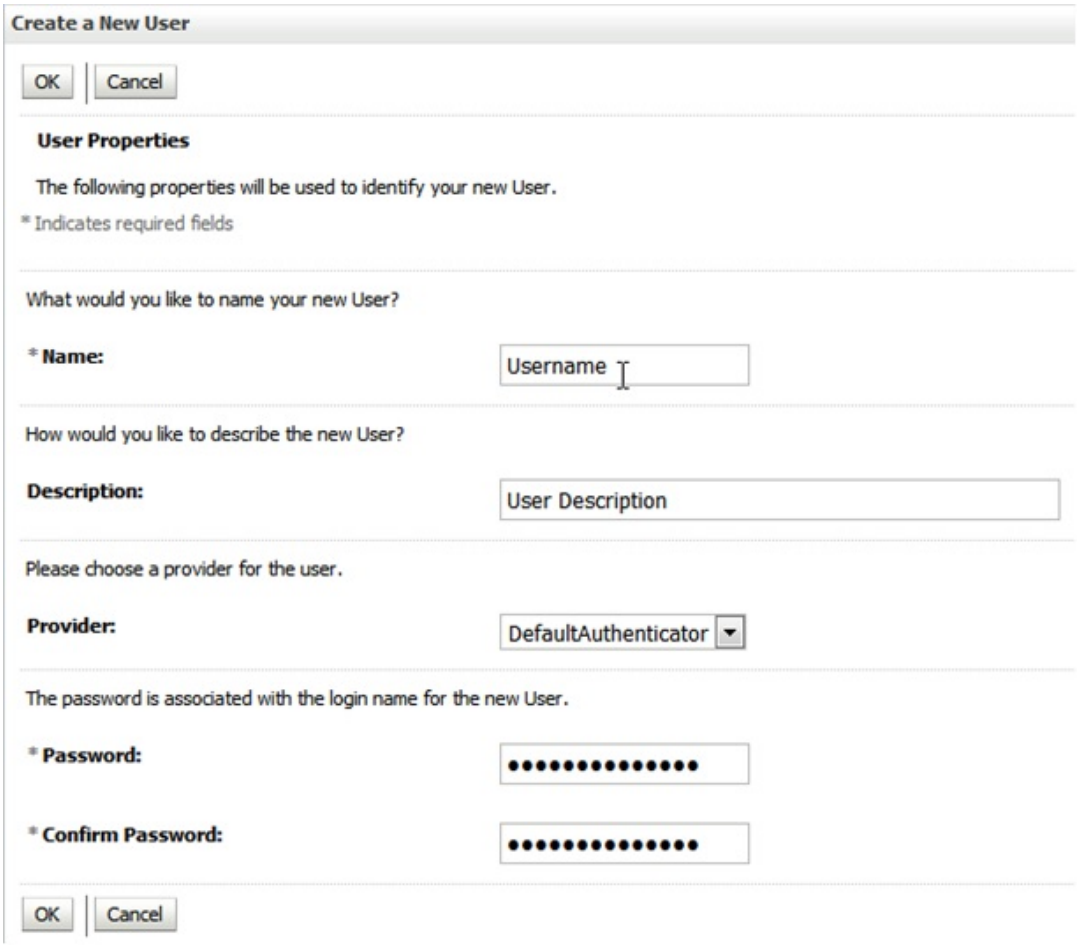
4. Create the following groups by entering the **Name** and **Description**, and click **OK.**
   - PVAAdmin
   - PVASafetyGroup
   - PVASafetyConsumersGroup



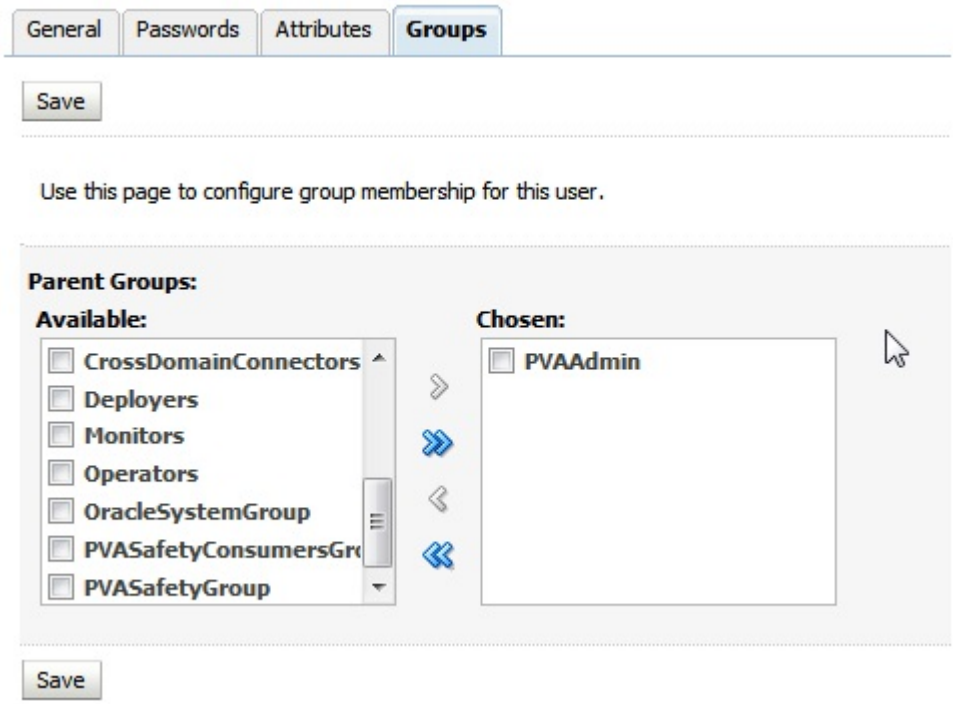
Create users in the Oracle Fusion Middleware Control

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

   The Create a New User dialog box appears



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



Create Roles and Policies with Oracle Fusion Middleware Control

> **Note:**
>
> This section is applicable only when you manually upload the RPD file and Catalog. For more details, refer to Configure Oracle Analytics Server Repository and Webcatalog

For more information, see:

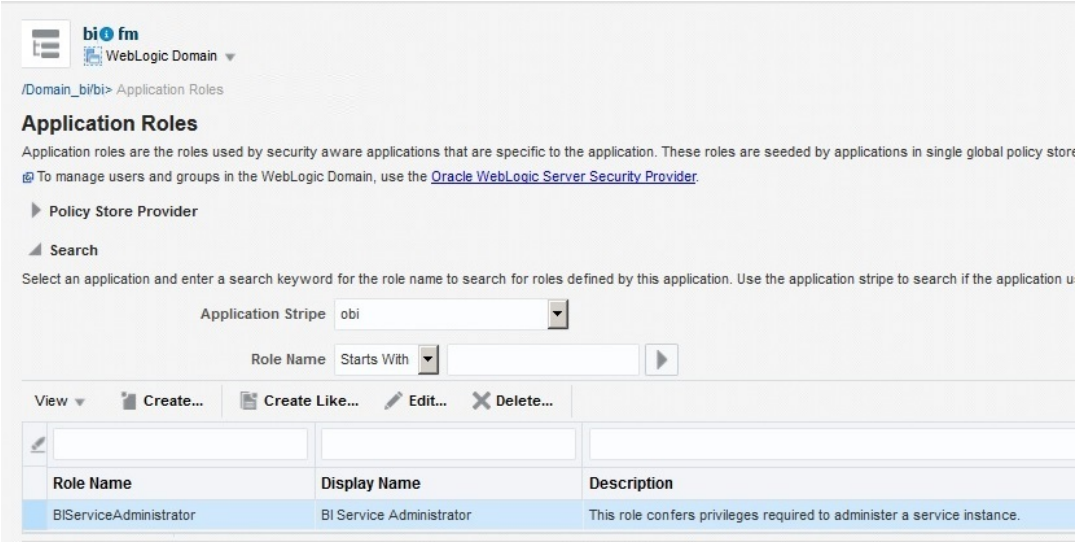
- Create new application roles
- Create new application policy

Create new application roles

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

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

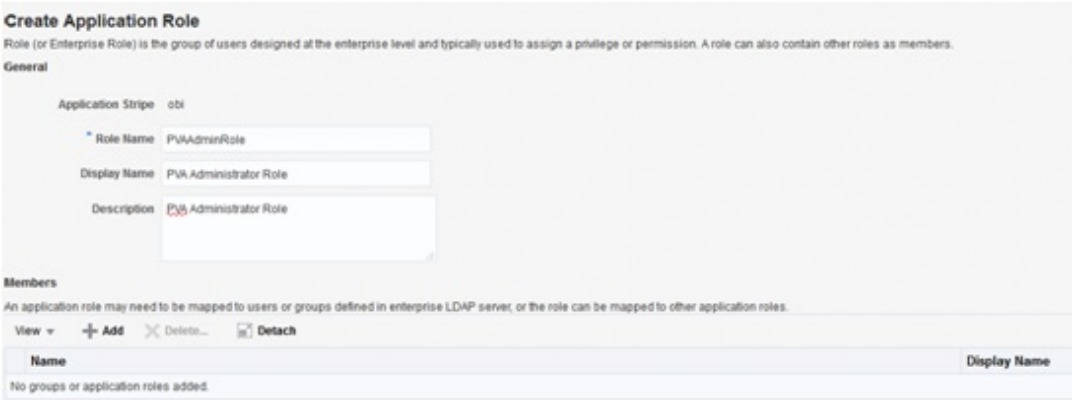
   The default role available in clean slate installation appears.



4. Click **Create**.

   The Create Application Role dialog box appears.

5. In the **Role Name** field, enter **PVAAdminRole**.



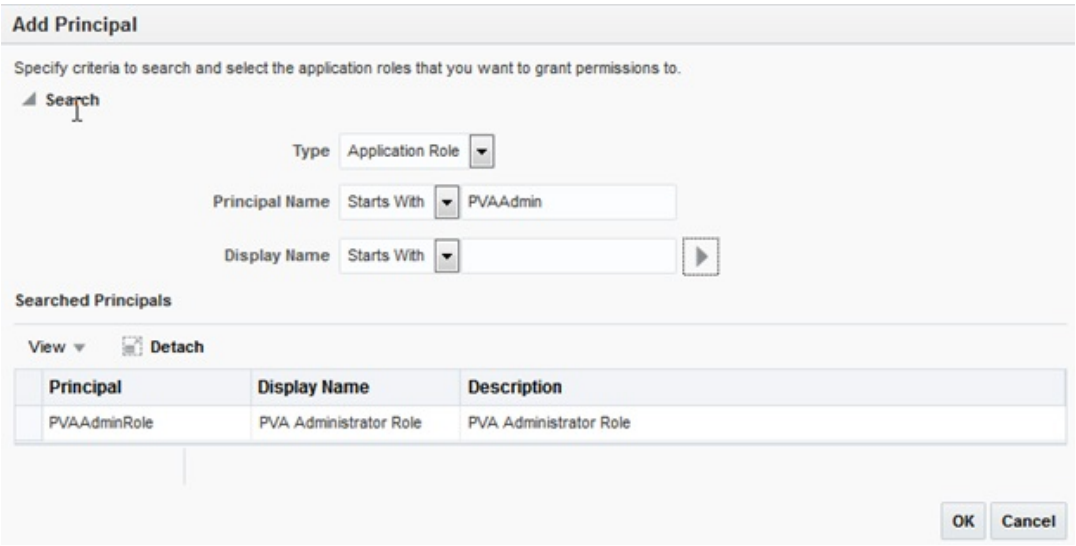
6. From the Members section, click **+Add**.

   The Add Principal dialog box appears.

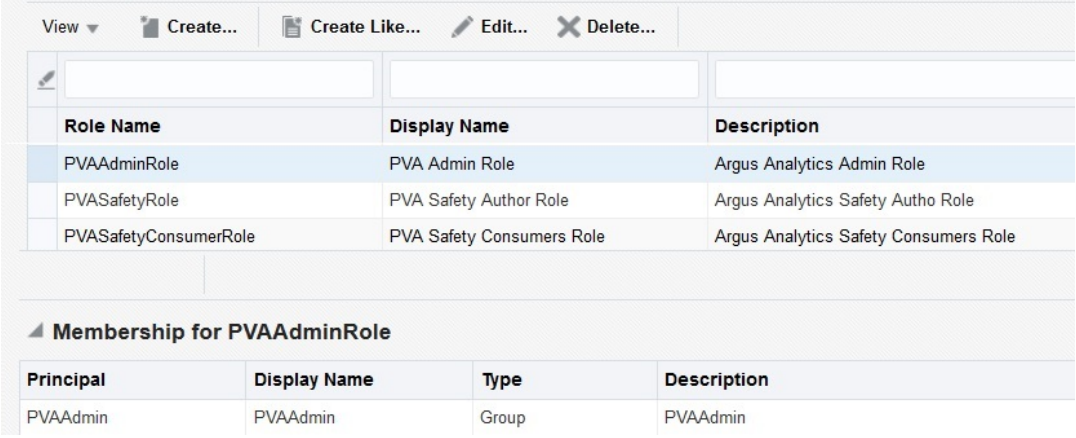
7. From the **Type** drop-down list, select **Group**, and click **Search**.

   A list of principals appears.

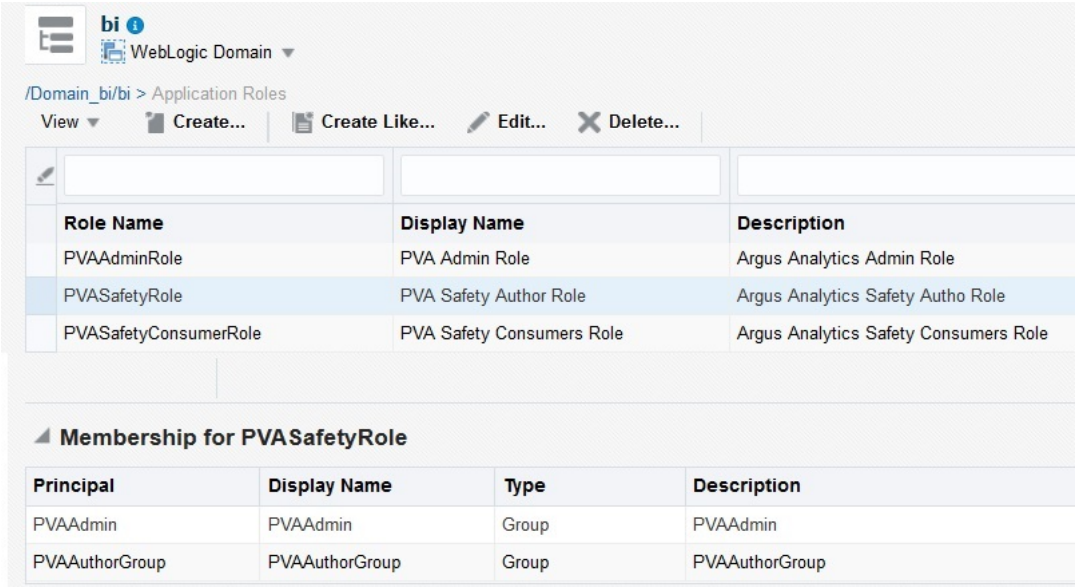
8. From the list of Searched Principals, select **PVAAdmin**, and click **OK**.



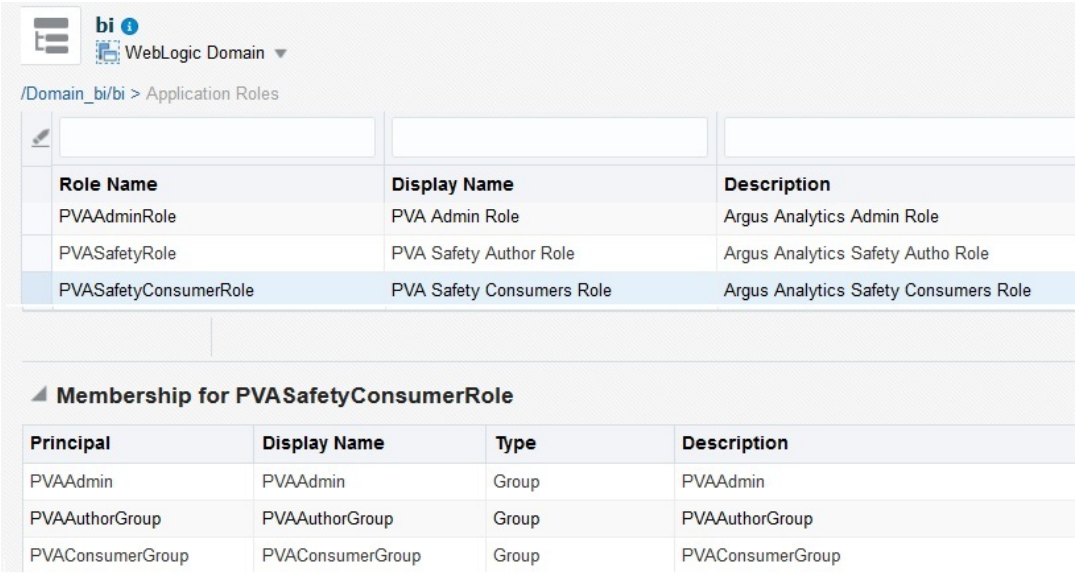
The Membership for **PVAAdminRole** appears as below:



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



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



> **Note:**
>
> For more details, refer to *Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition.*

Create new application policy

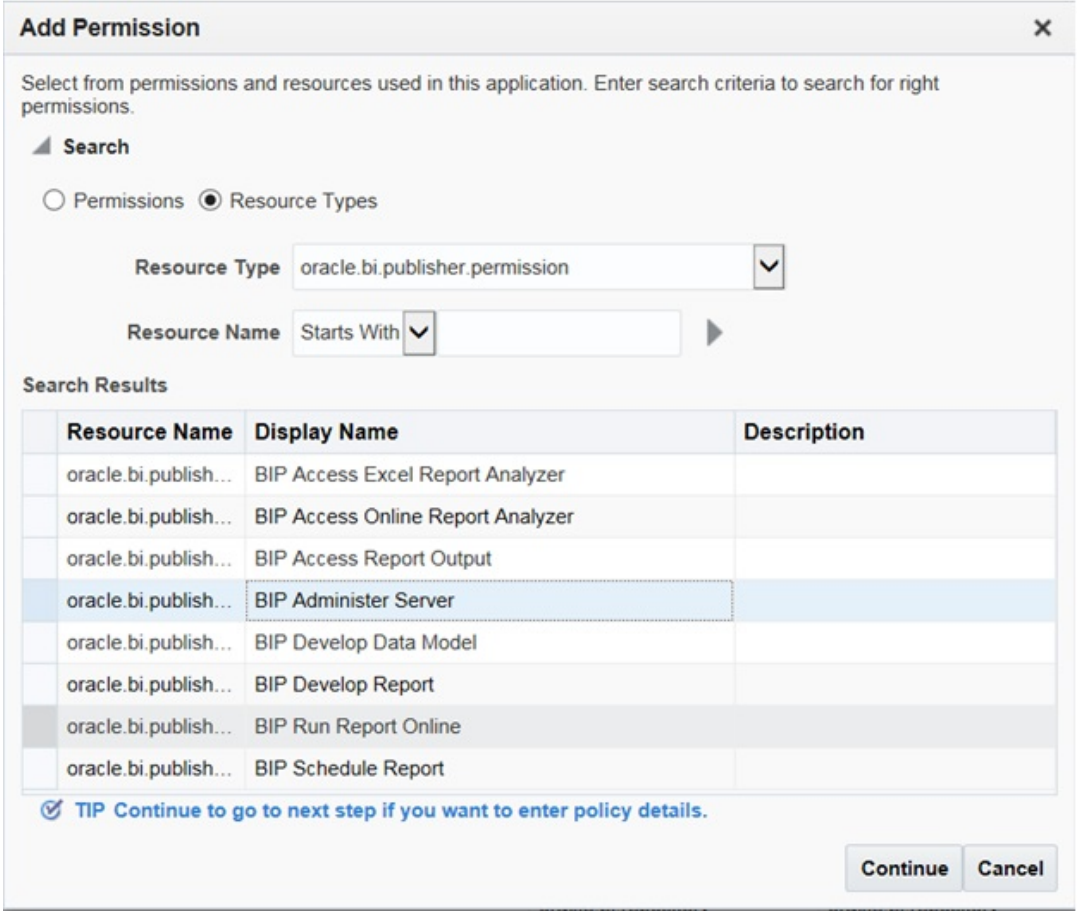
1. Login to Oracle Fusion Middleware Control Oracle Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Policies**.

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

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

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

   The Add Permission dialog box appears.



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

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

Policy Name/ Principal	Resource Type	Resource Name	Permission Actions
PVAAdminRole	oracle.bi.catalog	*	manage
PVAAdminRole	oracle.bi.repository	oracle.bi.repository	manage
PVAAdminRole	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
PVAAdminRole	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
PVAAdminRole	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanager.permission	_all_
PVAAdminRole	oracle.bi.delivers.job	oracle.bi.delivers.job	manage

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

Note:

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

Oracle Analytics Server Catalog Folder-level Permissions

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

   The Permissions dialog box appears.

2. Set the Permissions as follows:

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

a. Select **Apply Permissions** to sub-folders.
b. Select **Permissions** to items within folder.
c. Click **OK**.

3. For each of the following folders, set the account permissions:
   - **Shared Folders** > **Shared Folder** > **Current** > **Permissions**
   - **Shared Folders** > **Shared Folder** > **Personal User** > **Permissions**
   - **Shared Folders** > **Shared Folder** > **Retrospective** > **Permissions**

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

a. Select **Apply Permissions** to sub-folders.
b. Select **Permissions** to items within folder.
c. Click **OK**.

Oracle Analytics Server Default Application Roles

To view and administer privileges of Oracle Analytics components:

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

> **Note:**
>
> Create these privileges only when you manually upload the RPD and Catalog.
>
> You do not need to create these privileges when you import the BAR file.
>
> You must NOT remove the privileges already present in the Manage Privileges tab for the various components. The below mentioned default role grants should only be appended to the existing grants in Oracle Analytics Server components.

Component	Privilege	Default Role Granted
Access	Access to Dashboards	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Answers	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to Oracle Analytics Composer	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to Delivers	PVA Safety Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Access	Access to Briefing Books	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Mobile	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Administration	PVA Admin Role, Oracle Analytics Service Administrator
Access	Access to Segments	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Segment Trees	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to List Formats	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to Metadata Dictionary	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to Oracle Analytics for Microsoft Office	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Oracle Analytics Client Installer	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Catalog Preview Pane UI	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to Export	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Access	Access to KPI Builder	PVA Safety Author Role, Oracle Analytics Service Administrator
Access	Access to Scorecard	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Actions	Create Navigate Actions	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Actions	Create Invoke Actions	PVA Safety Author Role, Oracle Analytics Service Administrator
Actions	Save Actions containing embedded HTML	PVA Admin Role, Oracle Analytics Service Administrator
Admin: Catalog	Change Permissions	PVA Safety Author Role, Oracle Analytics Service Administrator
Admin: Catalog	Toggle Maintenance Mode	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Sessions	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Create Dashboards	PVA Safety Author Role, Oracle Analytics Service Administrator
Admin: General	See sessions IDs	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Change Log Configuration	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Issue SQL Directly	PVA Admin Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Admin: General	View System Information	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Performance Monitor	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Agent Sessions	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Device Types	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Map Data	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	See privileged errors	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	See SQL issued in errors	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Admin: General	Manage Global Variables	PVA Admin Role, Oracle Analytics Service Administrator
Admin: General	Diagnose Oracle Analytics Server Query	Denied: Authenticated User
Admin: General	Manage Marketing Jobs	PVA Safety Author Role, Oracle Analytics Service Administrator
Admin: General	Manage Marketing Defaults	PVA Admin Role, Oracle Analytics Service Administrator
Admin: Security	Manage Catalog Accounts	PVA Admin Role, Oracle Analytics Service Administrator
Admin: Security	Manage Privileges	PVA Admin Role, Oracle Analytics Service Administrator
Admin: Security	Set Ownership of Catalog Objects	PVA Admin Role, Oracle Analytics Service Administrator
Admin: Security	User Population - Can List Users	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
Admin: Security	User Population - Can List Catalog Groups	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
Admin: Security	User Population - Can List Application Roles	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
Admin: Security	Access to Permissions Dialog	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Briefing Book	Add To or Edit a Briefing Book	PVA Safety Author Role, Oracle Analytics Service Administrator
Briefing Book	Download Briefing Book	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Briefing Book	Add to Snapshot Briefing Book	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Catalog	Personal Storage (My Folders and My Dashboard)	PVASafetyConsumerRole, Oracle Analytics Service Administrator

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

Component	Privilege	Default Role Granted
Home and Header	New Menu	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	Help Menu	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	Dashboards Menu	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	Favorites Menu	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	My Account Link	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	Custom Links	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Data Loader	Denied: Authenticated User
My Account	Access to My Account	PVASafetyConsumerRole, Oracle Analytics Service Administrator
My Account	Change Preferences	PVASafetyConsumerRole, Oracle Analytics Service Administrator
My Account	Change Delivery Options	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Answers	Create Views	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Create Prompts	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Access Advanced Tab	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Edit Column Formulas	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Save Content with HTML Markup	PVA Admin Role, Oracle Analytics Service Administrator
Answers	Enter XML and Logical SQL	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Edit Direct Database Analysis	PVA Admin Role, Oracle Analytics Service Administrator
Answers	Create Analysis From Simple SQL	PVA Admin Role, Oracle Analytics Service Administrator
Answers	Create Advanced Filters and Set Operations	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Save Filters	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Save Column	PVA Safety Author Role, Oracle Analytics Service Administrator
Answers	Add EVALUATE_PREDICATE Function	PVA Safety Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Answers	Execute Direct Database Analysis	PVA Admin Role, Oracle Analytics Service Administrator
Answers	Upload Images	PVA Safety Author Role, Oracle Analytics Service Administrator
Delivers	Create Agents	PVA Safety Author Role, Oracle Analytics Service Administrator
Delivers	Publish Agents for Subscription	PVA Safety Author Role, Oracle Analytics Service Administrator
Delivers	Deliver Agents to Specific or Dynamically Determined Users	PVA Admin Role, Oracle Analytics Service Administrator
Delivers	Chain Agents	PVA Safety Author Role, Oracle Analytics Service Administrator
Delivers	Modify Current Subscriptions for Agents	PVA Admin Role, Oracle Analytics Service Administrator
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Scorecard	Create/Edit Scorecards	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	View Scorecards	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Scorecard	Create/Edit Objectives	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Create/Edit Initiatives	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Create Views	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Create/Edit Causes And Effects Linkages	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Create/Edit Perspectives	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Add Annotations	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Scorecard	Override Status	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Scorecard	Create/Edit KPIs	PVA Safety Author Role, Oracle Analytics Service Administrator
Scorecard	Write Back to Database for KPI	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Scorecard	Add Scorecard Views To Dashboards	PVASafetyConsumerRole, Oracle Analytics Service Administrator
List Formats	Create List Formats	PVA Safety Author Role, Oracle Analytics Service Administrator
List Formats	Create Headers and Footers	PVA Safety Author Role, Oracle Analytics Service Administrator
List Formats	Access Options Tab	PVA Safety Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
List Formats	Add/Remove List Format Columns	PVA Admin Role, Oracle Analytics Service Administrator
Segmentation	Create Segments	PVA Safety Author Role, Oracle Analytics Service Administrator
Segmentation	Create Segment Trees	PVA Safety Author Role, Oracle Analytics Service Administrator
Segmentation	Create/Purge Saved Result Sets	PVA Admin Role, Oracle Analytics Service Administrator
Segmentation	Access Segment Advanced Options Tab	PVA Admin Role, Oracle Analytics Service Administrator
Segmentation	Access Segment Tree Advanced Options Tab	PVA Admin Role, Oracle Analytics Service Administrator
Segmentation	Change Target Levels within Segment Designer	PVA Safety Author Role, Oracle Analytics Service Administrator
Mobile	Enable Local Content	PVASafetyConsumerRole, Oracle Analytics Service Administrator
Mobile	Enable Search	PVASafetyConsumerRole, Oracle Analytics Service Administrator
SOAP	Access SOAP	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Impersonate as system user	Oracle Analytics System
SOAP	Access MetadataService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ScorecardAssessmentService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access MsgdbService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ReportEditingService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access KPIAssessmentService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ConditionEvaluationService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access SecurityService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access Tenant Information	Oracle Analytics System
SOAP	Access SchedulerService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System

Component	Privilege	Default Role Granted
SOAP	Access DashboardService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ScorecardMetadataService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access JobManagementService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access CatalogIndexingService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access UserPersonalizationService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access AnalysisExportViewsService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator
SOAP	Access CatalogService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access AdministrationSOAPService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access HtmlViewService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access XmlGenerationService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access IBotService Service	PVASafetyConsumerRole, Oracle Analytics Service Administrator, Oracle Analytics System
Subject Area: "Current"	Access within Oracle Analytics Answers	PVA Admin Role, Oracle Analytics Service Administrator
Subject Area: "Retrospective"	Access within Oracle Analytics Answers	PVA Admin Role, Oracle Analytics Service Administrator
View Canvas	Add/Edit Canvas View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Column Selector	Add/Edit Column Selector View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Compound Layout	Add/Edit Compound Layout View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Contribution Wheel	Add/Edit Contribution Wheel View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Graph	Add/Edit Graph View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Funnel	Add/Edit Funnel View	PVA Safety Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
View Gauge	Add/Edit Gauge View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Micro Chart	Add/Edit Micro Chart View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Filters	Add/Edit Filters View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Dashboard Prompt	Add/Edit Dashboard Prompt View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Performance Tile	Add/Edit Performance Tile View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Heat Matrix	Add/Edit Heat Matrix View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Static Text	Add/Edit Static Text View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Javascript view	Edit Javascript View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Legend	Add/Edit Legend View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Map	Add/Edit Map View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Narrative	Add/Edit Narrative View	PVA Safety Author Role, Oracle Analytics Service Administrator
View No Results	Add/Edit No Results View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Pivot Table	Add/Edit Pivot Table View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Generic Plugin View	Add/Edit Generic Plugin View View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Report Prompt	Add/Edit Report Prompt View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Create Segment	Add/Edit Create Segment View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Selection Steps	Add/Edit Selection Steps View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Logical SQL	Add/Edit Logical SQL View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Table	Add/Edit Table View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Create Target List	Add/Edit Create Target List View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Ticker	Add/Edit Ticker View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Title	Add/Edit Title View	PVA Safety Author Role, Oracle Analytics Service Administrator
View Treemap	Add/Edit Treemap View	PVA Safety Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
View Trellis	Add/Edit Trellis View	PVA Safety Author Role, Oracle Analytics Service Administrator
View View Selector	Add/Edit View Selector View	PVA Safety Author Role, Oracle Analytics Service Administrator
Write Back	Manage Write Back	PVA Admin Role, Oracle Analytics Service Administrator
Write Back	Write Back to Database	Denied: Authenticated User

Change the Oracle Analytics Server RPD Password

To change the password for Oracle Analytics Server RPD, execute the following steps:

1. Open the Oracle Analytics Administrator Tool and open `<ARGUS_ANALYTICS_HOME>\report\opva.rpd` in **Offline** mode.
2. Select **File** > **Change Password.**
3. Enter the password set in Deploy Oracle Analytics Server 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.

5

Configure Oracle Analytics Server Help Files

> **Note:**
>
> If the Oracle Analytics Server is not the same machine where the installer is run, then copy the opva_help.zip file into the machine where Oracle Analytics Server is installed.

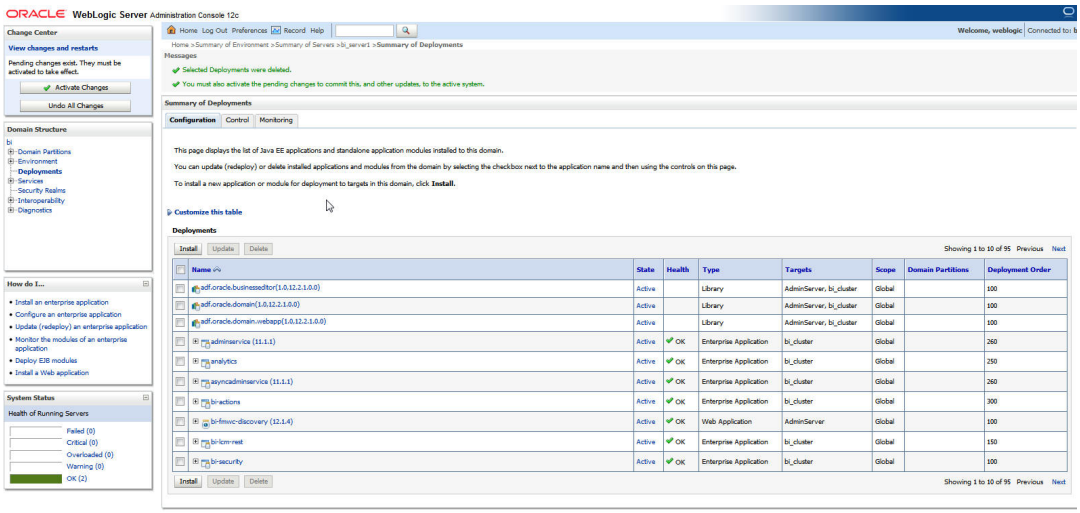
For more information, see:

- Configure the Help links in the Dashboards and Reports

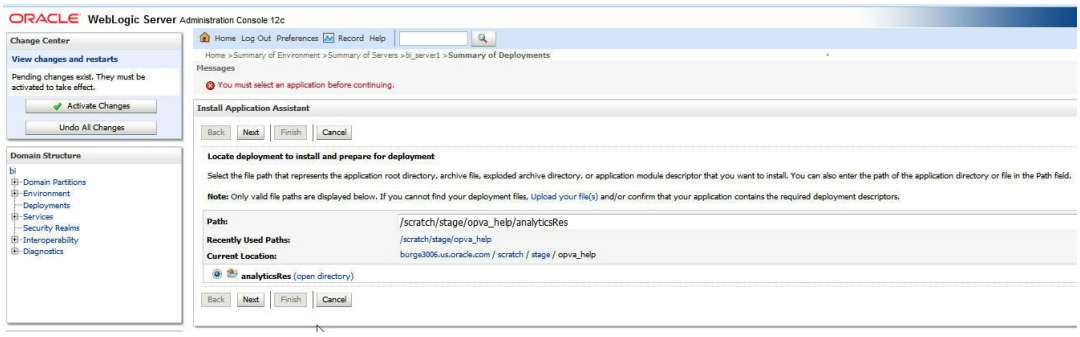
Configure the Help links in the Dashboards and Reports

1. Extract the contents of the `opva_help.zip` file at any location on the Oracle Analytics Server. For example: `/scratch/stage/opva_help`

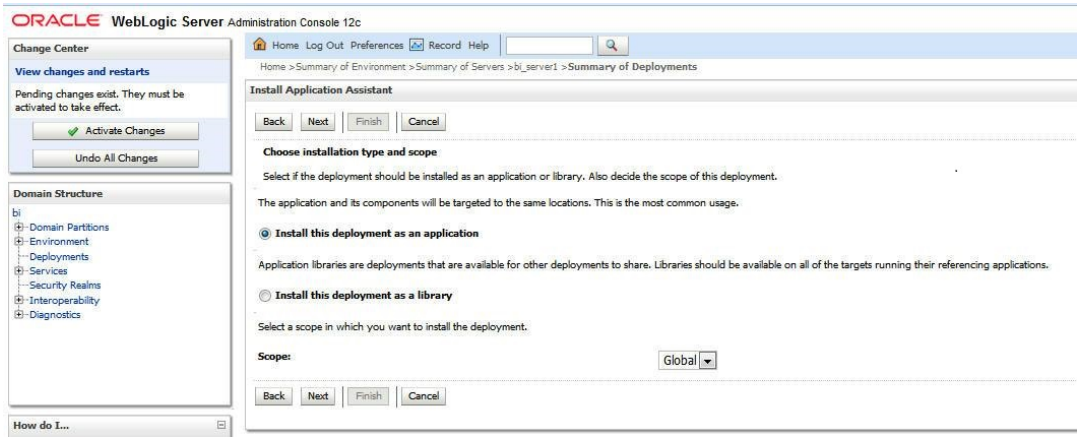
   The `opva_help` folder contains `analyticsRes` folder.
2. Log in to the Oracle WebLogic Server.
3. Navigate to **Deployments**.
4. Click **Lock & Edit** in the left pane to enable the **Install** button.



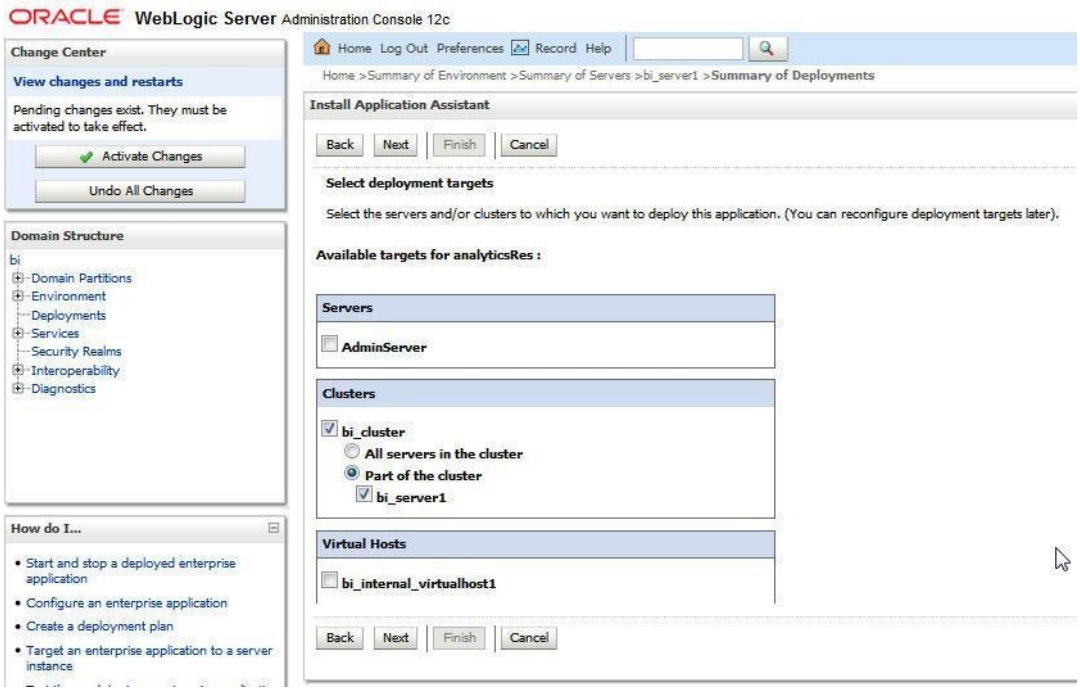
5. Click **Install**, and navigate to the location where `opva_help.zip` was extracted in Step 1.
6. Select **analyticsRes**, and click **Next**.



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



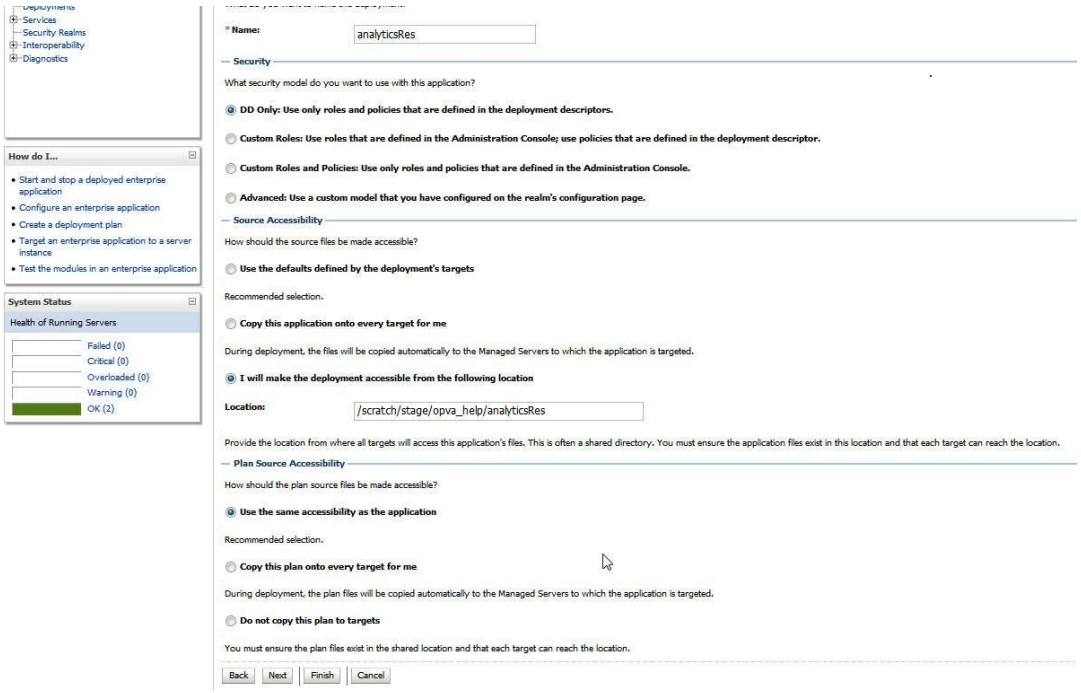
8. Select **Deployment targets**, choose **bi_server1**, and click **Next**.



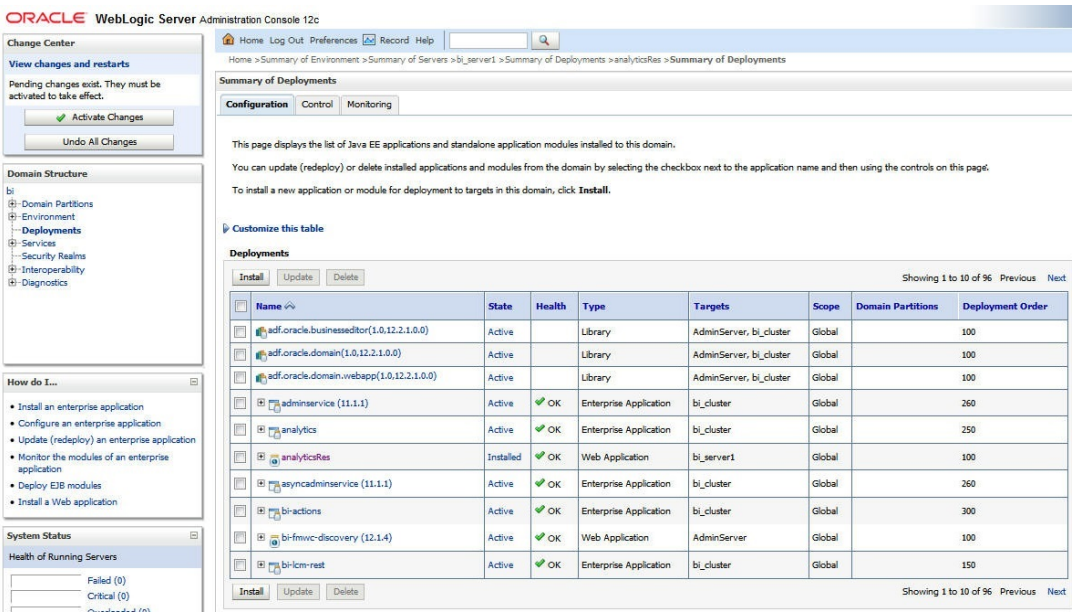
9. Under **Source accessibility:**

Select **I will make the deployment accessible from the following location** option, and select the path for analyticsRes as selected in step 6. For example: `/scratch/stage/opva_help/analyticsRes`

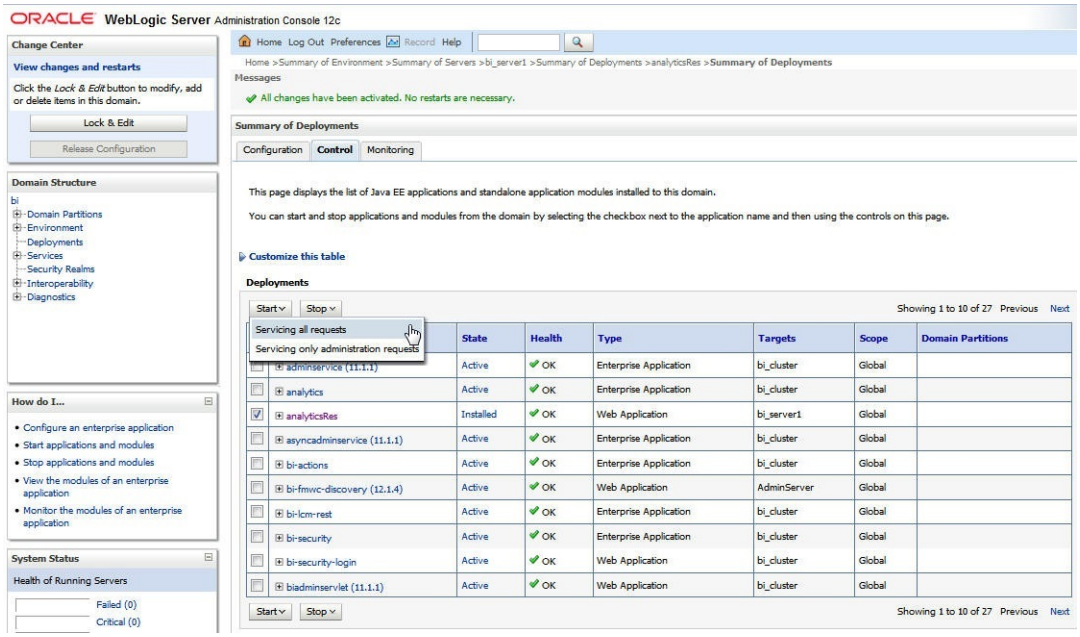
10. Click **Finish**.



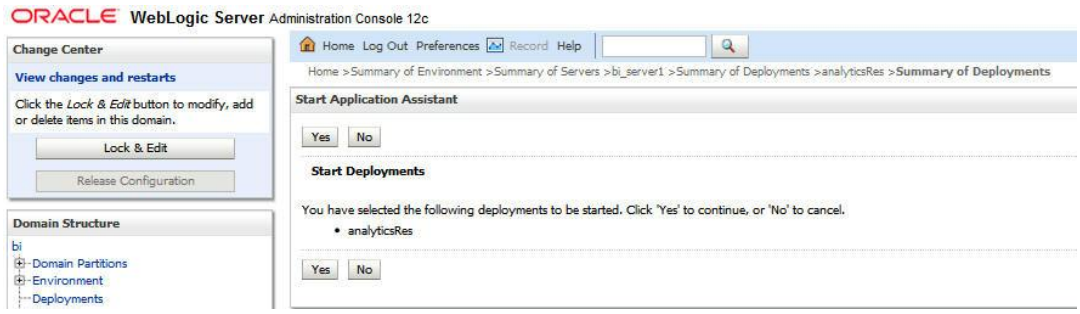
The **analyticsRes** appears under Deployments.



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



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



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

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

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

6

Configure SSO using the Oracle Access Manager 12c

In this chapter:

- Prerequisites
- Install SSO on Oracle Access Manager 12c

Prerequisites

- There must be an Oracle Access Manager 12c 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 Oracle Argus Safety with the same credentials (login information).
- Oracle Webgate 12c must be installed on the same server where the Oracle Analytics Server is installed, as mentioned above.

Install SSO on Oracle Access Manager 12c

1. Navigate to the Oracle Access Manager 12c Oracle Access Manager Console URL (http://oam_server:port/oamconsole) and login with the Oracle Access Manager Admin credentials.
2. Click **Agents**.
3. On the **SSO Agents** tab, click the **Create Webgate** button and enter the following details:
   - **Name**: ArgusAnalyticsPolicy
   - **Security**: Open
   - **Host Identifier**: <oas_server>
   - **Auto Create Policies**: Checked

   > **Note:**
   >
   > The <oas_server> refers to the server where the Oracle Analytics Server is installed along with Oracle Web Tier and Oracle Webgate.

4. Click **Apply** to save the changes.
5. On the subsequent page, update the details for the **ArgusAnalyticsPolicy** created in the above step:
   - **Cache Pragma Header**: Private
   - **Cache Control Header**: Private
6. Click **Apply**.

7. Navigate to the **Application Security** > **Host identifiers**.
8. Search for **ArgusAnalyticsPolicy**, click the **Search Results** tab, and add the following details:
   - <oas_server>
   - <oas_server> <port>
   - <oas_server_ip>
   - <oas_server_ip> <port>

   > **Note:**
   >
   > <oas_server> refers to the server where the Oracle Analytics Server is installed along with Oracle Web Tier and Oracle Webgate. The port refers to the Oracle Web Tier Port.

   Example:

Hostname	Port
oas_server.oracle.com	--
oas_server.oracle.com	7777
<ip address>	--
<ip address>	7777

9. Navigate to **Application Security** > **Access Manager** > **Application Domains**.
10. Search for **ArgusAnalyticsPolicy**, and click **Search Results**.
11. Ensure that the Authentication Scheme is set as **LDAPScheme**.
12. Ensure that the following resources are present:
    - /
    - /…/*
13. Add the following Response variables:
    - **Name**: OAM_REMOTE_USER
    - **Type**: Header
    - **Value**: $user.attr.uid [based on the LDAP schema setup]
14. Click **Apply** and save the changes.
15. Expand and double-click **Application Domains** > **ArgusAnalyticsPolicy** > **Authorization Policies** > **Protected Resource Policy**.
16. Ensure that the following resources are present:
    - /
    - /…/*
17. Add the following Response variables:
    - **Name**: OAM_REMOTE_USER
    - **Type**: Header

- **Value**: $user.attr.uid [as based on the LDAP schema setup]

18. Click **Apply** to save the changes
19. Navigate to the OPVA Web Tier Machine [<oas_server>], which is the machine where you have installed the OPVA Oracle Analytics Server, and run the installer for Webgate (OFM Webgate 12c for Oracle Access Manager 12c) to complete the installation.
20. Configure the 12c Webgate using the following steps to communicate with the Oracle Access Manager 12c 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 Oracle Access Manager 12c server.

The 12c Webgate Agent (ArgusAnalyticsPolicy), which was created in the Oracle Access Manager 12c Oracle Access Manager Console earlier, would have also created the following artifacts on the Oracle Access Manager 12c server:

cwallet.sso

ObAccessClient.xml

This is based on the Security Mode that you have configured, which in this case is **Open**.

On the Oracle Access Manager 12c server, these files are present at the following location:

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

Copy these files to the <oas_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
```

21. Configure the HTTP Server as a reverse proxy for the WebLogic Server. To execute this, modify the **mod_wl_ohs.conf** file present at the following location: `OracleWebTierHome\instances\instance2\config\OHS\ohs1`

The following is a template to configure **mod_weblogic**:

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

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

<IfModule weblogic_module>

WebLogicHost <WEBLOGIC_HOST>

WebLogicPort <WEBLOGIC_PORT>

Debug ON

WLLogFile /tmp/weblogic.log

MatchExpression *.jsp

<Location /console>

SetHandler weblogic-handler

WebLogicHost hsdevwv0096.oracle.com

WeblogicPort 7001

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

<Location /em>

SetHandler weblogic-handler

WebLogicHost hsdevwv0096.oracle.com

WeblogicPort 7001

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

<Location /analytics>

SetHandler weblogic-handler

WebLogicHost hsdevwv0096.oracle.com

WeblogicPort 9704

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

<Location /analyticsRes>

SetHandler weblogic-handler

WebLogicHost hsdevwv0096.oracle.com

WeblogicPort 9704

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

<Location /xmlpserver>

SetHandler weblogic-handler

WebLogicHost hsdevwv0096.oracle.com

WeblogicPort 9704

WLProxySSL ON

WLProxySSLPassThrough ON

</Location>

</IfModule>

<Location /weblogic>

SetHandler weblogic-handler

PathTrim /weblogic

ErrorPage http:/WEBLOGIC_HOME:WEBLOGIC_PORT/

</Location>

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

22. Configure a new Authenticator for Oracle WebLogic Server on the Oracle Analytics Server using the following steps:
    a. Login to the WebLogic Server Administrator Console and navigate to **Security Realms**> **myrealm**.
    b. Click the **Providers** tab.
    c. Click **Lock & Edit** on the right corner of the webpage, highlighted as Change Center.
    d. Click **New** to create a new Authentication Provider and add the following details:

       Name: OPVAOIDAuthenticator, or a name of your choice

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

       In the sub tab change the Control Flag as **SUFFICIENT**
    f. Click **Save**.

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

- **Host:** Your LDAP host.

  For example: oid_server.oracle.com
- **Port:** Your LDAP host listening port.

  For example: 3060
- **Principal:** LDAP administrative user.

  For example: cn=orcladmin,cn=Users,dc=us,dc=oracle,dc=com
- **Credential:** LDAP administrative user password
- **User Base DN:** Same searchbase as in Oracle Access Manager.

  For example: cn=Users,dc=us,dc=oracle,dc=com
- **All Users Filter:**

  For example: (&(uid=*) (objectclass=person))
- **User Name Attribute:** Set as the default attribute for username in the directory server.

  For example: uid
- **Group Base DN:** The group searchbase

  For example: cn=Groups,dc=us,dc=oracle,dc=com
- Leave the other defaults as is.
- **GUID Attribute:** The GUID attribute defined in the OID LDAP Server

  For example: uid
- Click **Save**.

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

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

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

Name: OPVAOAMIdentityAsserter, or a name of your choice

Type: OAMIdentityAsserter

c. Click **OK**.

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

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

f. Click **Save**.

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

- **Transport Security:** open
- **Application Domain:** ArgusAnalyticsPolicy, as set in the Oracle Access Manager 12c Console
- **Access Gate Name:** ArgusAnalyticsPolicy, as specified in the Oracle Access Manager 12c Console

- **Primary Access Server:** oam_server.oracle.com:5575, Oracle Access Manager 12c 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

24. 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 Oracle Analytics 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 Oracle Enterprise Manager of Oracle Analytics Server or the Oracle Fusion Middleware Control page and navigate in the tree structure to the **Business Intelligence** > **coreapplication** node.

m. In the Oracle Analytics 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 Oracle 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.

25. Enable the SSO Authentication in the Weblogic Server for Oracle Analytics Server using the following steps:

a. Login to Oracle 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 Analytics components using Oracle Fusion Middleware Control.

7
Enable SSL

In this chapter:

- Enable SSL in Oracle WebLogic Server
- Configure SSL for SSO with Oracle Access Manager 12c
- Enable default SSL Configuration in OAS

Enable SSL in Oracle WebLogic Server

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 Oracle Argus Analytics) To further configure Oracle Analytics 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 Oracle Analytics Server.

   a. Login to Oracle WebLogic Server 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**.

Configure SSL for SSO with Oracle Access Manager 12c

1. Configure Oracle Analytics Server in SSL mode as given in the Enable SSL in Oracle WebLogic Server.
2. Follow the steps as mentioned in the Configure SSO using the Oracle Access Manager 12c, except for the deviations as mentioned here:

   Update/Create the Webgate Registration in Oracle Access Manager 12c, which you have created in the Configure SSO using the Oracle Access Manager 12c.

   > **Note:**
   >
   > The Oracle Access Manager Server configured in Oracle Access Manager 12c must be running with Security set to **Simple**, else it does not let you create a Webgate with Security set as **Simple**.

   a. Open the Oracle Access Manager 12c Oracle Access Manager Console.
   b. Navigate to the **Policy Configuration** tab.
   c. Expand and double-click **Shared Components** > **Resource Type** > **Host Identifiers** > **<oas_server>** (for example, www.example.com) to open the Host Identifiers window and add the following details in addition to the ones that are already present:

      <oas_server>

      <oas_server> <ssl port>

      <oas_server_ip>

      <oas_server_ip> <ssl port>

      > **Note:**
      >
      > **<oas_server>** refers to the server, where the Oracle Analytics Server 12c is installed along with Oracle Web Tier and Oracle Webgate. The <ssl port> refers to the Oracle Web Tier SSL Port.

   d. Click **Apply**.
   e. From the **System Configuration** tab, access the **Manager Settings** section, expand the **SSO Agents** node, and expand **OAM Agents**.
   f. On the **Search** page, define your criteria in the **Name** field as **ArgusAnalyticsPolicy** and click **Search**.
   g. In the Search results, click **ArgusAnalyticsPolicy** to edit the **Agent Registration**.

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

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

j. This generates the artifacts again or afresh. Copy the generated Files (Artifacts) to the Webgate Instance Location from the OAM 12c server.

   The 12c Webgate Agent (ArgusAnalyticsPolicy), which is updated/created in the Oracle Access Manager 12c Oracle Access Manager Console, also creates the following artifacts on the Oracle Access Manager 12c 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 Oracle Access Manager 12c 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 **<oas_server>** in the `<Webgate_Instance_Directory>/webgate/config` directory For example:

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

   Copy the **aaa_cert.pem** and **aaa_key.pem** files to the **<oas_server>** in the `<Webgate_Instance_Directory>/webgate/config/simple` directory. For example:

   ```
   <MW_HOME>/Oracle_WT1/instances/instance2/config/OHS/ohs1/webgate/config/simple
   ```

k. Restart the Oracle Access Manager Server.

3. The Oracle Web Tier is configured with Oracle Analytics Server as a reverse proxy, as mentioned in step 22 of the Configure SSO using the Oracle Access Manager 12c, 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`.

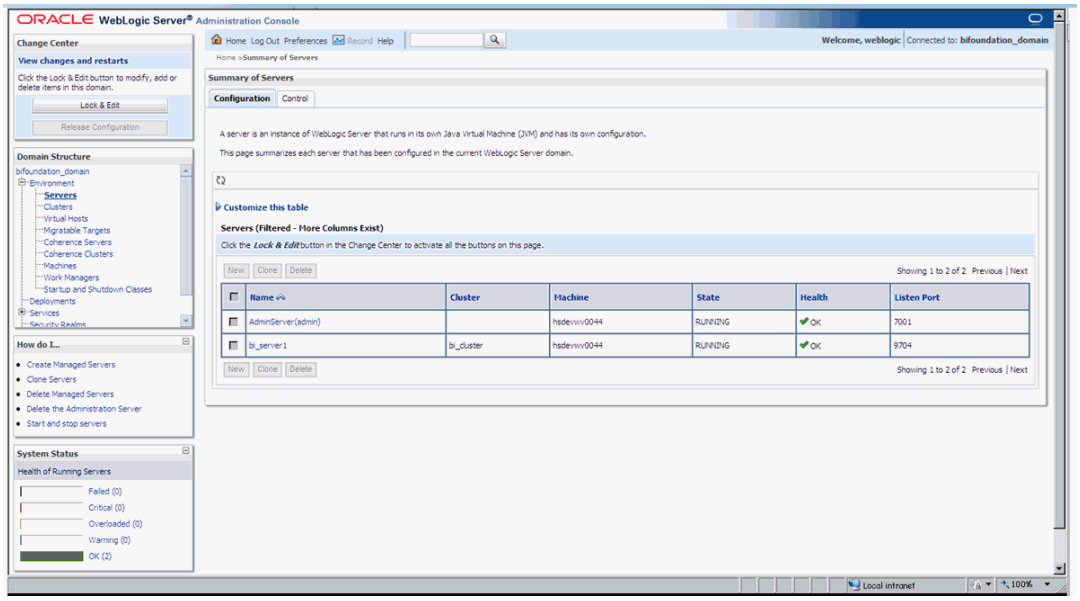
   b. Find the `VirtualHost` section and ensure the following entry is present:

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

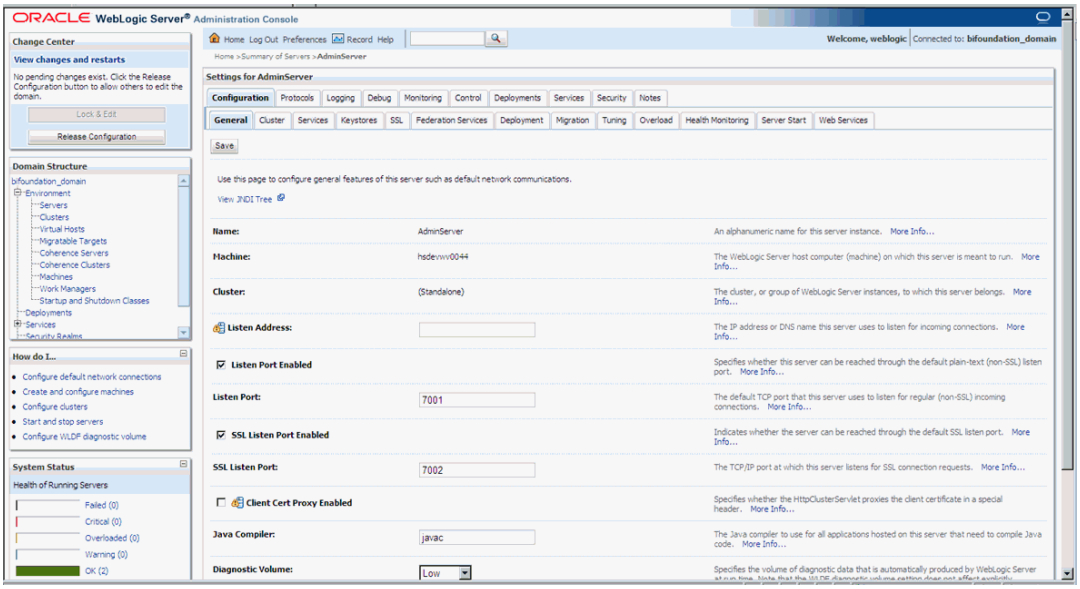
   c. Save the file and restart the HTTP Server.

Enable default SSL Configuration in OAS

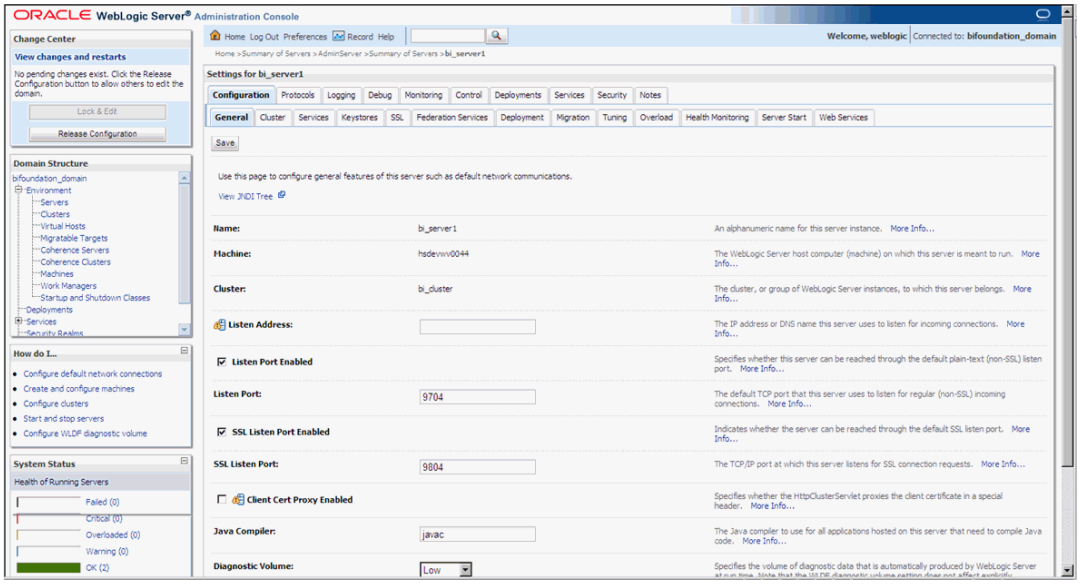
1. Open the Oracle WebLogic Server Administrator console for Oracle Analytics Server.
2. Navigate to **Environment** > **Servers** in the tree view displayed on the left side.



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:



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



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:**
   >
   > Edit the Path names according to your installation directories.

10. Restart all the Managed Oracle Analytics Servers.

   > **Note:**
   >
   > For more detailed information on configuring SSL certificates in Oracle Analytics Server, refer to the guide - *Oracle Fusion Middleware Security Guide for Oracle Analytics Server*.

A

Create ODBC Connection for Oracle Analytics Server Administration Tool

This appendix comprises the steps to create ODBC connection for Oracle Analytics Server Administration tool.

1. Navigate to **Control Pane**l > **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 Oracle Analytics Server DSN Configuration dialog box appears.
5. Enter the following fields:
   a. **Name**—AN_DSN (or any name)
   b. **Description**
   c. **Server**—Oracle Analytics 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 Oracle Analytics Server.

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