Oracle® Argus Insight

Installation Guide

Release 8.1

E68412-01

June 2016

Oracle Argus Insight Installation Guide, Release 8.1

E68412-01

Contents

Preface vii

Audience vii
Documentation Accessibility vii
Finding Information and Patches on My Oracle Support vii
Finding Oracle Documentation ix
Conventions ix

1 Introduction

1.1 Argus Insight Product Overview 1-1
1.1.1 Argus Insight Architecture 1-2
1.2 Software and Hardware Requirements 1-3
1.3 Important Installation Information 1-6
1.3.1 Installation Requirements for the Servers 1-6
1.3.2 Installation Requirements for the Argus Insight Client 1-7
1.3.3 General Installation Notes and Information 1-8

2 Installing Argus Insight

2.1 Before You Install the Argus Insight Application 2-1
2.2 Installing Argus Insight Components onto the Web Server 2-1
2.2.1 Changing the APR_USER Password 2-4
2.3 Enabling SSL Support for the Argus Insight Website 2-5

3 Creating the Argus Insight Data Mart Structure

3.1 Before You Run the Argus Insight Schema Creation Tool 3-1
3.2 Argus Insight Configuration Requirements 3-2
3.2.1 Database Parameters 3-2
3.2.2 Database I/O Configuration 3-3
3.2.3 Recommended Configuration for the Database Server 3-4
3.3 Argus Insight Data Mart Tablespaces 3-4
3.4 Starting the Argus Insight Schema Creation Tool 3-5
3.5 Creating the Database Schema 3-6
3.5.1 Creating Users and Roles in the Argus Safety Database 3-6
3.5.2 Clearing the Cache 3-9
3.5.3 Creating a New Schema for Argus Insight 3-10
3.5.4 Loading Factory Data 3-18

3.6 Validating the Schema ... 3-19
3.7 Creating a Database Link from Argus Safety to Insight Database ... 3-22
3.8 Upgrading Database from Argus Insight 8.0 to Argus Insight 8.1 ... 3-24
3.9 Running Additional Grant Scripts for Single DB Instance ... 3-27
3.10 Creating Argus Insight Read-Only User ... 3-27

4 Configuring the Argus Insight Application

4.1 Logging In to Argus Insight for Configuration and Setup ... 4-1
4.2 Configuring the Argus Insight Application Profile Switches ... 4-2
4.2.1 Accessing and Modifying the Profile Switches ... 4-3
4.2.2 Setting the Populate Data Attributes ... 4-3
4.2.3 Setting the Email Attributes ... 4-4
4.2.4 Setting the Attributes Specific ONLY to Argus Mart ... 4-5
4.2.5 Setting the Attributes Specific ONLY to BIP ... 4-7
4.2.6 Setting the Attributes Specific ONLY to OBIEE ... 4-7
4.2.7 Setting the Attributes Specific ONLY to BusinessObjects ... 4-8
4.2.8 Setting the Attributes Specific ONLY to Cognos ... 4-8
4.3 Configuring Duration Value Bands ... 4-9
4.4 Configuring Derivation Functions ... 4-12
4.4.1 Opening the Derivation Fields Dialog Box ... 4-12
4.4.2 Icons in the Derivation Fields Dialog Box ... 4-13
4.4.3 Field Mapping Derivation Rules ... 4-13
4.4.4 Fields and Check Boxes in the Derivation Fields Dialog Box ... 4-14
4.4.4.1 LM Table ... 4-14
4.4.4.2 Suppress ... 4-14
4.4.4.3 Value ... 4-14
4.4.4.4 Priority ... 4-15
4.4.4.5 SQL ... 4-15
4.5 Configuring the Argus Insight Windows Service ... 4-16
4.6 Configuring the IIS File Download Limit ... 4-16
4.6.1 Configuring the Maximum Requesting Entity Body Limit ... 4-17
4.7 Using Export and Import to Copy Configuration Data ... 4-17
4.7.1 Exporting Data ... 4-18
4.7.2 Importing Data ... 4-19
4.8 Using Argus Safety to Configure Enterprises for Argus Insight ... 4-21
4.9 Securing Sensitive Configuration and Operational Data ... 4-22

5 Extracting, Transforming, and Loading Data

5.1 Prerequisites, Cautions, and Warnings ... 5-1
5.2 Running the Initial ETL ... 5-2
5.2.1 Generating the Balance Logs ... 5-3
5.2.2 Closing the Initial ETL Status Dialog Box ... 5-4
5.2.3 Stopping the Execution of ETL ... 5-4
5.3 Running the Initial ETL Again ... 5-5
5.4 Processing a Failed ETL ... 5-5
5.4.1 Continuing the Failed Initial ETL Process ... 5-6
5.4.2 Ignoring the Failed Initial ETL Process ... 5-7

5.4.3 Modifying the Attributes of ETL Data Exclusion 5-7
5.5 Restarting the Initial ETL Process 5-8

6 Configuring the BIP Environment

6.1 Creating PRMART JDBC Connection 6-1
6.2 Managing Users and Roles: BI Publisher Standalone Installation with BI Publisher Security 6-3
6.2.1 Creating Users and Assigning Roles to Users 6-4
6.2.2 Creating Roles, Adding Data Sources, and Assigning Roles 6-5
6.3 Managing Users and Roles: BI Publisher Standalone Installation with OFM Security 6-7
6.3.1 Creating Users and Assigning Roles to Users 6-7
6.3.2 BI Publisher Standalone Installation in OFM Security 6-8
6.3.2.1 Creating Users and Groups 6-8
6.3.2.2 Creating Roles and Policies 6-10
6.3.3 Creating Roles, Adding Data Sources, and Assigning Roles in WebLogic Enterprise Manager 6-14
6.3.4 Creating Application Policy 6-17
6.3.5 Uploading the Argus Insight.xdrz file to BIP 6-18
6.4 Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model 6-20
6.4.1 Configuring BIP Roles 6-21
6.4.2 Folder Level Permissions 6-22

7 Configuring the BusinessObjects XI Environment

7.1 Checking Requirements 7-1
7.2 Configuring the BusinessObjects Server 7-1
7.3 Configuring the Argus Insight Web Server 7-2

8 Configuring the Cognos 10 Environment

8.1 Setting Up Cognos Server and Configuration for New Installation 8-1
8.1.1 Configuring IIS 7.0 on the Cognos 10 Server 8-1
8.1.1.1 Checking that CGI or ISAPI Is Enabled in IIS 8-2
8.1.1.2 Creating the Cognos 10 Virtual Directories 8-3
8.1.1.3 Editing ISAPI or CGI Extensions 8-4
8.1.1.4 Adding the Module Mapping 8-5
8.1.1.5 Editing the Module Mapping 8-7
8.1.1.6 Allowing CGI Application to Use Execute 8-8
8.1.2 Configuring the Java Database Components 8-8
8.1.3 Configuring Custom Java Authentication 8-8
8.1.3.1 Configuring Custom Java Authentication for Windows 8-8
8.1.3.2 Configuring Custom Java Authentication for Linux 8-10
8.1.4 Configuring the Cognos 10 Environment 8-11
8.1.4.1 Opening the IBM Cognos 10 Configuration Window 8-11
8.1.4.2 Setting the Security Properties for Cognos 10 8-12
8.1.4.3 Setting the Data Access Properties for Cognos 10 8-13
8.1.4.4 Creating the Namespace for Argus Insight Authentication 8-16
8.1.4.5 Saving the Configuration and Starting the Cognos 10 Service 8-17

8.1.5 Creating Cognos Data Source (PRMART) 8-18
8.1.6 Configuring Cognos Security.... 8-20
8.1.6.1 Activating the PowerReports Namespace 8-21
8.1.7 Configuring Roles and Permissions.... 8-23

9 Configuring the OBIEE Environment

9.1 Pre-installation Configuration 9-1
9.2 Configuring the OBIEE Repository and Web Catalog using the BAR File 9-2
9.2.1 Importing the BAR file in an existing OBIEE instance.... 9-2
9.2.2 Importing the BAR file when creating a new OBIEE Instance.... 9-4
9.3 Configuring OBIEE Repository and Web Catalog Manually.... 9-5
9.4 Creating Users and Groups in OBIEE.... 9-6
9.4.1 Creating Users and Groups in WebLogic Server 9-7
9.4.2 Creating Roles and Policies with Fusion Middleware Control.... 9-8
9.5 OBIEE Catalog Folder-level Permissions 9-13
9.6 OBIEE Default Application Roles.... 9-15

10 Managing the Argus Insight Cryptography Key

10.1 Updating the Cryptography Key.... 10-1
10.1.1 Copying Initialization Files to Other Servers 10-2
10.1.2 Restarting IIS and Running ETL.... 10-2

11 Uninstalling the Argus Insight Application

11.1 Uninstalling Argus Insight from the Web Server 11-1
11.1.1 Deleting the Argus Insight Folder from the Web Server 11-1
11.1.2 Resetting the IIS 11-2

Preface

This *Oracle Argus Insight Installation Guide* describes installing — or upgrading to — Argus Insight 8.1. You perform some of these tasks once. Other tasks you repeat as your system and business requirements change.

This preface includes the following topics:

- Audience
- Documentation Accessibility
- Finding Information and Patches on My Oracle Support
- Finding Oracle Documentation
- Conventions

Audience

This document is intended for all Argus Insight administrators who are responsible for installing and maintaining the Argus Insight application.

Documentation Accessibility

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

Access to Oracle Support

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

Finding Information and Patches on My Oracle Support

Your source for the latest information about Argus Insight is Oracle Support's self-service website My Oracle Support.

Before you install and use Argus Insight, always visit the My Oracle Support website for the latest information, including alerts, White Papers, and bulletins.

Creating a My Oracle Support Account

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

To register for My Oracle Support:

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

Signing In to My Oracle Support

To sign in to My Oracle Support:

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

Finding Information on My Oracle Support

There are many ways to find information on My Oracle Support.

Searching by Article ID

The fastest way to search for information, including alerts, White Papers, and bulletins is by the article ID number, if you know it.

To search by article ID:

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

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

Searching by Product and Topic

You can use the following My Oracle Support tools to browse and search the knowledge base:

- Product Focus — On the Knowledge page under Select Product, type part of the product name and the system immediately filters the product list by the letters you have typed. (You do not need to type "Oracle.") Select the product you want from the filtered list and then use other search or browse tools to find the information you need.
- Advanced Search — You can specify one or more search criteria, such as source, exact phrase, and related product, to find information. This option is available from the **Advanced** link on almost all pages.

Finding Patches on My Oracle Support

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

To locate and download a patch:

1. Sign in to My Oracle Support at `https://support.oracle.com`.
2. Click the **Patches & Updates** tab. The Patches & Updates page opens and displays the Patch Search region. You have the following options:
   - In the **Patch ID or Number** field, enter the number of the patch you want. (This number is the same as the primary bug number fixed by the patch.) This option is useful if you already know the patch number.
   - To find a patch by product name, release, and platform, click the **Product or Family** link to enter one or more search criteria.
3. Click **Search** to execute your query. The Patch Search Results page opens.
4. Click the patch ID number. The system displays details about the patch. In addition, you can view the Read Me file before downloading the patch.
5. Click **Download.** Follow the instructions on the screen to download, save, and install the patch files.

Finding Oracle Documentation

The Oracle website contains links to all Oracle user and reference documentation. You can view or download a single document or an entire product library.

Finding Oracle Health Sciences Documentation

To get user documentation for Oracle Health Sciences applications, go to the Oracle Health Sciences documentation page at:

`http://www.oracle.com/technetwork/documentation/hsgbu-154445.html`

> **Note:** Always check the Oracle Health Sciences Documentation page to ensure you have the latest updates to the documentation.

Finding Other Oracle Documentation

To get user documentation for other Oracle products:

1. Go to the following web page:

   `http://www.oracle.com/technology/documentation/index.html`

   Alternatively, you can go to `http://www.oracle.com`, point to the Support tab, and then click **Documentation.**
2. Scroll to the product you need and click the link.
3. Click the link for the documentation you need.

Conventions

The following text conventions are used in this document:

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

1 Introduction

Argus Insight is a highly optimized reporting module for querying, case series management and reporting that compliments Argus Safety.

The Argus Insight Extract Transform and Load (ETL) engine extracts data from the Argus Safety database and populates Argus Insight data mart in a format to enable efficient querying. The query, drill-down, and output features of Argus Insight let you analyze your safety data from a scientific angle and produce queries, case series and reports that provide medical and scientific understanding of your aggregated adverse event information.

Argus Insight also supports Argus Mart as an additional data source. If you are using Argus Mart as a data source in a multi-tenant environment, then you may create Argus Mart Advanced Condition that queries Argus Mart database.

This chapter includes the following topics:

- Argus Insight Product Overview
- Software and Hardware Requirements
- Important Installation Information

Note: **Power Reports** has been renamed **Argus Insight**.

1.1 Argus Insight Product Overview

In Argus Insight, you can generate a report through a query. The query retrieves a set of specific type of cases (*Case Series*) from the data mart (Insight Mart/Argus Mart) and then runs the report on only those cases.

Use these Argus Insight components to retrieve the Case Series: *Query By Example (QBE)*, *Filters*, and *Advanced Conditions*. Next, run reports using any of the supported reporting tools (BIP/BusinessObjects/Cognos) on these Case Series.

The following flowchart shows the typical workflow for generating a report.

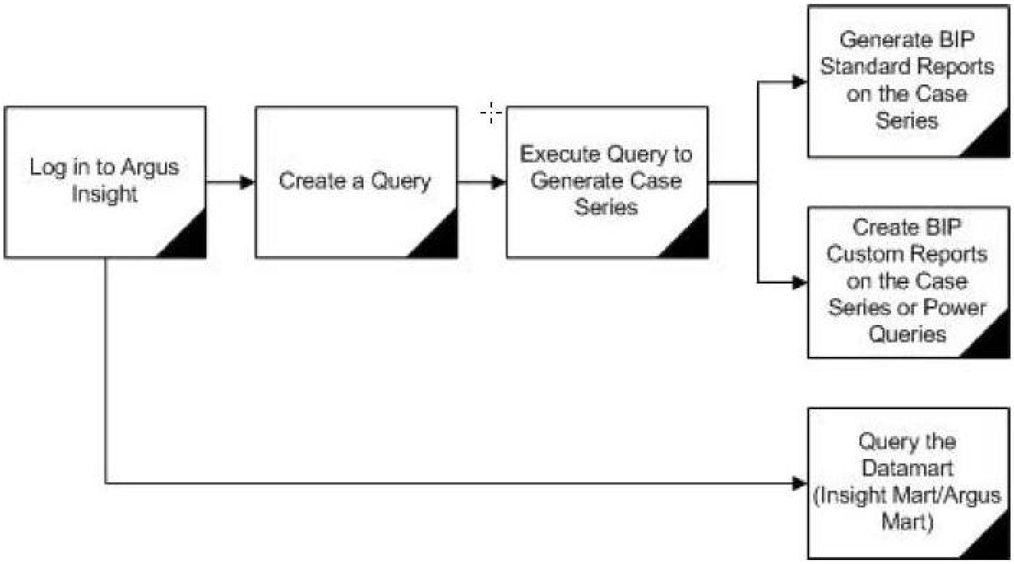

Log in to Argus Insight
Create a Query
Execute Query to Generate Case Series
Generate BIP Standard Reports on the Case Series
Create BIP Custom Reports on the Case Series or Power Queries
Query the Datamart (Insight Mart/Argus Mart)

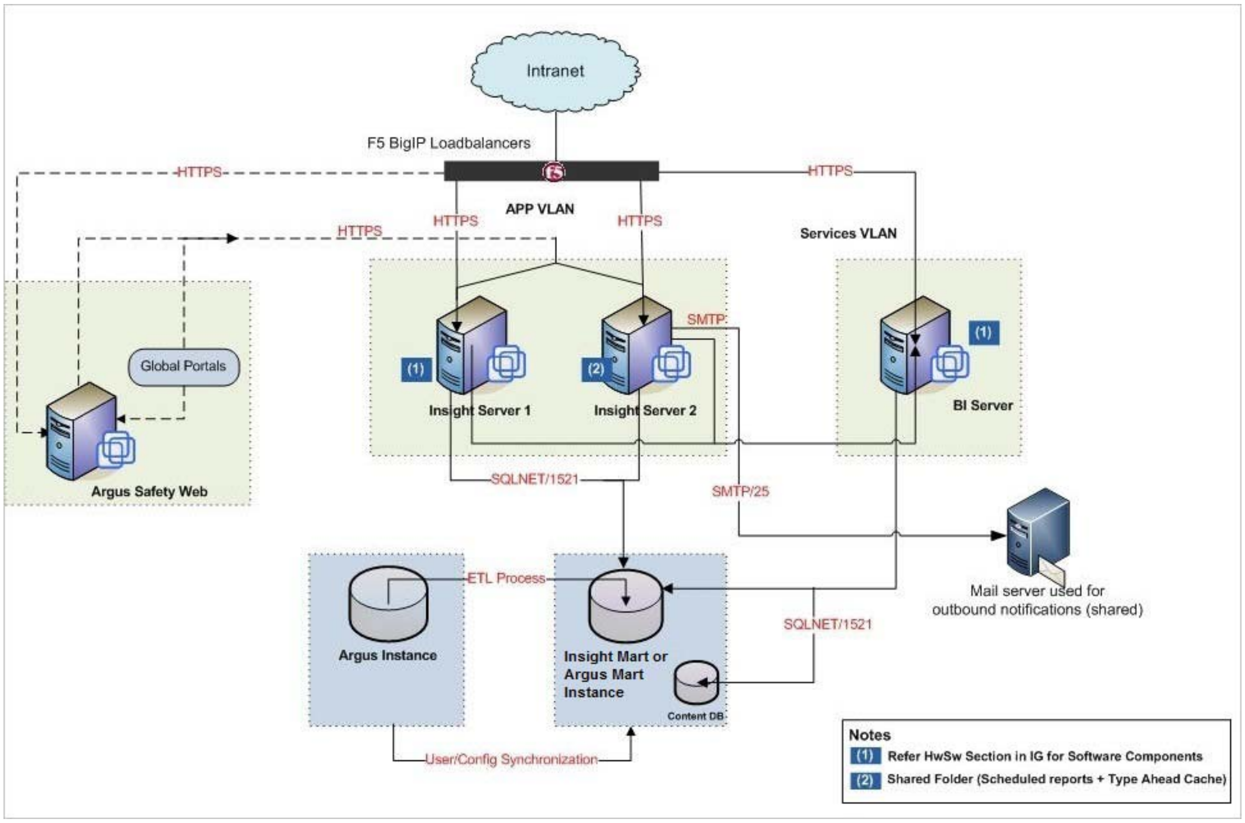
Table 1–1 describes the various features of Argus Insight:

Table 1–1 Argus Insight Features

Features	Description
Query by Example (QBE)	Lets you create simple queries by entering specific values in fields on a form that looks substantially like the Argus Safety case form.
Filters	Lets you create queries by selecting a set of predefined fields and specifying multiple values in a field.
Advanced Conditions	Lets you create complex queries by selecting any of the various different fields in the data mart (Insight Mart/Argus Mart) and applying Boolean and Set operations on them. You may use Advanced Conditions to query data on Argus Mart.
Case Series	A list of cases that match the query criteria with revisions (applicable only for Argus Mart).

1.1.1 Argus Insight Architecture

The following figure illustrates the Argus Insight architecture:



1.2 Software and Hardware Requirements

Table 1–2 lists the software and hardware requirements for the following components in an Argus Insight installation:

- Argus Insight Web Server
- Database Server
- BusinessObjects Server, Cognos, or OBIEE/BI Publisher (depending on which Business Intelligence tool you are using with Argus Insight)

> **Note:** Argus Insight can be used together with a reporting tool, which can be BusinessObjects, Cognos, OBIEE/BI Publisher, or any combination of these.

- Argus Insight Client

Table 1–2 Argus Insight Software and Hardware Requirements

Component	Requirements
Argus Insight Web Server	**Supported Operating Systems:** ■ Windows Server 2012 Standard ■ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ Oracle Client 12c Release 1 (12.1.0.2) ■ Oracle Data Provider 12c Release 1 (12.1.0.2) for .Net **Hardware Requirements:** ■ Up to 5000 cases in the system: 2x2.6 GHz processors, 4 GB memory ■ More than 5000 cases in the system: 4x2 GHz processors, 8 GB memory **Additional Software Requirements:** ■ Dotnet Framework 3.5 Service Pack 1 ■ IIS 8 (Windows 2012) ■ IIS 8.5 (Windows 2012 R2) ■ Microsoft Visual C++ 2005 SP1 Redistributable Package MFC Security Update ■ Microsoft Visual C++ Redistributable for Visual Studio 2012 Update 4 (x86) ■ MSXML 6.0 ■ WebGate 10.1.4.3 (optional) **Note:** The Argus Insight Web Server should be configured for Simple Mail Transfer Protocol (SMTP) for email support.
Database Server	**Supported Operating Systems:** ■ Solaris 10 ■ Solaris 11 ■ Oracle Linux 6.7 ■ Oracle Linux 7.1 ■ Windows Server 2012 Standard ■ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ Oracle Database Server (Standard/Enterprise) 12c Release 1 (12.1.0.2) (both CDB/PDB and Non-CDB formats) ■ Oracle RAC 12c Release 1 (12.1.0.2) ■ Exadata 12c Release 1 (12.1.0.2) **Note:** Oracle database standard edition is supported for single tenant deployment only. **Hardware Requirements:** ■ Up to 5000 cases in the system: 2x2 GHz processors, 4 GB memory ■ More than 5000 cases in the system: 4x2 GHz processors, 16 GB memory

Table 1–2 (Cont.) Argus Insight Software and Hardware Requirements

Component	Requirements
Oracle Business Intelligence Enterprise Edition (OBIEE) or **BI Publisher (BIP)**	**Supported Operating Systems:** ▪ Oracle Virtual Machine Server 3.2.10 (64 bit) ▪ Solaris 10 ▪ Solaris 11 ▪ Oracle Linux 6.7 ▪ Oracle Linux 7.1 ▪ Windows Server 2012 Standard ▪ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ▪ Same as Database Server. **Tool Version:** ▪ OBIEE or BIP 12c (12.2.1.0) **Note:** You can either install OBIEE or the stand alone BI Publisher (Dashboards are not available with standalone BI Publisher). **Additional Software Requirements:** ▪ Dotnet Framework 3.5 Service Pack 1 ▪ Java Development Kit (JDK) version 1.8 ▪ OBIEE Administrator Tool 12c (12.2.1.0.0) must be installed for configuring the repository file (RPD). Note that if you install OBIEE on a Linux machine, you need to install Oracle Business Intelligence Developer Client tools on a Windows machine. It will include the BI Administration tool. Refer to the *Oracle OBIEE Installation Manual* for further hardware and software requirements. ▪ WebGate 11.1.2.2 (optional)
BusinessObjects Server	**Supported Operating Systems:** ▪ Windows Server 2012 Standard ▪ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** Oracle Client 12 c Release 1 (12.1.0.2) (with SQL Plus, SQL Loader, Oracle and OLEDB Objects) **Hardware Requirements:** Same as the Argus Insight Web Server **Reporting Tool:** ▪ BusinessObjects XI Release 4.0 Service Pack 6 (only for single tenant installations)

Table 1–2 (Cont.) Argus Insight Software and Hardware Requirements

Component	Requirements
Cognos Server	**Supported Operating Systems:** ■ Windows Server 2012 Standard ■ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** Oracle Client 12 c Release 1 (12.1.0.2) (with SQL Plus, SQL Loader, Oracle and OLEDB Objects) **Hardware Requirements:** Same as the Argus Insight Web Server **Reporting Tool:** ■ Cognos 10.2.x BI Server (default installation with all components except Cognos Content Database) ■ Cognos 10.2 BI Modeling (default installation with all components) **Additional Software Requirements:** ■ WebGate 10.1.4.3 (32 bit) (optional)
Argus Insight Client	**Supported Operating Systems:** ■ Windows 7 (32 bit), (English version) ■ Windows 8.1 (64 bit), (English version) ■ Windows 10, (English version) **Hardware Requirements:** ■ 2.0 GHz Minimum, 1 GB Memory **Additional Software Requirements:** ■ Adobe Acrobat Reader 11 or DC ■ Microsoft Excel 2010, or 2013 ■ Microsoft Internet Explorer 11 (32/64 bit)

Note: Argus Insight also supports:

- Oracle Identity Manager 11.1.2.2
- Oracle Virtual Machine Server 3.2.10 (64 bit)

1.3 Important Installation Information

Before installing Argus Insight, review the information in this section carefully. You may need to modify several settings or install required software *before* you install the Argus Insight application.

1.3.1 Installation Requirements for the Servers

For the Argus Insight Web Server, BI Publisher, BusinessObjects Server, or Cognos Server:

- **Installation Language —** You must install all software with the language setting configured to English. For example, if Oracle is installed in a language other than English, the registry entries are created with different names. Therefore, to avoid errors, install all software in English.
- **Oracle Client —** You must install the Oracle client with the default *ORACLE_HOME* name, provided by the Oracle Universal Installer. Failure to do so will

display an error message, stating that the Oracle OLE DB provider was not found during installation.

- **Time Zone —** You must set all servers to the same time zone.
- **Default Language Setting —** All the servers must have the default language setting enabled for US English.

  To enable US English as the default language setting:

  1. Open the Microsoft System Registry Editor.
     a. Click **Start.**
     b. Select **Run.**
     c. Enter **regedit**, and then click **OK.**
  2. Navigate to the following folder:

     HKEY_USERS\.DEFAULT\Control Panel\International
  3. Double-click the **sCountry** key in the right pane.
     a. In the **Value data** field, enter **United States.**
     b. Click **OK** to save changes.
  4. Exit from the Registry Editor.
  5. Restart the server to reflect the changes.

Additional Notes:

- **For Argus Insight Web Server:**
  - Install the Oracle client *after* you install the Dotnet Framework.
  - Ensure that either you have disabled the firewall or you have added the Argus Insight port number in the Windows Firewall Exception list. The default port number for Argus Insight is 8084.
- **For BI Publisher:**
  - Ensure that you have disabled the firewall. Alternatively, if the firewall is enabled, ensure that BI Publisher is accessible from other machines on the network.
- **For BusinessObjects Server:**
  - Ensure that you have disabled the firewall. Alternatively, if the firewall is enabled, ensure that BusinessObjects is accessible from other machines on the network.
- **For Cognos Server:**
  - Ensure that you have disabled the firewall. Alternatively, if the firewall is enabled, ensure that Cognos is accessible from other machines on the network.

1.3.2 Installation Requirements for the Argus Insight Client

To run the Argus Insight application, you must configure the following settings on the Argus Insight client machine:

- Add the Argus Insight URL to the trusted sites.
- Enable Cookies to the lowest possible security level.

- Enable Javascript.
- Enable the **Allow script-initiated windows without size or position constraints** setting in Internet Explorer.

  To enable this setting:

  1. Start Internet Explorer.
  2. Open the **Tools** menu, and select **Internet Options.**
  3. Select the **Security** tab.
  4. Click **Custom level.**
  5. Scroll to the Miscellaneous settings.
  6. Enable the **Allow script-initiated windows without size or position constraints** setting.
  7. Click **OK** to save changes.

1.3.3 General Installation Notes and Information

- All the information about LDAP, Single Sign-On Header, and SMTP configuration will be synchronized in real-time and also by ETL.
- Ensure that you have configured the Argus Safety URL in the Argus Safety Load Balancer Server.

  To do so:

  1. Navigate to **Argus Console, System Management** (Common Profile Switches), and select **Network Settings.**
  2. In the Argus Safety Load Balancer Server text box, enter either the Argus Safety URL or the Argus Safety Load Balancer URL.

2 Installing Argus Insight

This chapter explains how to use the installation wizard to install Argus Insight, including the application software and standard reports, and the Schema Creation Tool.

This chapter includes the following topics:

- Before You Install the Argus Insight Application
- Installing Argus Insight Components onto the Web Server
- Enabling SSL Support for the Argus Insight Website

2.1 Before You Install the Argus Insight Application

Before you begin to install the Argus Insight application, you must verify or obtain the following information:

1. **Requirements —** Read Section 1.2, "Software and Hardware Requirements" and verify that your system meets the minimum requirements.
2. **Database Instance —** Verify that the Argus Insight database instance has been created and that it is running. In addition, verify that the database has been created using the character set of your Argus Safety database.
3. **Cryptographic Key —** Log in to the Argus Safety Web Server. Copy the **UserCryptoKey** from the ArgusSecureKey.ini file located at C:\Windows. You need to specify this key during the installation of Argus Insight.
4. **Security —** Log in to the Argus Insight Web Server.
   a. Ensure that the **IUSR** user or the user configured in Internet Information Services (IIS) has sufficient privileges for running the Argus Insight application. See the *Oracle Argus Insight Minimum Security Configuration Guide* for more information.
   b. Ensure that the ASP and ASP.Net extensions are enabled in IIS.

2.2 Installing Argus Insight Components onto the Web Server

Note: If you are upgrading Argus Insight from 8.0 to Argus Insight 8.1, first uninstall the application using Argus Insight application, and then run the Argus Insight 8.1 Installer.

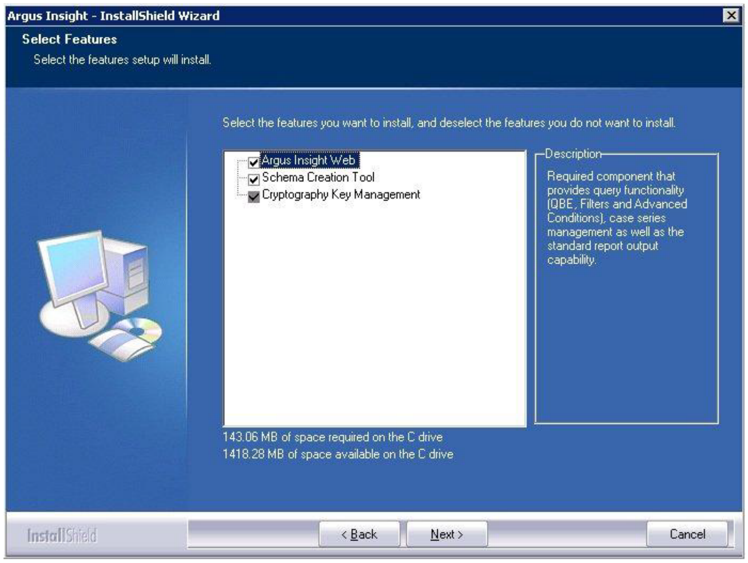
To uninstall the existing application, see Section 11, "Uninstalling the Argus Insight Application".

To run the installation wizard and install the Argus Insight components onto the Web Server:

1. Download the Argus Insight software from Oracle E-delivery and copy the software to the Argus Insight Web Server.
2. Log in to the Argus Insight Web Server as a user with administrator privileges.
3. Click **setup.exe.**

   The Welcome screen of the installation wizard appears.
4. Click **Next** to continue.
5. Enter your user name and company name into the appropriate fields.
6. Click **Next** to continue.

   The Select Features dialog box appears.



Argus Insight - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Argus Insight Web
☑ Schema Creation Tool
☑ Cryptography Key Management

Description

Required component that provides query functionality (QBE, Filters and Advanced Conditions), case series management as well as the standard report output capability.

143.06 MB of space required on the C drive
1418.28 MB of space available on the C drive

7. Clear any feature that you do not want to install. By default, the wizard installs all features.
8. Click **Next** to continue.

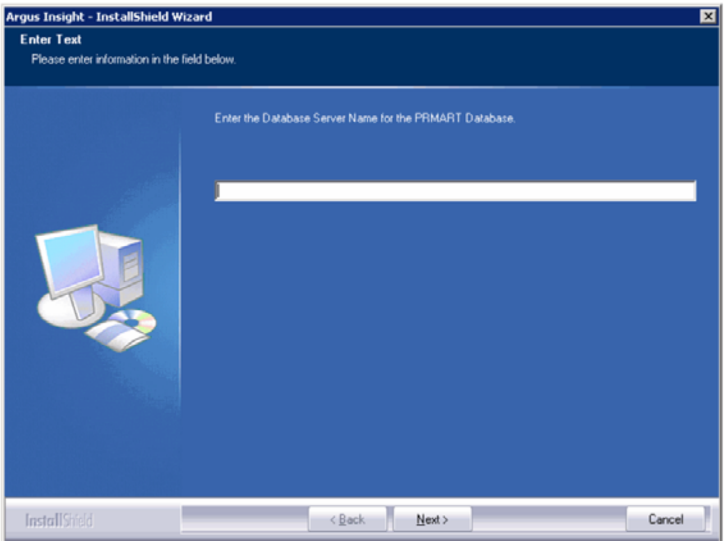
   The Choose Destination Location dialog box appears.
9. Specify the folder where the system installs the Argus Insight application.

   - To install into the default folder (C:\Program Files\Oracle), click **Next.**
   - To install into a different folder, click **Browse,** select another folder, and then click **Next.**

   A message appears stating that the wizard is ready to install the Argus Insight files.
10. Click **Install** to start the installation.

    A message appears stating that Argus Insight is configuring your new software along with the progress bar.

    When the installation is done, the following dialog box appears:



Argus Insight - InstallShield Wizard

Enter Text

Please enter information in the field below.

Enter the Database Server Name for the PRMART Database.

11. Enter the name of the host database server where the Argus Insight data mart is located, and click **Next.**
12. Enter the instance name for the Argus Insight data mart, and click **Next.**
13. Enter the database port number you want to assign to the Argus Insight database, and click **Next.**

    The system updates the TNSNAME.ORA file with the information as specified.

    When the update is done, the Cryptographic Key dialog box appears.
14. Enter the cryptographic key for Argus Insight, and then click **Next** to continue.

    Note: The cryptographic key is in the ArgusSecureKey.ini file located at C:\Windows on the Argus Safety Web Server with name as **UserCryptoKey**. You should have obtained this key during the pre-installation tasks.

15. Enter the password for APR_USER.

    Note: The APR_USER database user provides initial database access to the application user (APR_APP) of Argus Insight. Make sure that this password is the same on all machines where any Argus Insight components are stored.

    You will be prompted to create or update this user during schema creation. You can modify this password by running the Argus Insight installer and selecting the Modify option. For information about updating the APR_USER password, see Section 2.2.1, "Changing the APR_USER Password."

16. Click **Next** to continue.

    The Confirm Password dialog box appears.
17. Re-enter the APR_USER password for verification.
18. Click **Next.**

The Port Number dialog box appears.

19. Enter the port number you want to assign to the Argus Insight website.

    The default value is **8084.** If you are unsure of the port number, use the default value.

20. Click **Next.**

    The Argus Insight application is installed successfully.

21. Click **Finish** to exit from the installation wizard.

    A confirmation dialog box appears — Argus Insight Install wizard will now reboot the system. Please save any unsaved work.

22. Click **OK** to restart the Argus Insight Web Server.

2.2.1 Changing the APR_USER Password

You need to update the password on the database level and the Argus Insight Web Server or Cognos Server. The Argus Insight application uses this password to communicate with the database initially.

Before changing the password for the APR_USER on any Argus Insight Web Server or Cognos Server:

- Stop the Argus Insight service.
- Stop IIS on the Argus Insight Web Server.
- Stop the IIS and the Cognos service on the Cognos Server.

  This is required only when you are using Cognos 10 as your Business Intelligence tool.
- Update the password of APR_USER on database level.

  You need to update the password at the database level before you can modify the password for the Argus Insight Web Server.

You can modify the password for APR_USER on any Argus Insight Web Server or Cognos Server by running the Argus Insight installer on each server.

To modify the APR_USER password:

1. Run **setup.exe** to start the Argus Insight installer.

   The Argus Insight Setup Maintenance dialog box appears.

2. Select **Modify**, and click **Next.**
3. Select **Change the password for APR_USER,** and click **Next.**
4. Enter the **APR_USER** password.

   The password you enter must be the same password for each server being used by Argus Insight and must be configured in the Argus Insight database.

5. Click **Next.**

   A dialog box to confirm new password appears.

6. Enter the new **APR_USER** password a second time for verification.
7. Click **Next.**

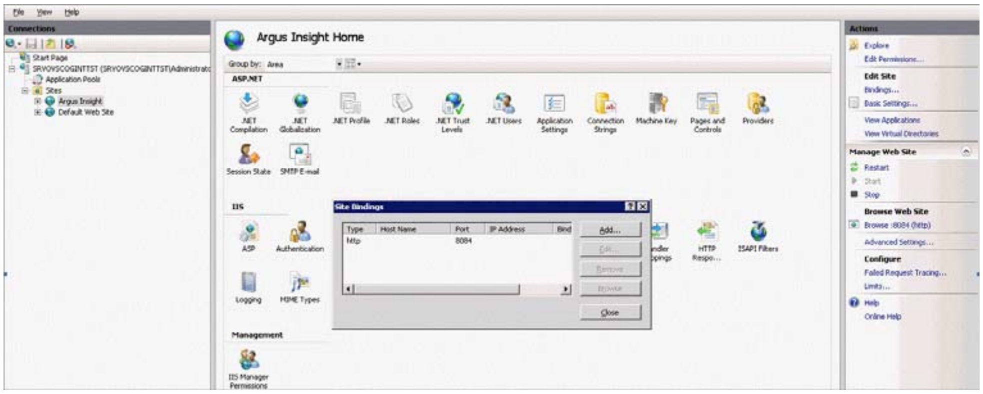
   The system updates the password for APR_USER.

2.3 Enabling SSL Support for the Argus Insight Website

To enable SSL support for the Argus Insight website:

1. Log in to the Argus Insight Web Server.
2. Obtain and install the SSL certificate.
3. Go to IIS Manager.
4. Select **Argus Insight**, and select **Bindings.**

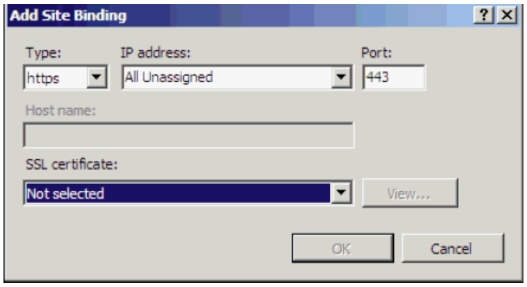
   The Site Bindings dialog box appears.



Type	Host Name	Port	IP Address	Bind
http		8084		

5. Click **Add.**

   The Add Site Binding dialog box appears.



Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: Not selected

6. Enter the following details in the Add Site Binding dialog box:
   a. In the **Type** field, select **https.**
   b. In the **SSL certificate** field, select your security certificate.
   c. Click **OK.**

3

Creating the Argus Insight Data Mart Structure

The Argus Insight Schema Creation Tool lets you create the Argus Insight data mart structure. It creates a link between source Argus database and new Argus Insight data mart. The Extract Transform and Load (ETL) process uses this link to transfer data from Argus Safety database to the Argus Insight data mart for reporting purposes.

During the schema creation process, you are required to create database users:

- To login in to the Argus Insight application.
- As schema owners.
- To support private database links (DB Links).

This chapter includes the following topics:

- Before You Run the Argus Insight Schema Creation Tool
- Argus Insight Configuration Requirements
- Argus Insight Data Mart Tablespaces
- Starting the Argus Insight Schema Creation Tool
- Creating the Database Schema
- Validating the Schema
- Creating a Database Link from Argus Safety to Insight Database
- Upgrading Database from Argus Insight 8.0 to Argus Insight 8.1
- Running Additional Grant Scripts for Single DB Instance
- Creating Argus Insight Read-Only User

Note: The Argus Insight database must be created with the same character set as the Argus Safety database. Make sure you have installed the requisite software as explained in Section 1.2, "Software and Hardware Requirements".

3.1 Before You Run the Argus Insight Schema Creation Tool

The **GLOBAL_NAME** and **NLS_LENGTH_SEMANTICS** database parameters must be configured properly in order for the Argus Insight Schema Creation Tool to run. You must check those settings *before* you run the Argus Insight Schema Creation Tool. If the parameters are not set properly, the Schema Creation Tool will fail.

To review and modify these database settings:

1. Contact your database administrator (DBA).
2. Verify that the database configuration file for the Argus Insight database defines the following database parameter values:
   - GLOBAL_NAME = FALSE

     (This parameter must be set to FALSE for Argus Insight to be able to create the database links.)
   - NLS_LENGTH_SEMANTICS = CHAR
3. Restart the database instance to reflect the changes.

To create a DBA user:

If you want to use a different user than SYSTEM user to execute the Schema Creation Tool, then create a DBA user by executing the following .bat file:

ARGUS_INSIGHT_INSTALL_PATH/Database/Utils/ai_create_dba_user.bat

Besides creating the DBA user, this .bat file also provides minimum necessary privileges required for executing the Schema Creation Tool.

3.2 Argus Insight Configuration Requirements

This section lists the required and recommended values for:

- Database parameters
- Database I/O configuration
- RAM and CPU

3.2.1 Database Parameters

Table 3–1 lists the database parameters and the values that must be set for Argus Insight.

For those parameters that require a numeric value, Table 3–1 lists the minimum value recommended. You may need to increase the value depending on your system configuration and the number of cases. It is the responsibility of the database administrator to monitor the system and adjust the database parameters as necessary.

Table 3–1 Database Parameters for Argus Insight

Database Parameter	Required Value
COMPATIBLE (for Oracle 12*c* R1)	12.1.0.2 or later
CURSOR_SHARING	EXACT
GLOBAL_NAME	FALSE
JOB_QUEUE_PROCESSES	10 (Minimum value recommended)
NLS_LENGTH_SEMANTICS	CHAR
OPTIMIZER_MODE	ALL_ROWS
OPTIMIZER_SECURE_VIEW_MERGING	TRUE
PARALLEL_MAX_SERVERS	Minimum value recommended based on the total number of cases: ■ Small (< 30,000 cases): 16 ■ Medium (30,000 to 200,000 cases): 32 ■ Large (200,000 to 1,000,000 cases): Default ■ Extra Large (> 1,000,000 cases): Default
PGA_AGGREGATE_TARGET	Minimum value recommended based on the total number of cases: ■ Small (< 30,000 cases): 0.5 GB ■ Medium (30,000 to 200,000 cases): 2 GB ■ Large (200,000 to 1,000,000 cases): 3 GB ■ Extra Large (> 1,000,000 cases): 4 GB
QUERY_REWRITE_ENABLED	TRUE (if computing statistics regularly) FALSE (if not computing statistics regularly)
SGA_MAX_SIZE	Greater than or equal to the value of the SGA_TARGET parameter.
SGA_TARGET	Minimum value recommended based on the total number of cases: ■ Small (< 30,000 cases): 1 GB ■ Medium (30,000 to 200,000 cases): 2.5 GB ■ Large (200,000 to 1,000,000 cases): 3.5 GB ■ Extra Large (> 1,000,000 cases): 4.5 GB The 32-bit architecture allows for 4 GB of physical memory to be addressed. DBAs should verify the maximum addressable RAM for their respective architectures.
UNDO_MANAGEMENT	AUTO
WORKAREA_SIZE_POLICY	AUTO
DB_BLOCK_BUFFERS (in MB) / DB_CACHE_SIZE	Leave set to the Oracle default value
DB_BLOCK_SIZE (in bytes)	Leave set to the Oracle default value
QUERY_REWRITE_INTEGRITY	Leave set to the Oracle default value
SHARED_POOL_SIZE	Leave set to the Oracle default value

3.2.2 Database I/O Configuration

Table 3–2 lists the minimum amount of disk space to allocate for the redo log files, TEMP tablespace, and UNDO tablespace.

Table 3–2 Recommended Database I/O Configuration for Argus Insight

	Total Number of Cases			
Database I/O Configuration	Small (< 30,000)	Medium (30,000 to 200,000)	Large (200,000 to 1,000,000)	Extra Large (> 1,000,000)
Number and Size of Redo Log Files	Default	3 X 500 MB	5 X 500 MB	5 X 500 MB
	The value depends on the characteristics of the I/O subsystem such as the I/O bandwidth, storage disks type, and RAID level. (Oracle recommends RAID 1+0 or similar.)			
TEMP Tablespace Size	32 GB	32 GB	64 GB	128 GB
UNDO Tablespace Size	16 GB	32 GB	64 GB	128 GB

	The recommended UNDO tablespace size is based on the projections with the following two parameter values:
	RETENTION=NOGUARANTEE
	UNDO_RETENTION=900 (seconds)			

3.2.3 Recommended Configuration for the Database Server

Table 3–3 lists the recommended configuration (RAM and CPU) for the Argus Insight Database Server.

Table 3–3 Recommended Configuration for the Argus Insight Database Server

	Total Number of Cases			
Database Server Configuration	Small (< 30,000)	Medium (30,000 to 200,000)	Large (200,000 to 1,000,000)	Extra Large (> 1,000,000)
RAM	4–8 GB	8–16 GB	16–32 GB	16–32 GB
CPU	Equivalent to 2–4 Dual Core, 3 GHz	Equivalent to 4–8 Dual Core, 3 GHz	Equivalent to 8–12 Dual Core, 3 GHz	Equivalent to 8–12 Dual Core, 3 GHz

Note: The Argus Insight Database and Argus Safety Database TNS names entry must be available in both Argus Insight Database Server and Argus Safety Database Server. Argus Safety Database TNS should also be present in the Argus Insight Web Server.

3.3 Argus Insight Data Mart Tablespaces

Table 3–4 lists the tablespaces for the Argus Insight data mart. Argus Insight creates these tablespaces when you create a database schema.

Note that the tablespace names begin with APR. The Argus Power Reports (APR) product was renamed to Argus Insight.

Table 3–4 Tablespaces Created for the Argus Insight Data Mart

APR_CFG_DATA_01	APR_MEDM_DATA_01	APR_MRPT_INDEX_01
APR_MCAS_DATA_01	APR_MEDM_INDEX_01	APR_MRPT_INDEX_02
APR_MCAS_DATA_02	APR_MEDM_LOB_01	APR_MRPT_INDEX_03
APR_MCAS_HIST_DATA_01	APR_MFACT_DATA_01	APR_MWHOC_DATA_01
APR_MCAS_HIST_DATA_02	APR_MFACT_HIST_DATA_01	APR_MWHOC_INDEX_01

Table 3–4 (Cont.) Tablespaces Created for the Argus Insight Data Mart

APR_MCAS_HIST_INDEX_01	APR_MFACT_HIST_INDEX_01	APR_SESM_DATA_01
APR_MCAS_HIST_LOB_01	APR_MFACT_INDEX_01	APR_SESM_INDEX_01
APR_MCAS_INDEX_01	APR_MRPT_DATA_01	APR_SESM_LOB_01
APR_MCAS_INDEX_02	APR_MRPT_DATA_02	APR_STAGE_DATA_01
APR_MCAS_LOB_01	APR_MRPT_DATA_03	APR_STAGE_DATA_02
APR_MCFG_DATA_01	APR_MRPT_HIST_DATA_01	APR_STAGE_DATA_03
APR_MCFG_HIST_INDEX_01	APR_MRPT_HIST_DATA_02	APR_STAGE_INDEX_01
APR_MCFG_HIST_LOB_01	APR_MRPT_HIST_DATA_03	APR_STAGE_INDEX_02
APR_MCFG_INDEX_01	APR_MRPT_HIST_INDEX_01	APR_STAGE_INDEX_03
APR_MCFG_LOB_01	APR_MRPT_HIST_INDEX_02	APR_STAGE_LOB_01
APR_MCFG_LOG_01	APR_MRPT_HIST_INDEX_03	APR_SWHOC_DATA_01

3.4 Starting the Argus Insight Schema Creation Tool

To start the Argus Insight Schema Creation Tool:

1. Log in to the Argus Insight Web Server.
2. Click **Start.**
3. Navigate to **Programs > Oracle > Argus Insight,** and select **Schema Creation Tool.**

   The Schema Creation Tool appears.

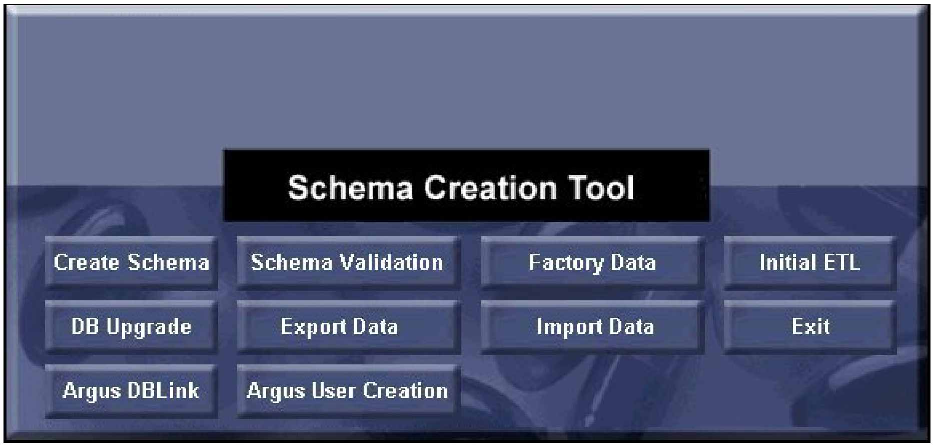


Table 3–5 Summary of the Schema Creation Tool options

Option	Description	Reference
Create Schema	Creates a new database schema for Argus Insight.	Section 3.5, "Creating the Database Schema"
Schema Validation	Validates a newly-created database schema.	Section 3.6, "Validating the Schema"
Factory Data	Loads the factory data into the database.	Section 3.5.4, "Loading Factory Data"

Table 3–5 (Cont.) Summary of the Schema Creation Tool options

Option	Description	Reference
Initial ETL	Runs the initial process of extracting, transforming, and loading data.	Chapter 5, "Extracting, Transforming, and Loading Data"
DB Upgrade	Upgrades an existing Argus Insight 8.0 database to an Argus Insight 8.1 database.	Section 3.8, "Upgrading Database from Argus Insight 8.0 to Argus Insight 8.1"
Export Data	Exports data.	Section 4.7.1, "Exporting Data"
Import Data	Imports data.	Section 4.7.2, "Importing Data"
Argus DBLink	Creates a link between Argus Insight and Argus Safety.	Section 3.7, "Creating a Database Link from Argus Safety to Insight Database"
Argus User Creation	Lets you create Argus Insight users and roles.	Section 3.5.1, "Creating Users and Roles in the Argus Safety Database"
Exit	Exits from the Schema Creation Tool.	NA

3.5 Creating the Database Schema

This section describes the tasks associated with creating the database schema:

- Creating Users and Roles in the Argus Safety Database
- Clearing the Cache
- Creating a New Schema for Argus Insight
- Loading Factory Data

3.5.1 Creating Users and Roles in the Argus Safety Database

To create users and roles:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Argus User Creation.**

   The Oracle Database Connect dialog box appears.
3. Connect to the Oracle Database:

   a. In the **User** field, enter the name of Argus Safety SYSTEM or DBA user.

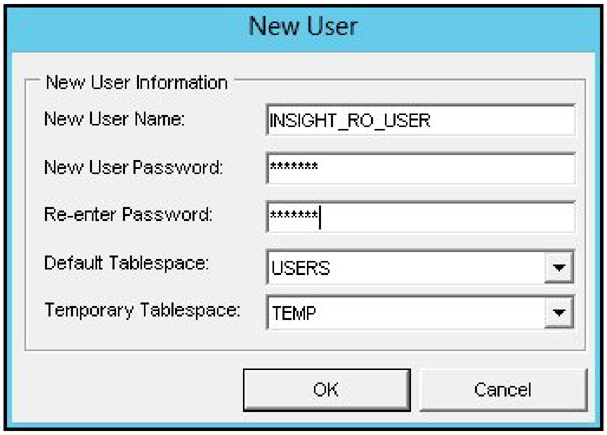
   b. In the **Password** field, enter the password for Argus Safety SYSTEM or DBA user.

   c. In the **Argus Safety Database** field, enter the name of your Argus Safety database instance.

   d. Click **OK.**

   The Argus Safety Read Only User Creation dialog box appears.
4. Click **New User.**

   The New User dialog box appears.



New User

New User Information

New User Name: INSIGHT_RO_USER

New User Password: *******

Re-enter Password: *******

Default Tablespace: USERS

Temporary Tablespace: TEMP

5. Complete the New User dialog box as follows:

   a. Enter a name for the new user.

   b. Specify and confirm the password for the user.

   c. Select the default and temporary tablespaces required by your corporate standards, or leave the default values.

   d. Click **OK.**

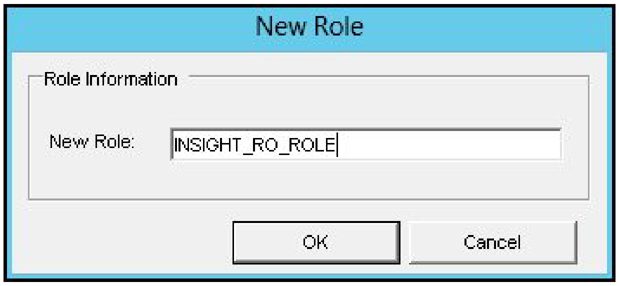
   You return to the Argus Safety Read Only User Creation dialog box.

   Note: You must create the INSIGHT_RO_USER and INSIGHT_RO_ROLE, if they do not exist in the Argus Safety schema. Make the appropriate selection in Step 8 below for **New User Name** and **New Role** drop-downs and proceed.

   ---

6. Click **New Role.**

   The New Role dialog box appears:



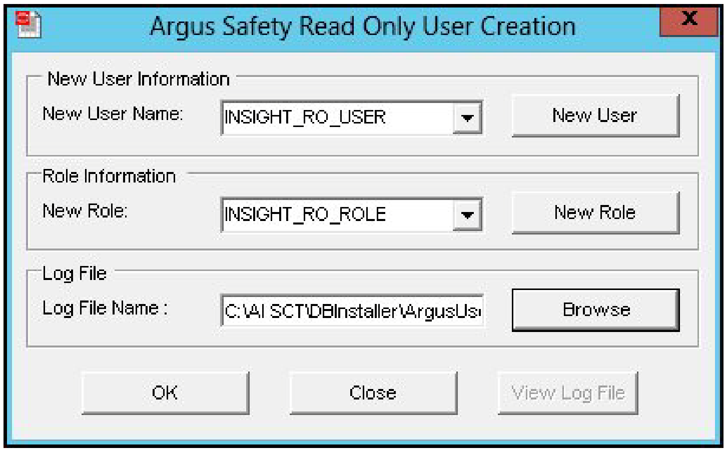
New Role

Role Information

New Role: INSIGHT_RO_ROLE

7. Enter the name of the new role to create, and then click **OK.**

   You return to the Argus Safety Read Only User Creation dialog box.



New User Information

New User Name: INSIGHT_RO_USER

Role Information

New Role: INSIGHT_RO_ROLE

Log File

Log File Name : C:\AI SCT\DBInstaller\ArgusUs

Note: In case you have upgraded the database from Argus Insight 8.0 to 8.1, you can also select the existing user, which you have already created earlier, from the **New User Name** drop-down list.

---

8. Complete the Argus Safety Read Only User Creation dialog box as follows:

   a. In the **New User Name** field, select **INSIGHT_RO_USER.**

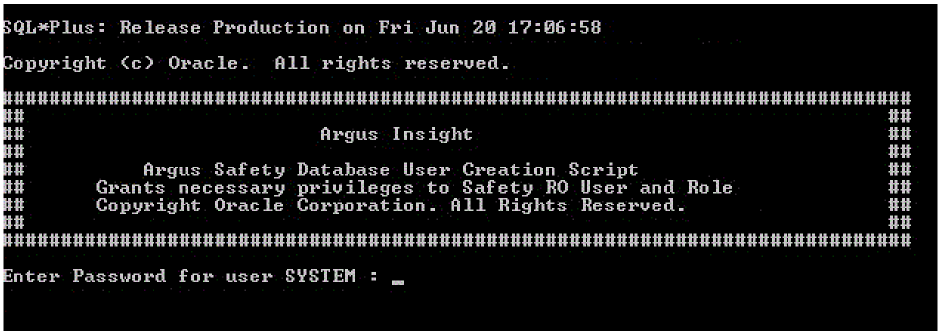
   b. In the **New Role** field, select **INSIGHT_RO_ROLE.**

   c. In the **Log File Name** field, enter the complete path for the location and name of the log file.

      Alternatively, you can click **Browse** to select the location for the log file, enter the file name, and then click **Save.**

9. Click **OK** when you are ready to create the specified user with the specified role.

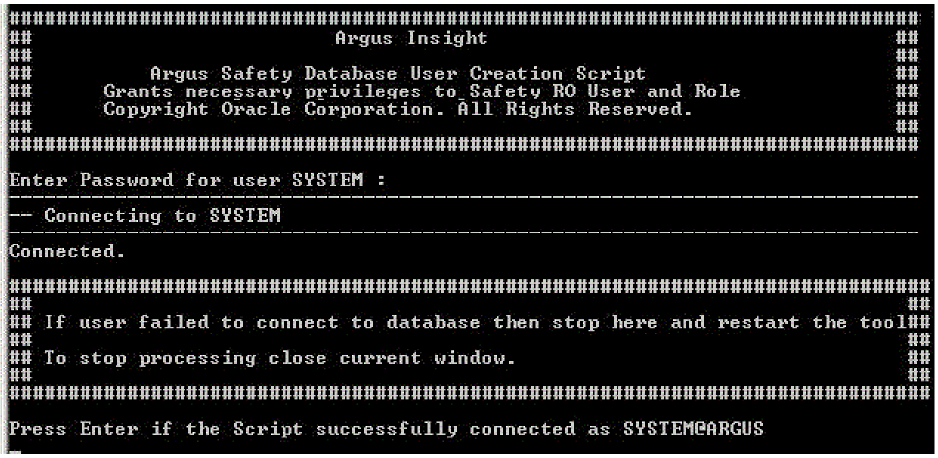
   The command prompt screen appears.



```
SQL*Plus: Release Production on Fri Jun 20 17:06:58

Copyright (c) Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                            Argus Insight                                 ##
##                                                                          ##
##              Argus Safety Database User Creation Script                  ##
##          Grants necessary privileges to Safety RO User and Role          ##
##          Copyright Oracle Corporation. All Rights Reserved.              ##
##                                                                          ##
##############################################################################

Enter Password for user SYSTEM : _
```

10. Enter the password for the Argus Insight SYSTEM or SAFETY_DBA_USER user, and press **Enter**.

11. Verify that the script is successfully connected as <SYSTEM/DBA User Name>@<Argus Safety Database Name>.



```
################################################################################
##                              Argus Insight                                 ##
##                                                                            ##
##           Argus Safety Database User Creation Script                       ##
##       Grants necessary privileges to Safety RO User and Role               ##
##       Copyright Oracle Corporation. All Rights Reserved.                   ##
##                                                                            ##
################################################################################

Enter Password for user SYSTEM :
--------------------------------------------------------------------------------
-- Connecting to SYSTEM
--------------------------------------------------------------------------------
Connected.

################################################################################
##                                                                            ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                            ##
## To stop processing close current window.                                   ##
##                                                                            ##
################################################################################

Press Enter if the Script successfully connected as SYSTEM@ARGUS
```

12. Press **Enter**.

    The information about the Argus Safety database name, the name of the user to create, the role to assign to the user, and the name of the log file appears.

13. Verify that the information is correct, and then press **Enter** to continue.

    The additional information about creating the user and granting privileges appears.

14. Press **Enter** to complete the installation.

    A message stating that the user account has been created successfully appears along with the folder location of the log files.

15. Click **OK** to close the message box.

    You return to the **Argus Safety Read Only User Creation** dialog box.

16. Click **View Log File.**

    a. Review the information in the log file and check for any errors.

    b. After reviewing, close the log file.

17. Click **Close** to close the **Argus Safety Read Only User Creation** dialog box.

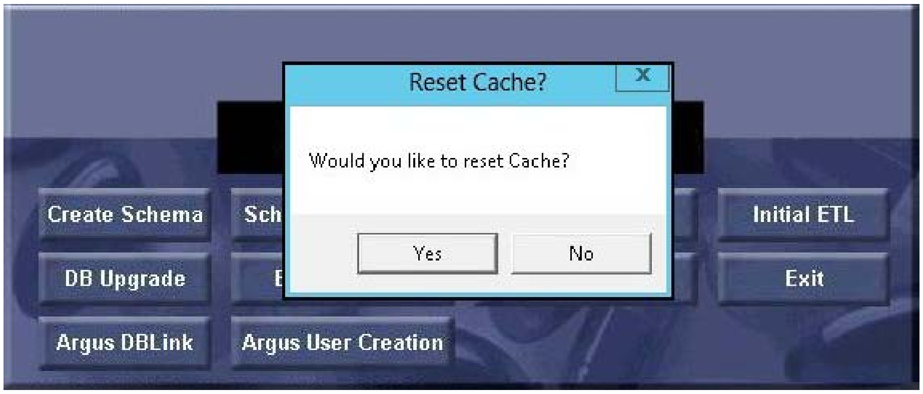
3.5.2 Clearing the Cache

If you are using the same Database Installer used to create an earlier schema, you **must** clear its cache.

To clear the cache:

1. Press and hold the CTRL key, and right-click the mouse.

   The Reset Cache? dialog box appears.



Reset Cache?

Would you like to reset Cache?

2. Click **Yes.**

   The cache is cleared and actions are logged in the **createlog.rtf** file.

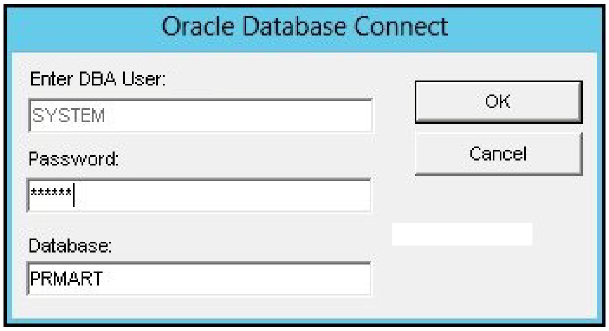
3.5.3 Creating a New Schema for Argus Insight

> **Note:** Before executing the steps for creating a new schema for Argus Insight, ensure that you have remote access to the SYS user.
>
> If you **do not** have remote access to SYS user, execute the **ai_sys{grant}.sql** script through SYS user. This SQL script is located in the following folder:
>
> drive:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\DDL Folder

To create a new schema for Argus Insight:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Create Schema.**

   The Oracle Database Connect dialog box appears.



Oracle Database Connect

Enter DBA User: SYSTEM

Password: ******

Database: PRMART

3. Connect to the Oracle Database:

   a. In the **User** field, enter the name of Argus Insight SYSTEM or DBA user.

   b. In the **Password** field, enter the password for Argus Insight SYSTEM or DBA user.

   c. In the **Database** field, enter the TNS entry for the Argus Insight database.

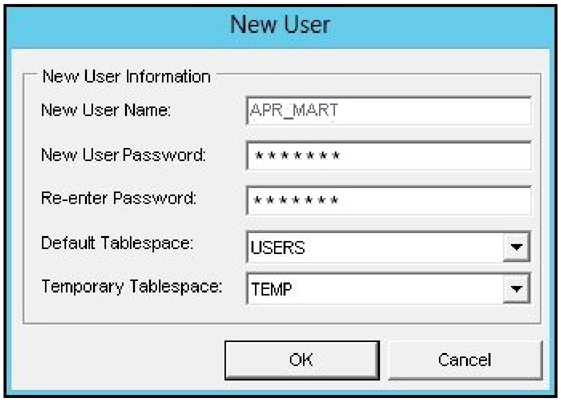
   d. Click **OK.**

Note that:

- If the NLS_LENGTH_SEMANTICS database parameter is not set to **CHAR**, an error message appears. You cannot proceed with the process of creating a new schema. You must set the NLS_LENGTH_SEMANTICS parameter to CHAR in the Argus Insight data mart and then restart the database instance.

  See Section 3.1, "Before You Run the Argus Insight Schema Creation Tool" for details.

- If the NLS_LENGTH_SEMANTICS database parameter is set to **CHAR**, the New User dialog box for the **APR_MART** user appears.



New User Name: APR_MART

New User Password: *******

Re-enter Password: *******

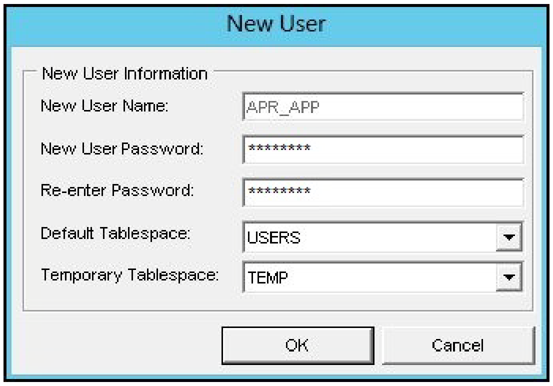
Default Tablespace: USERS

Temporary Tablespace: TEMP

4. Enter a password for the **APR_MART** user (which is the schema owner), and then re-enter to confirm the password.

5. Click **OK.**

   The New User dialog box for the **APR_APP** user appears.



New User Name: APR_APP

New User Password: ********

Re-enter Password: ********

Default Tablespace: USERS

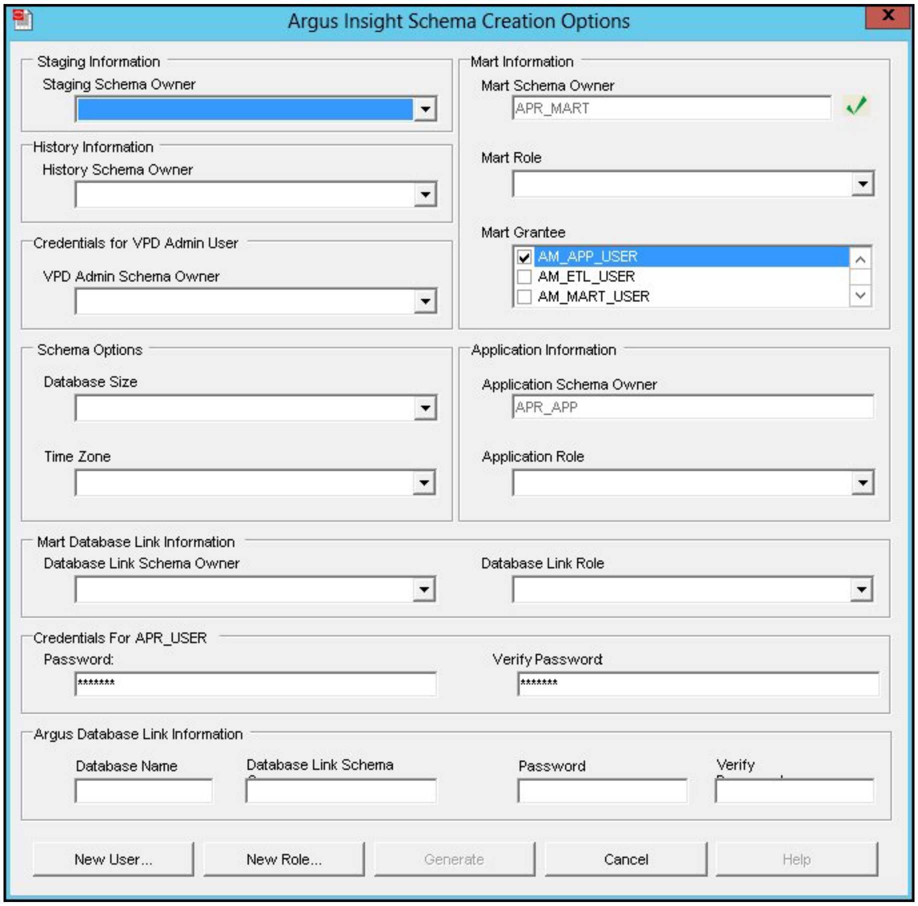
Temporary Tablespace: TEMP

6. Enter a password for the **APR_APP** user, and then re-enter to confirm the password.

Note: Argus Insight uses the **APR_APP** user account for all application access and reporting. The password for this user is stored in encrypted form in the **CMN_PROFILE_GLOBAL** table. If you need to change this password in the future or if you forget the password, you must contact Oracle Support for assistance in resetting the **APR_APP** password in the **CMN_PROFILE_GLOBAL** table. If the password for this user is not in synchronization with the value in the **CMN_PROFILE_GLOBAL** table, the Argus Insight application will not work.

7. Click **OK.**

   The Argus Insight Schema Creation Options dialog box appears.



Mart Schema Owner: APR_MART ✓

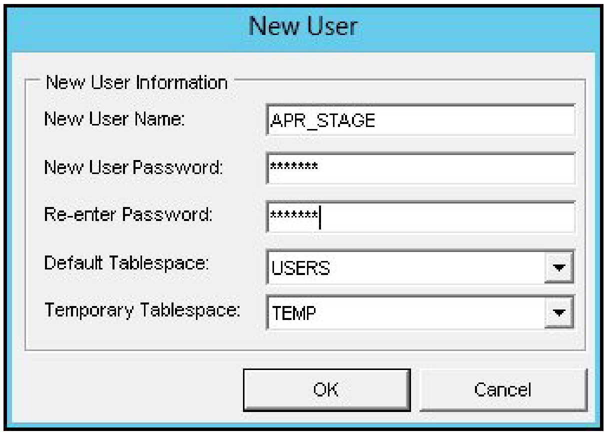
Mart Grantee:
☑ AM_APP_USER
□ AM_ETL_USER
□ AM_MART_USER

Application Schema Owner: APR_APP

Credentials For APR_USER
Password: *******
Verify Password: *******

8. Click **New User.**

   The New User dialog box appears.



New User

New User Information

New User Name: APR_STAGE

New User Password: *******

Re-enter Password: *******

Default Tablespace: USERS

Temporary Tablespace: TEMP

a. In the **New User Name** field, enter one of the following names:

   - APR_STAGE
   - APR_LOGIN
   - APR_LINK_USER
   - APR_HIST
   - RLS_USER

b. In the **New User Password** field, enter the password for the specified user.

c. In the **Re-enter Password** field, enter the user password again for verification.

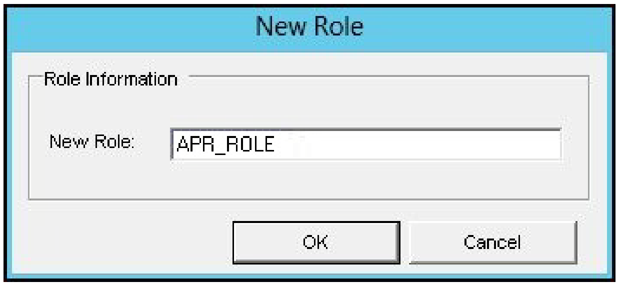
d. Click **OK.**

   You return to the Argus Insight Schema Creation Options screen.

Repeat this step until you have created all the above users.

9. Click **New Role.**

   The New Role dialog box appears.



New Role

Role Information

New Role: APR_ROLE

a. Enter one of the following names in the **New Role** field:

   - APR_ROLE
   - APR_LINK_ROLE
   - APR_APP_ROLE

b. Click **OK.**

   You return to the Argus Insight Schema Creation Options screen.

Repeat this step until you have created all the above roles.

10. Define the following users and roles in the Argus Insight Schema Creation Options screen:

    a. From the **Staging Schema Owner** drop-down list, select **APR_STAGE**.

    b. From the **History Schema Owner** drop-down list, select **APR_HIST**.

    c. From the **VPD Admin Schema Owner** field, select **RLS_USER.**

    d. In the **Schema Options** section, select the Database Size and the Time Zone.

    e. From the **Mart Role** drop-down list, select **APR_ROLE**.

    f. In **Mart Grantee** section, select the **APR_LOGIN** check box.

    g. From the **Application Role** drop-down list, select **APR_APP_ROLE**.

    h. Under the MART Database Link Information section:

       i. In the **Database Link Schema Owner** drop-down list, select **APR_LINK_USER.**

       ii. In the **Database Link Role** drop-down list, select **APR_LINK_ROLE.**

    i. In the Argus Database Link Information section:

       Note: The value you enter in the Database Link Schema Owner field should be the name of the Argus Insight read-only user that you created earlier in the installation process. See Section 3.5.1, "Creating Users and Roles in the Argus Safety Database" for details.

       i. In the **Database Name** field, enter the name of the Argus Safety database.

       ii. In the **Database Link Schema Owner** field, enter **INSIGHT_RO_USER**.

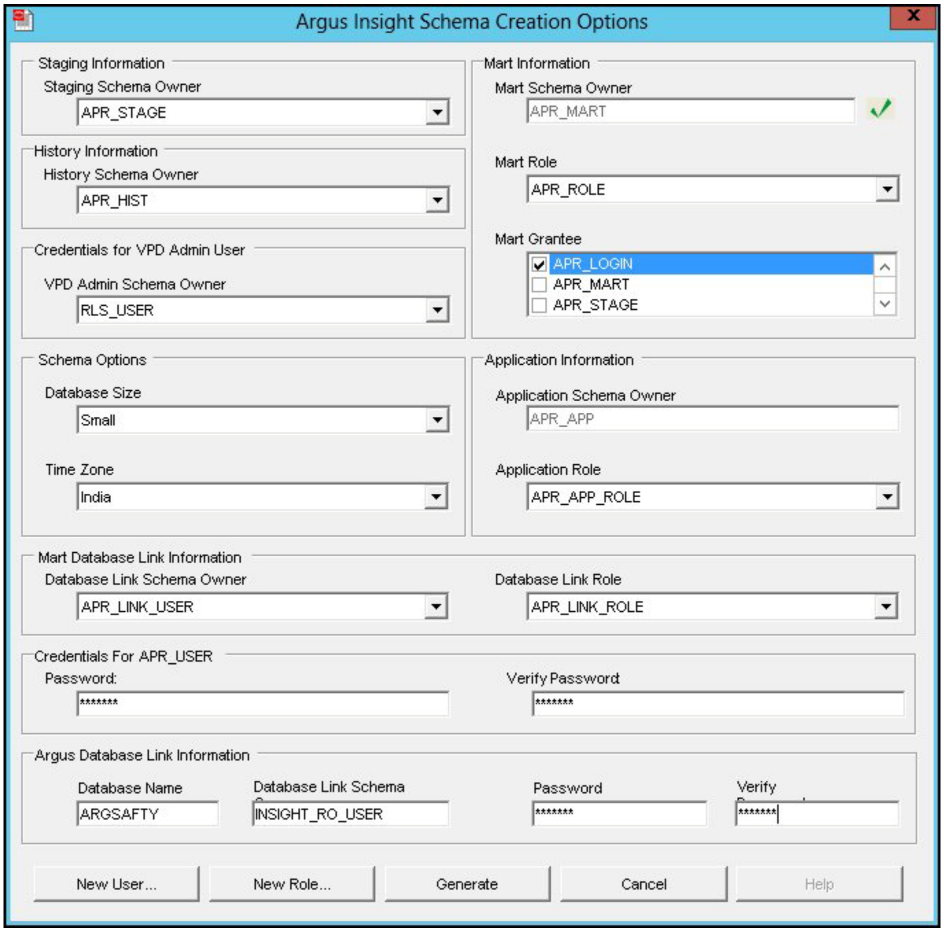
       iii. In the **Password** field, enter the password for the INSIGHT_RO_USER.

       iv. In the **Verify Password** field, re-enter the password.

    j. Optionally, in the Credentials for **APR_USER** section, enter and verify a new password only if you want to change the password for **APR_USER**.

       All these inputs have been depicted in the following figure:

       Note: You must update the **APR_USER** password using the instructions in the Section 2.2.1, "Changing the APR_USER Password" section, if you change the default **APR_USER** password. This is to update the password on the database level and the Argus Insight Web Server/Cognos Server.



Argus Insight Schema Creation Options

Staging Information
Staging Schema Owner: APR_STAGE

History Information
History Schema Owner: APR_HIST

Credentials for VPD Admin User
VPD Admin Schema Owner: RLS_USER

Mart Information
Mart Schema Owner: APR_MART ✓
Mart Role: APR_ROLE
Mart Grantee:
☑ APR_LOGIN
☐ APR_MART
☐ APR_STAGE

Schema Options
Database Size: Small
Time Zone: India

Application Information
Application Schema Owner: APR_APP
Application Role: APR_APP_ROLE

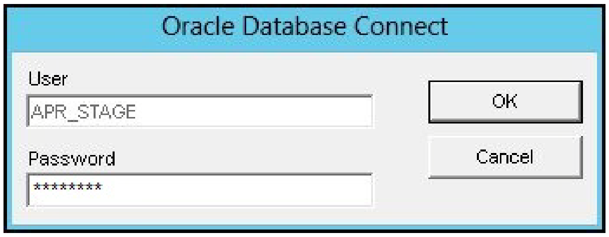
Mart Database Link Information
Database Link Schema Owner: APR_LINK_USER
Database Link Role: APR_LINK_ROLE

Credentials For APR_USER
Password: *******
Verify Password: *******

Argus Database Link Information
Database Name: ARGSAFTY
Database Link Schema: INSIGHT_RO_USER
Password: *******
Verify: *******

11. Click **Generate.**

    A dialog box to enter the password of the staging user (APR_STAGE user) appears.



Oracle Database Connect

User
APR_STAGE

Password: ********

12. Enter the password, and click **OK**.

    The system checks that Argus Insight and Argus Safety use the same character set. How the system continues depends on the result:

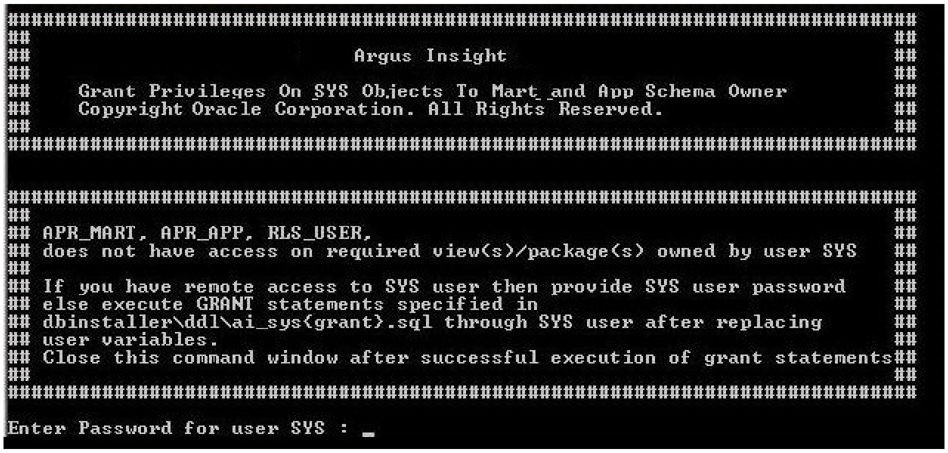
    - **Different Character Set —** If the character set for the Argus Insight database (that is, the MART character set) is different from the character set for the Argus Safety database, the system displays a warning message and prompts for confirmation that you want to proceed.

      Determine whether you want to continue with the schema creation.

      If the Argus Safety database uses the UTF character set and the Argus Insight database uses the ISO character set, the ETL process may fail due to the different character sets. In this case, Oracle recommends that you click **No,** fix the character set issue, and restart the create schema process.

If the Argus Safety database uses the ISO character set and the Argus Insight database uses the UTF character set, then the system can proceed by ignoring the character set difference. In this case, you can click **Yes.**

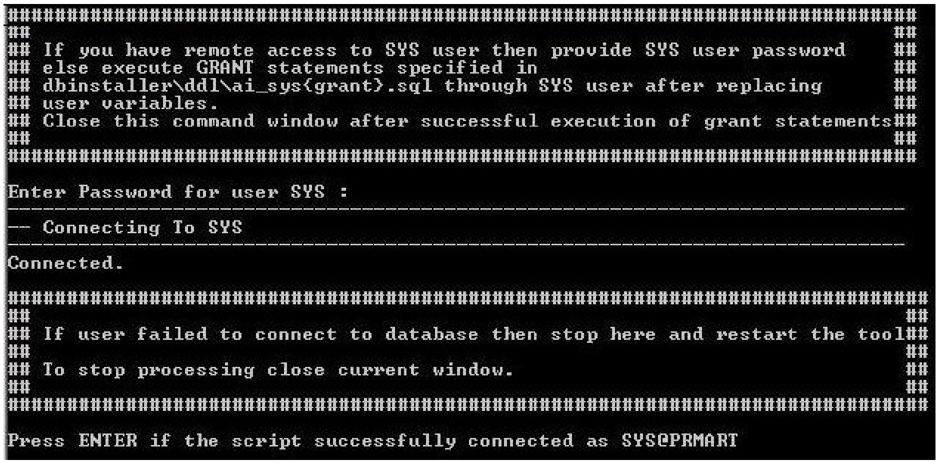
- **Same Character Set —** If the character set for the Argus Insight database is the same as the character set for the Argus Safety database, the following command prompt screen appears:



```
###############################################################################
##                                                                           ##
##                              Argus Insight                                ##
##                                                                           ##
##    Grant Privileges On SYS Objects To Mart and App Schema Owner           ##
##    Copyright Oracle Corporation. All Rights Reserved.                     ##
##                                                                           ##
###############################################################################


###############################################################################
##                                                                           ##
## APR_MART, APR_APP, RLS_USER,                                              ##
## does not have access on required view(s)/package(s) owned by user SYS     ##
##                                                                           ##
## If you have remote access to SYS user then provide SYS user password      ##
## else execute GRANT statements specified in                                ##
## dbinstaller\ddl\ai_sys{grant}.sql through SYS user after replacing        ##
## user variables.                                                           ##
## Close this command window after successful execution of grant statements##
##                                                                           ##
###############################################################################

Enter Password for user SYS : _
```

13. If you have remote access to the SYS user, enter the password for the SYS user, and press **Enter**.

    The command prompt screen appears.



```
###############################################################################
##                                                                           ##
## If you have remote access to SYS user then provide SYS user password      ##
## else execute GRANT statements specified in                                ##
## dbinstaller\ddl\ai_sys{grant}.sql through SYS user after replacing        ##
## user variables.                                                           ##
## Close this command window after successful execution of grant statements##
##                                                                           ##
###############################################################################

Enter Password for user SYS :
------------------------------------------------------------------------------
-- Connecting To SYS
------------------------------------------------------------------------------
Connected.

################################################################################
##                                                                            ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                            ##
## To stop processing close current window.                                   ##
##                                                                            ##
################################################################################

Press ENTER if the script successfully connected as SYS@PRMART
```

OR

If you **do not** have remote access to SYS user, then execute **ai_sys{grant}.sql** script through SYS user. This SQL script is located in the following folder

drive:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\DDL Folder

Open the **ai_sys{grant}.sql** file from the above mentioned location.

Execute all the GRANT statements after replacing the names of the variables with their corresponding Schema Owner name. For example:

- &mart_user. = APR_MART schema owner (APR_MART)

- &mart_app_user. = APR_APP schema owner (APR_APP)
- &rls_user. = VPD schema owner (RLS_USER)

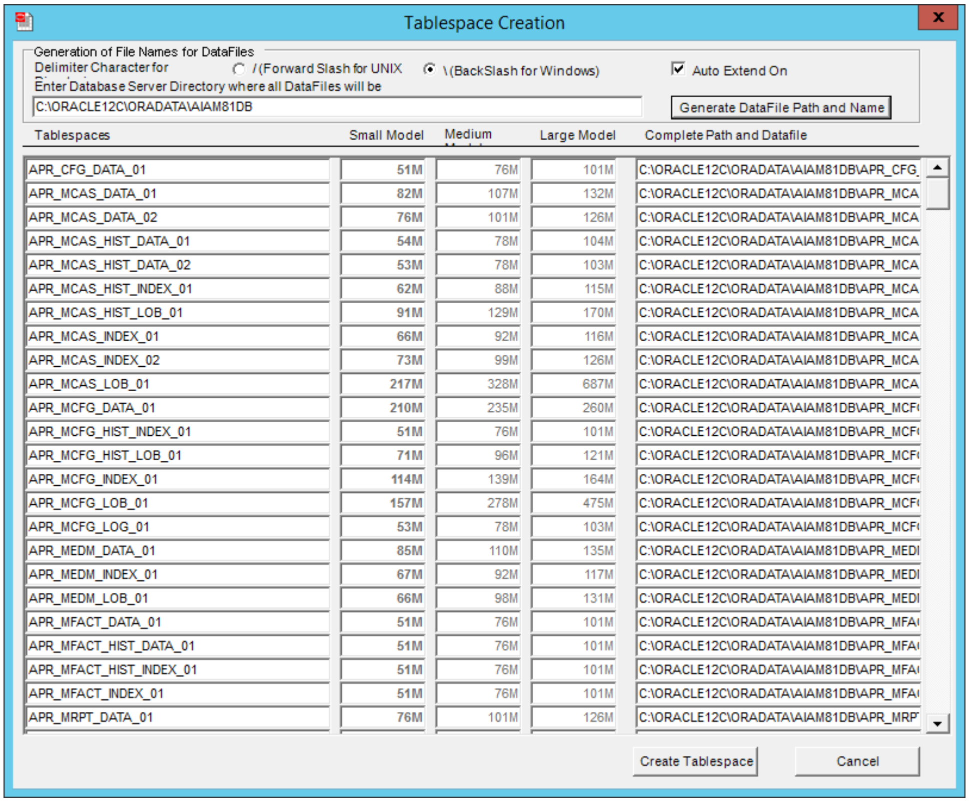
If you have already executed the **ai_sys{grant}.sql** script through SYS user, then go to Step17 of this procedure.

14. Verify that the script is successfully connected as <SYS User Name >@<Argus Insight Database Name>, and press **Enter**.

The command prompt screen with the Grant succeeded message appears multiple times along with the location of the log file.

15. Verify the location of the log file, and press **Enter**.

16. Wait until the **Tablespace Creation** dialog box appears.



Tablespace Creation

Generation of File Names for DataFiles

Delimiter Character for ○ /(Forward Slash for UNIX ● \(BackSlash for Windows) ☑ Auto Extend On

Enter Database Server Directory where all DataFiles will be

C:\ORACLE12C\ORADATA\AIAM81DB

Tablespaces	Small Model	Medium	Large Model	Complete Path and Datafile
APR_CFG_DATA_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_CFG_
APR_MCAS_DATA_01	82M	107M	132M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_DATA_02	76M	101M	126M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_HIST_DATA_01	54M	78M	104M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_HIST_DATA_02	53M	78M	103M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_HIST_INDEX_01	62M	88M	115M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_HIST_LOB_01	91M	129M	170M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_INDEX_01	66M	92M	116M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_INDEX_02	73M	99M	126M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCAS_LOB_01	217M	328M	687M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCA
APR_MCFG_DATA_01	210M	235M	260M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MCFG_HIST_INDEX_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MCFG_HIST_LOB_01	71M	96M	121M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MCFG_INDEX_01	114M	139M	164M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MCFG_LOB_01	157M	278M	475M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MCFG_LOG_01	53M	78M	103M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MCF
APR_MEDM_DATA_01	85M	110M	135M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MEDI
APR_MEDM_INDEX_01	67M	92M	117M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MEDI
APR_MEDM_LOB_01	66M	98M	131M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MEDI
APR_MFACT_DATA_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MFA
APR_MFACT_HIST_DATA_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MFA
APR_MFACT_HIST_INDEX_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MFA
APR_MFACT_INDEX_01	51M	76M	101M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MFA
APR_MRPT_DATA_01	76M	101M	126M	C:\ORACLE12C\ORADATA\AIAM81DB\APR_MRP

17. Complete the Tablespace Creation screen as follows:

a. In the **Enter Database Server Directory where all Data Files will be Created** field, enter the complete path to the directory for the tablespace data files that will be used by Argus Insight.

For example, /u01/app/oracle/SMTEST.

Note that the directory you specify must already exist.

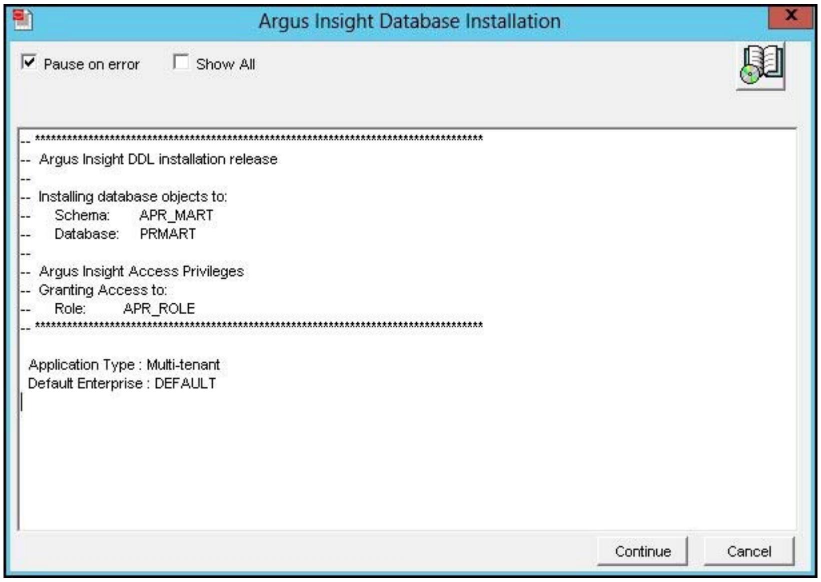
b. Click **Generate DataFile Path and Name.**

The Complete Path and Datafile column for all tablespaces are automatically filled.

Note that the system automatically selected the delimiter character to use for the directory path based on the Database Server operating system.

18. Click **Create Tablespace** to create all tablespaces.

19. Wait until the system creates the tablespaces and opens the Argus Insight Database Installation dialog box with the Application Type and the name of the default enterprise.



```
-- ********************************************************************************
-- Argus Insight DDL installation release
--
-- Installing database objects to:
--    Schema:     APR_MART
--    Database:   PRMART
--
-- Argus Insight Access Privileges
-- Granting Access to:
--    Role:       APR_ROLE
-- ********************************************************************************

 Application Type : Multi-tenant
 Default Enterprise : DEFAULT
```

20. Click **Continue** to start the schema creation.

    The system executes the scripts, displays status information during the schema creation process, and reports when the update is completed.

21. Click the **Book** icon to view the log file and check for errors.

    Alternatively, you can view the log file at any time at the following location:

    drive:\Argus_Insight_Working\AI81\Database\DBInstaller\CreateLog.rtf

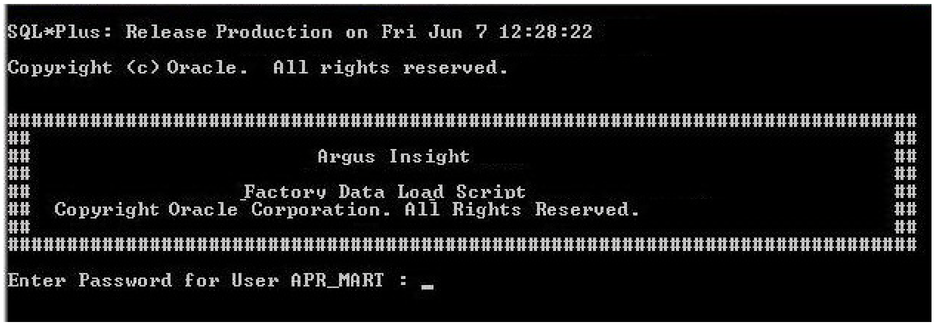
22. Click **Finish** to close the dialog box.

3.5.4 Loading Factory Data

To load the factory data:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Factory Data** to load the factory data.

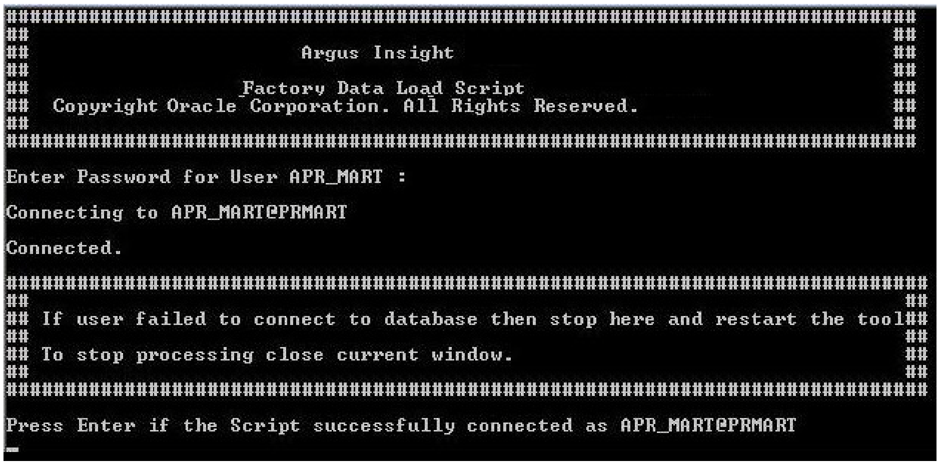
   The command prompt screen appears.



```
SQL*Plus: Release Production on Fri Jun 7 12:28:22

Copyright (c) Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                              Argus Insight                               ##
##                                                                          ##
##                        Factory Data Load Script                          ##
##  Copyright Oracle Corporation. All Rights Reserved.                      ##
##                                                                          ##
##############################################################################

Enter Password for User APR_MART : _
```

3. Enter the password for the **APR_MART** User, and press **Enter**.

   The command prompt screen appears.



```
##############################################################################
##                                                                          ##
##                          Argus Insight                                   ##
##                                                                          ##
##                      Factory Data Load Script                            ##
##   Copyright Oracle Corporation. All Rights Reserved.                     ##
##                                                                          ##
##############################################################################

Enter Password for User APR_MART :

Connecting to APR_MART@PRMART

Connected.

################################################################################
##                                                                            ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                            ##
## To stop processing close current window.                                   ##
##                                                                            ##
################################################################################

Press Enter if the Script successfully connected as APR_MART@PRMART
_
```

4. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name>, and press **Enter**.

   The row creation messages appears multiple times along with the name (insight_factory_data_log.txt) and location of the log file.

5. Press **Enter**.

   A message appears when the process to loading factory data is complete along with the location of the log file.

6. Click **OK** to return to the Schema Creation Tool screen.

3.6 Validating the Schema

To validate the database schema:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Schema Validation.**

   The Oracle Database Connect dialog box appears.

3. Connect to the Oracle Database:

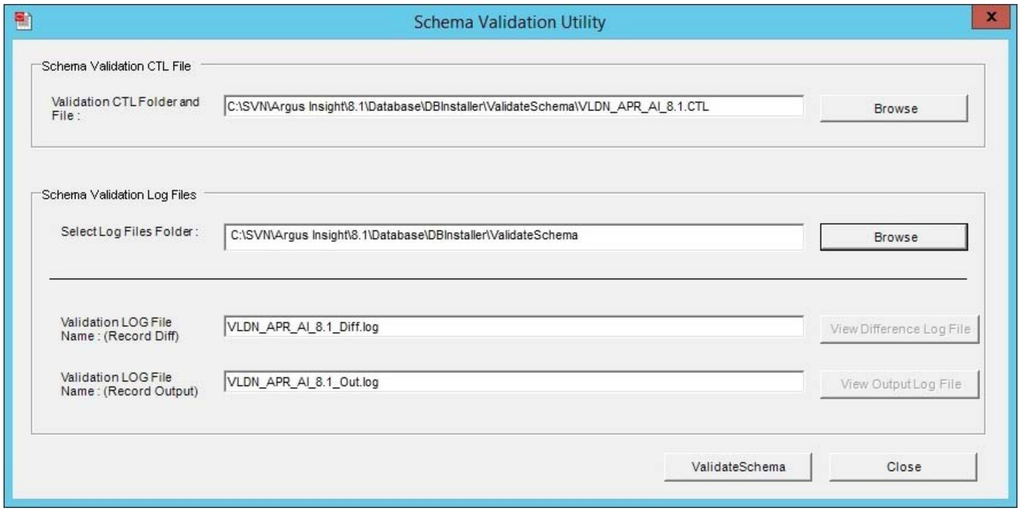
   a. In the **User** field, enter the name of the Argus Insight SYSTEM or DBA user.

   b. In the **Password** field, enter the password for the Argus Insight SYSTEM or DBA user.

   c. In the **Database** field, enter the name of the Argus Insight Data Mart instance.

   d. Click **OK.**

   The Schema Validation Utility dialog box appears.



Schema Validation Utility

Schema Validation CTL File

Validation CTL Folder and File : C:\SVN\Argus Insight\8.1\Database\DBInstaller\ValidateSchema\VLDN_APR_AI_8.1.CTL

Schema Validation Log Files

Select Log Files Folder : C:\SVN\Argus Insight\8.1\Database\DBInstaller\ValidateSchema

Validation LOG File Name : (Record Diff) VLDN_APR_AI_8.1_Diff.log

Validation LOG File Name : (Record Output) VLDN_APR_AI_8.1_Out.log

4. Complete the Schema Validation Utility dialog box as follows:

   a. For the **Validation CTL Folder and File** field, click **Browse** next to the field to navigate to the location of the CTL file that you want to verify. Select the CTL file, and then click **Open.**

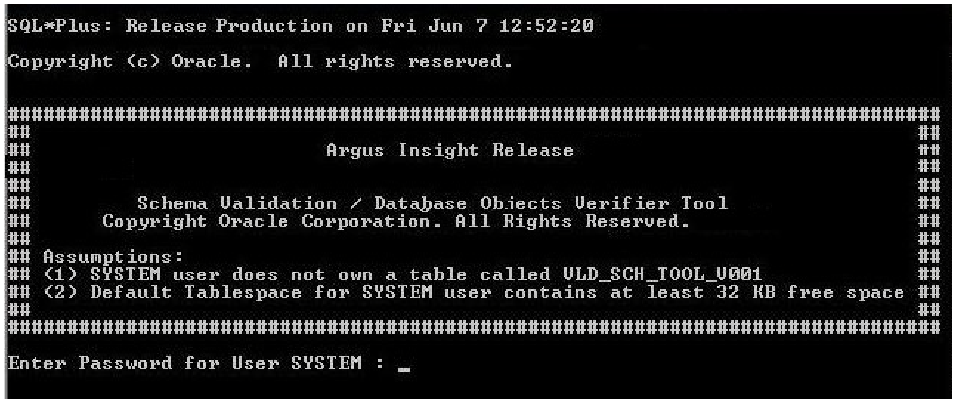
      You return to the Schema Validation Utility dialog box.

   b. For the **Select Log Files Folder** field, click **Browse** next to the field to navigate to and select the log files folder. Click **OK** to close the Select Folder dialog box and return to the Schema Validation Utility dialog box.

   Note that the default file names are automatically populated in the Validation LOG File Name (Record Diff) and Validation LOG File Name (Record Output) fields. You may change the log file names.

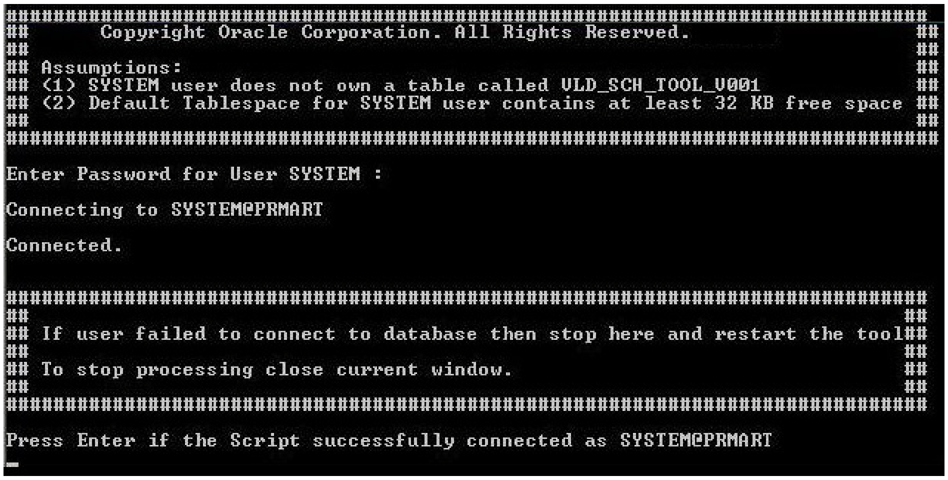
5. Click **Validate Schema.**

   The command prompt screen appears:



```
SQL*Plus: Release Production on Fri Jun 7 12:52:20

Copyright (c) Oracle.  All rights reserved.

################################################################################
##                                                                            ##
##                          Argus Insight Release                             ##
##                                                                            ##
##                                                                            ##
##         Schema Validation / Database Objects Verifier Tool                 ##
##      Copyright Oracle Corporation. All Rights Reserved.                    ##
##                                                                            ##
## Assumptions:                                                               ##
## (1) SYSTEM user does not own a table called VLD_SCH_TOOL_V001              ##
## (2) Default Tablespace for SYSTEM user contains at least 32 KB free space ##
##                                                                            ##
################################################################################

Enter Password for User SYSTEM : _
```

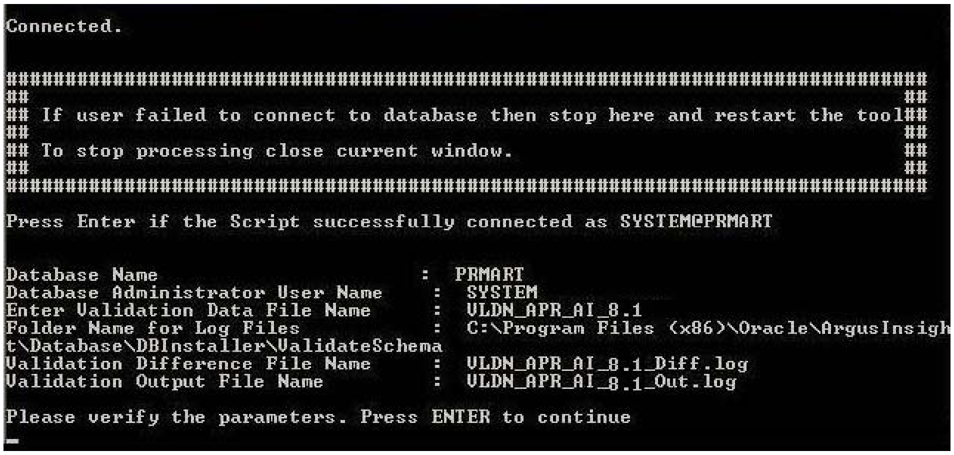
6. Enter the password for the Argus Insight SYSTEM or DBA user, and press **Enter**.



```
##############################################################################
##      Copyright Oracle Corporation. All Rights Reserved.                  ##
##                                                                          ##
## Assumptions:                                                             ##
## (1) SYSTEM user does not own a table called VLD_SCH_TOOL_V001            ##
## (2) Default Tablespace for SYSTEM user contains at least 32 KB free space ##
##                                                                          ##
##############################################################################

Enter Password for User SYSTEM :

Connecting to SYSTEM@PRMART

Connected.


##############################################################################
##                                                                        ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                        ##
## To stop processing close current window.                               ##
##                                                                        ##
##############################################################################

Press Enter if the Script successfully connected as SYSTEM@PRMART
_
```

7. Verify that the script is successfully connected as <SYSTEM/DBA User Name>@<Argus Insight Database Name>, and press **Enter**.

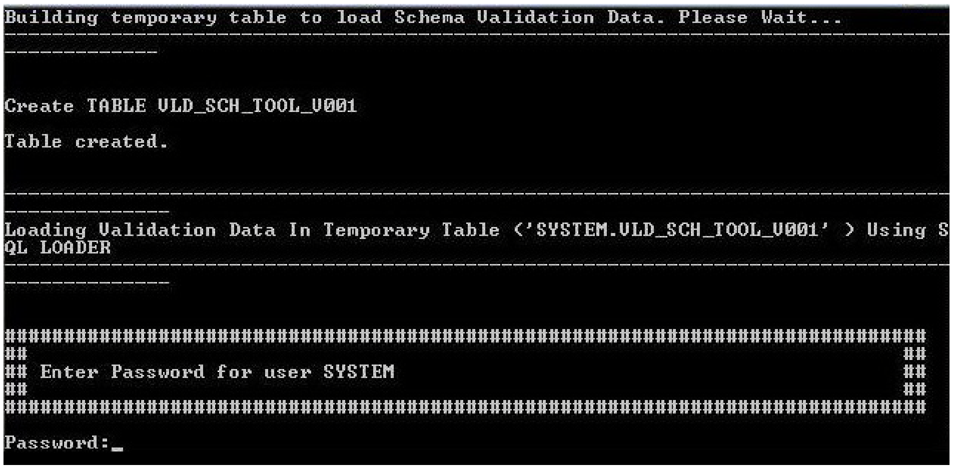
   The command prompt screen appears with the Database Name, Database Administrator User Name, Validation File Name, and the Folder Name for Log Files.



```
Connected.


##############################################################################
##                                                                        ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                        ##
## To stop processing close current window.                               ##
##                                                                        ##
##############################################################################

Press Enter if the Script successfully connected as SYSTEM@PRMART


Database Name                       :  PRMART
Database Administrator User Name    :  SYSTEM
Enter Validation Data File Name     :  VLDN_APR_AI_8.1
Folder Name for Log Files           :  C:\Program Files (x86)\Oracle\ArgusInsigh
t\Database\DBInstaller\ValidateSchema
Validation Difference File Name     :  VLDN_APR_AI_8.1_Diff.log
Validation Output File Name         :  VLDN_APR_AI_8.1_Out.log

Please verify the parameters. Press ENTER to continue
_
```

8. Review the information on the command prompt screen, and press **Enter.**

   The next command prompt screen appears.



```
Building temporary table to load Schema Validation Data. Please Wait...
--------------------------------------------------------------------------------
-------------


Create TABLE VLD_SCH_TOOL_V001

Table created.


--------------------------------------------------------------------------------
--------------
Loading Validation Data In Temporary Table ('SYSTEM.VLD_SCH_TOOL_V001' ) Using S
QL LOADER
--------------------------------------------------------------------------------
--------------


##############################################################################
##                                                                        ##
## Enter Password for user SYSTEM                                         ##
##                                                                        ##
##############################################################################

Password:_
```

9. Enter the password for the Argus Insight SYSTEM or DBA user, and press **Enter**.

10. Press **Enter** again on the next screen.

    A message appears stating that the validation of the Argus Insight Database is completed.

11. Click **OK.**

When the system returns to the Schema Validation Utility dialog box:

- To check for any schema discrepancies, such as missing objects, click **View Difference Log File**.
- To see the list of errors, if any, which occurred during schema validation, click **View Output Log File**.
- To close the dialog box, click **Close**.

If Argus Insight read-only user is created, then ignore the schema validation differences, where:

- Objects are R_% views/columns
- GRANTEE is Argus Insight Read-only user

3.7 Creating a Database Link from Argus Safety to Insight Database

This link allows real-time updates of some of the values from Argus Console to Argus Insight data mart.

To create the database link from the Argus Safety database to the Argus Insight database:

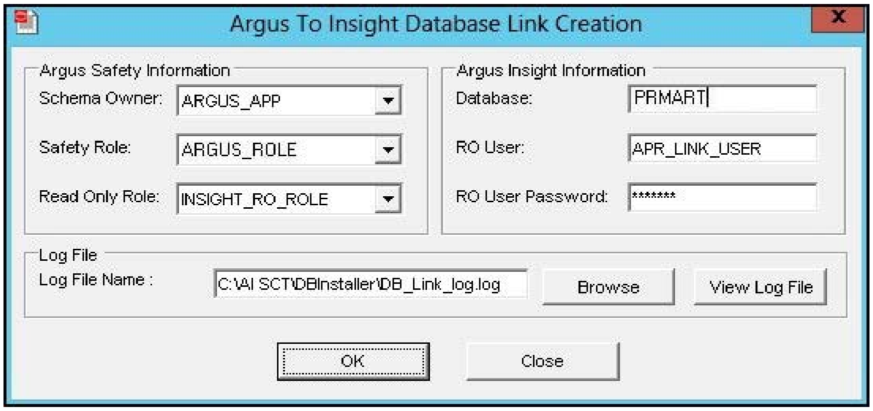
1. Start the Argus Insight Schema Creation Tool.
2. Click **Argus DBLink.**
3. Connect to the Oracle Database:

   a. In the **Password** field, enter the password for the Argus Safety SYSTEM or DBA user.

   b. In the **Argus Safety Database** field, enter the name of your Argus Safety database.

   c. Click **OK.**

   The Argus To Insight Database Link Creation dialog box appears.



Argus To Insight Database Link Creation

Argus Safety Information

Schema Owner: ARGUS_APP

Safety Role: ARGUS_ROLE

Read Only Role: INSIGHT_RO_ROLE

Argus Insight Information

Database: PRMART

RO User: APR_LINK_USER

RO User Password: *******

Log File

Log File Name : C:\AI SCT\DBInstaller\DB_Link_log.log

4. Complete the fields in the Argus Safety Information section as follows:

a. In the **Schema Owner** field, select the user account that owns the Argus Safety schema.

b. In the **Safety Role** field, select the Argus Safety role.

c. In the **Read Only Role** field, select the **INSIGHT_RO_ROLE,** which was created in Argus Safety.

5. Complete the fields in the Argus Insight Information section as follows:

   a. In the **Database** field, enter the name of the Argus Insight database.

   b. In the **RO User** field, enter the name of the read-only user.

      See step 8 (a) of the Section 3.5, "Creating the Database Schema" section (**APR_LINK_USER**).

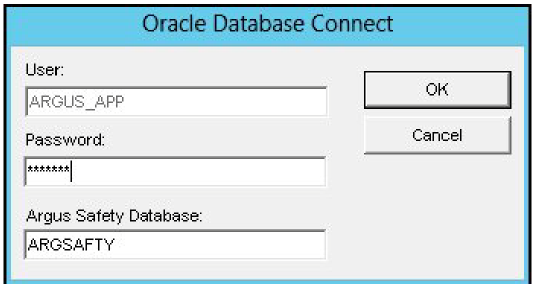
   c. In the **RO User Password** field, enter the password for the read-only user.

6. Click the **Log File Name** field to specify the name of the log file that will store the DBLink creation information.

   You may click **Browse** to navigate to the file location, select the file, and **Save** your selection.

7. Click **OK** to create the database link.

   A dialog box appears to enter the information required to connect to the database as the **ARGUS_APP** user.



Oracle Database Connect

User: ARGUS_APP

Password: *******

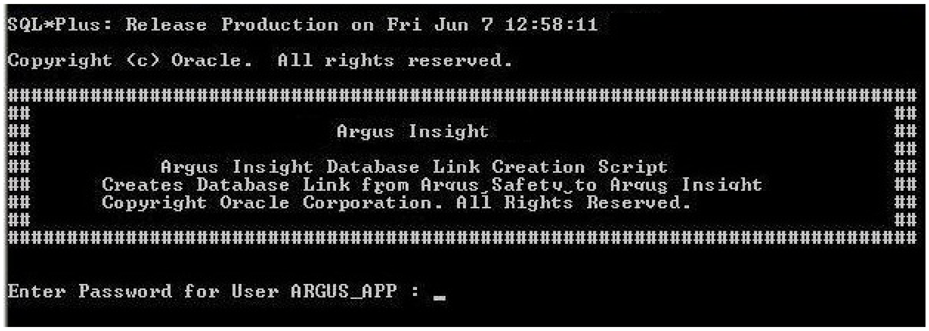
Argus Safety Database: ARGSAFTY

8. Enter the **ARGUS_APP** password and the Argus Safety database information. Click **OK.**

   A dialog box appears to enter the information to connect to the database as the Argus Safety SYSTEM or DBA user.

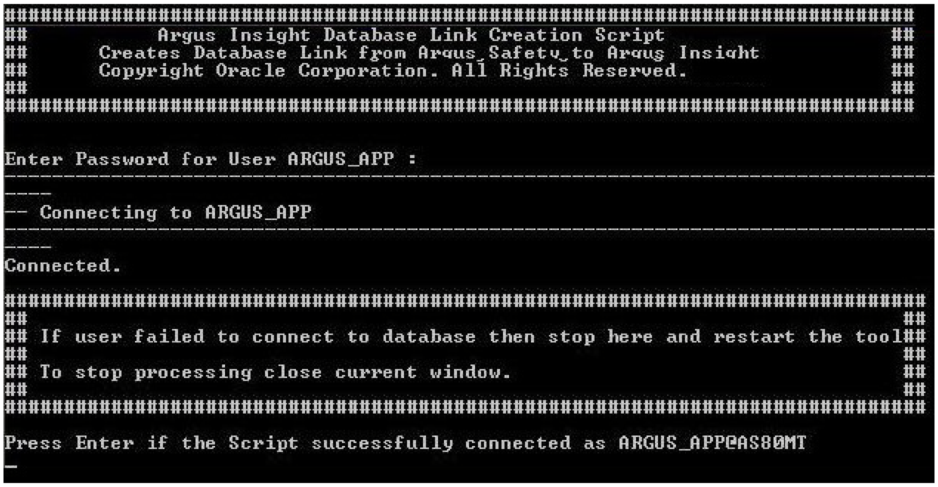
9. Enter the password for the Argus Safety SYSTEM or DBA user, and click **OK.**

   The command prompt screen appears.



```
SQL*Plus: Release Production on Fri Jun 7 12:58:11

Copyright (c) Oracle.  All rights reserved.

############################################################################
##                                                                        ##
##                            Argus Insight                               ##
##                                                                        ##
##              Argus Insight Database Link Creation Script               ##
##         Creates Database Link from Argus_Safety_to Argus Insight       ##
##         Copyright Oracle Corporation. All Rights Reserved.             ##
##                                                                        ##
############################################################################

Enter Password for User ARGUS_APP : _
```

10. Enter the password for the **ARGUS_APP** user, and press **Enter**.



```
##############################################################################
##           Argus Insight Database Link Creation Script                    ##
##      Creates Database Link from Argus_Safety_to Argus Insight            ##
##      Copyright Oracle Corporation. All Rights Reserved.                  ##
##                                                                          ##
##############################################################################


Enter Password for User ARGUS_APP :
--------------------------------------------------------------------------------
----
-- Connecting to ARGUS_APP
--------------------------------------------------------------------------------
----
Connected.

###############################################################################
##                                                                          ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                          ##
## To stop processing close current window.                                 ##
##                                                                          ##
###############################################################################

Press Enter if the Script successfully connected as ARGUS_APP@AS80MT
_
```

11. Verify that the script is successfully connected as <ARGUS_APP User Name>@<Argus Safety Database Name>, and press **Enter**.

12. Press **Enter** again.

    Wait until a message appears stating that the Argus Safety to Argus Insight database link is created successfully along with location of the log file.

13. Click **OK.**

14. Check the log files located in the following folder for status information:

    drive:\Program Files\Oracle\ArgusInsight\Database\DBInstaller

15. Click **Close** to close the Argus To Insight Database Link Creation dialog box.

3.8 Upgrading Database from Argus Insight 8.0 to Argus Insight 8.1

To upgrade the database from Argus Insight 8.0 to Argus Insight 8.1:

1. Start the Argus Insight Schema Creation Tool.

2. Click **DB Upgrade.**

   The Oracle Database Connect dialog box appears.

3. Connect to the Oracle Database:

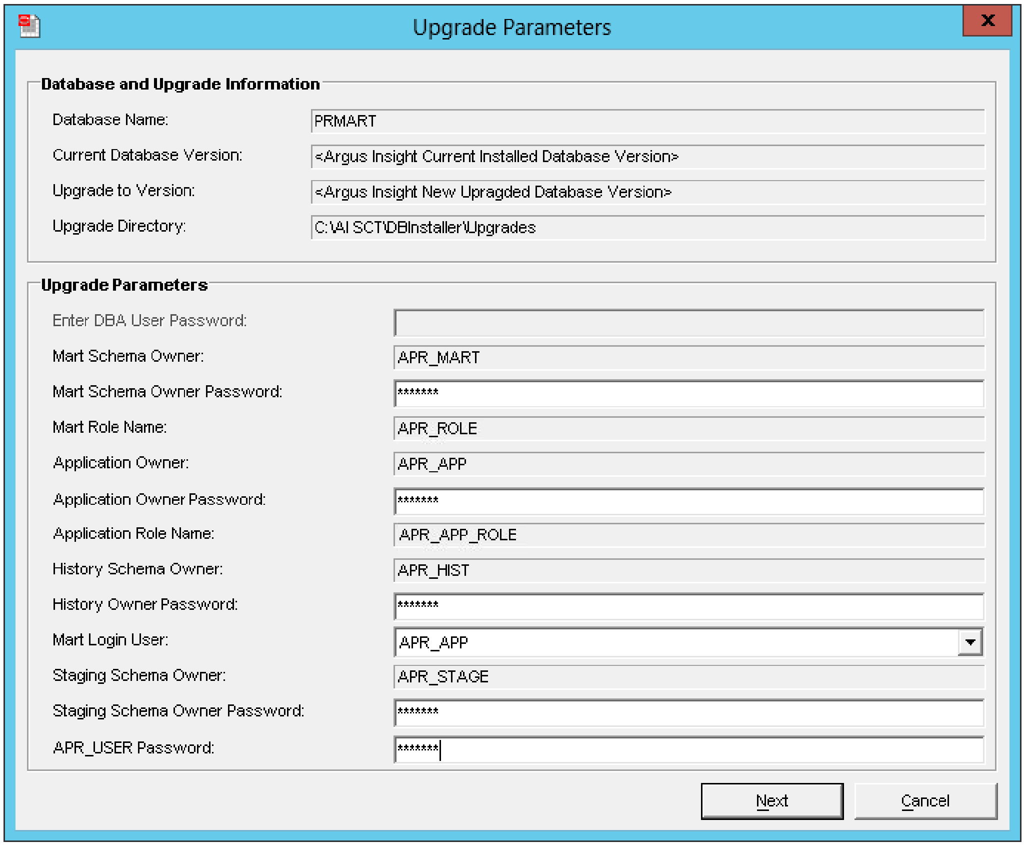
   a. In the **User** field, enter the name of the Argus Insight SYSTEM or DBA user.

   b. In the **Password** field, enter the password for the Argus Insight SYSTEM or DBA user.

   c. In the **Database** field, enter the name of your Argus Insight database.

   d. Click **OK.**

      The Upgrade Parameters dialog box appears.


Upgrade Parameters

Database and Upgrade Information

Database Name: PRMART

Current Database Version: <Argus Insight Current Installed Database Version>

Upgrade to Version: <Argus Insight New Upragded Database Version>

Upgrade Directory: C:\AI SCT\DBInstaller\Upgrades

Upgrade Parameters

Enter DBA User Password:

Mart Schema Owner: APR_MART

Mart Schema Owner Password: *******

Mart Role Name: APR_ROLE

Application Owner: APR_APP

Application Owner Password: *******

Application Role Name: APR_APP_ROLE

History Schema Owner: APR_HIST

History Owner Password: *******

Mart Login User: APR_APP

Staging Schema Owner: APR_STAGE

Staging Schema Owner Password: *******

APR_USER Password: *******

4. Complete the Upgrade Parameters dialog box as follows:

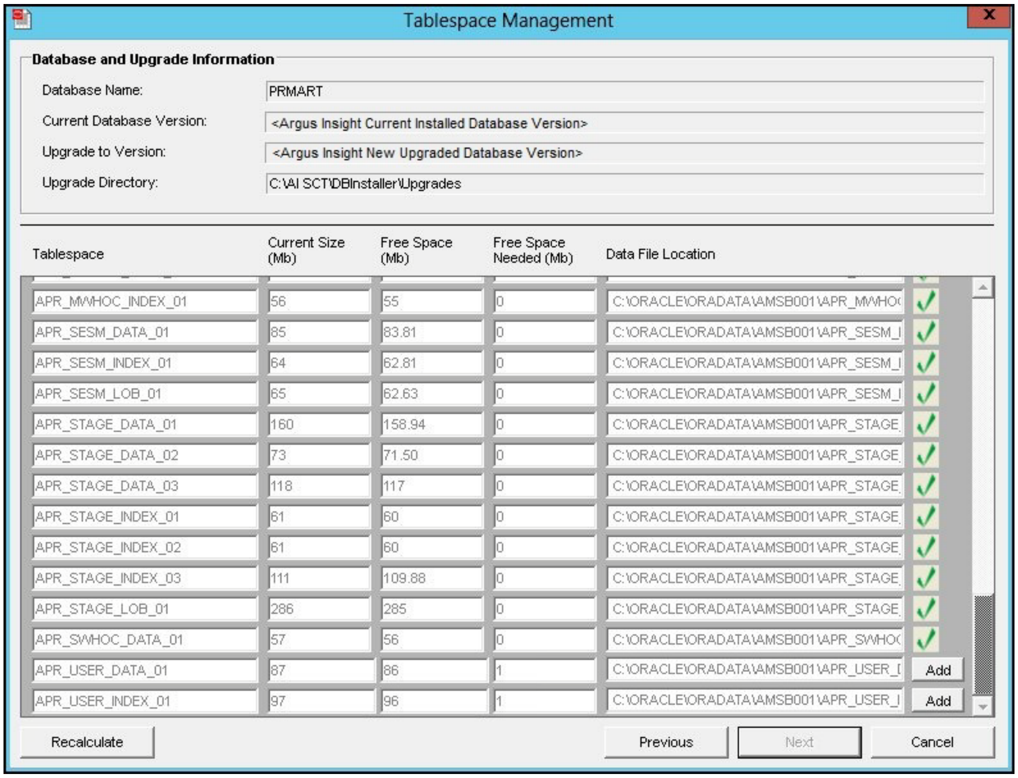
   a. In the top section, verify that the database and upgrade information is correct. If the information is incorrect, click **Cancel.**

   b. In the Upgrade Parameters section, enter the correct password for each owner and user.

   c. In the **Mart Login User** field, select the user defined as mart login user (APR_LOGIN user).

5. Click **Next.**

   The Tablespace Management dialog box appears.



Database and Upgrade Information

Database Name: PRMART

Current Database Version: <Argus Insight Current Installed Database Version>

Upgrade to Version: <Argus Insight New Upgraded Database Version>

Upgrade Directory: C:\AI SCT\DBInstaller\Upgrades

Tablespace	Current Size (Mb)	Free Space (Mb)	Free Space Needed (Mb)	Data File Location	
APR_MWHOC_INDEX_01	56	55	0	C:\ORACLE\ORADATA\AMSB001\APR_MWHO(	✓
APR_SESM_DATA_01	85	83.81	0	C:\ORACLE\ORADATA\AMSB001\APR_SESM_I	✓
APR_SESM_INDEX_01	64	62.81	0	C:\ORACLE\ORADATA\AMSB001\APR_SESM_I	✓
APR_SESM_LOB_01	65	62.63	0	C:\ORACLE\ORADATA\AMSB001\APR_SESM_I	✓
APR_STAGE_DATA_01	160	158.94	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_DATA_02	73	71.50	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_DATA_03	118	117	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_INDEX_01	61	60	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_INDEX_02	61	60	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_INDEX_03	111	109.88	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_STAGE_LOB_01	286	285	0	C:\ORACLE\ORADATA\AMSB001\APR_STAGE	✓
APR_SWHOC_DATA_01	57	56	0	C:\ORACLE\ORADATA\AMSB001\APR_SWHO(	✓
APR_USER_DATA_01	87	86	1	C:\ORACLE\ORADATA\AMSB001\APR_USER_I	Add
APR_USER_INDEX_01	97	96	1	C:\ORACLE\ORADATA\AMSB001\APR_USER_I	Add

6. Verify that all tablespaces have enough free space.

   The green check mark indicates that the tablespace has enough free space.

   If the tablespace does not have enough free space, increase the size of the tablespace by below mentioned methods:

   - To add a new datafile to the existing tablespace, click **Add**.

     A dialog box appears to add a name for the new datafile, containing the required additional space.

     Note: In case no datafile exists for any tablespace, click **Create**.

     A dialog box appears to create a new datafile containing the tablespace information.

   - Alternatively, if you do not wish to add a new data file, the database administrator can resize the tablespace from the back-end.

     After resizing, click the **Recalculate** button to re-evaluate the tablespace size and refresh the tablespace grid, as per the updated tablespace size.

     Once updated, the **Add or Create** button will not be displayed and the green check mark will be displayed, indicating that the tablespace has enough free space.

7. Click **Next.**

   The Argus Insight Database Upgrade dialog box appears.

8. Click **Continue** to start the upgrade process.

During the upgrade process, the system loads the factory data, and then displays a message reminding you to check the Factory_Data folder for any .BAD files.

9. Click **OK** to continue.

   The system executes the upgrade scripts, displays status information during the update, and reports when the update is completed.

10. Click the **Book** icon to view the log file, and check for errors.

    Alternatively, you can view the log file at any time at the following location:

    drive:\Program Files\Oracle\ArgusInsight\Database\Upgrades\UpgradeLog.rtf

11. Click **Finish**.

Post-upgrade Steps

When you have upgraded the database from Argus Insight 8.0 to Argus Insight 8.1, you must:

1. Re-create the read-only user in the Argus Safety database using the steps given in Section 3.5.1, "Creating Users and Roles in the Argus Safety Database".
2. Re-create the database links.
3. Re-run the Initial ETL.

3.9 Running Additional Grant Scripts for Single DB Instance

If Argus Insight and Argus Mart are running on the same database, execute the following:

Database\Utils\am_grants.bat

Note:

- During execution of the utility, if a prompt appears to enter the user details, then enter Argus Insight DBA user and password.
- After execution of the utility, Argus Insight schema validation file will reflect additional privileges.

3.10 Creating Argus Insight Read-Only User

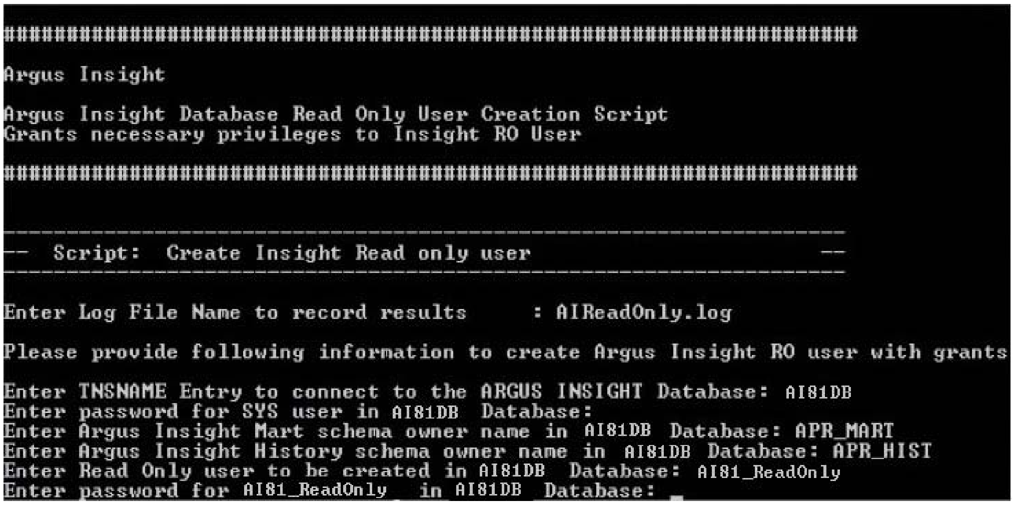
You can create a read-only schema in Argus Insight. This schema will have read-only (SELECT) access on all the tables and views of the APR_MART and APR_HIST schema. Besides, this read-only schema can also be used for customized reporting purpose.

To create Argus Insight Read-only user:

1. From the Utils folder, double click the AI_RO_USER.bat file.
2. Enter the following inputs:
   a. Name of the Log file
   b. Name of Argus Insight database
   c. Password of the SYS user
   d. Name of Argus Insight Mart schema user (for example, APR_MART)
   e. Name of the History schema user (for example, APR_HIST)

f. Name of Argus Insight Read-only user that you want to create

g. Password of Argus Insight Read-only user



```
####################################################################

Argus Insight

Argus Insight Database Read Only User Creation Script
Grants necessary privileges to Insight RO User

####################################################################


-------------------------------------------------------------------
--  Script:  Create Insight Read only user                       --
-------------------------------------------------------------------

Enter Log File Name to record results      : AIReadOnly.log

Please provide following information to create Argus Insight RO user with grants

Enter TNSNAME Entry to connect to the ARGUS INSIGHT Database: AI81DB
Enter password for SYS user in AI81DB  Database:
Enter Argus Insight Mart schema owner name in AI81DB  Database: APR_MART
Enter Argus Insight History schema owner name in  AI81DB  Database: APR_HIST
Enter Read Only user to be created in AI81DB  Database: AI81_ReadOnly
Enter password for AI81_ReadOnly  in AI81DB  Database: _
```

On successful connection to the SYS user, the script provides read-only access on objects of Argus Insight schema to the read-only user.

4

Configuring the Argus Insight Application

This chapter provides information about configuring the Argus Insight application and the Argus Insight scheduling service.

This chapter includes the following topics:

- Logging In to Argus Insight for Configuration and Setup
- Configuring the Argus Insight Application Profile Switches
- Configuring Duration Value Bands
- Configuring Derivation Functions
- Configuring the Argus Insight Windows Service
- Configuring the IIS File Download Limit
- Using Export and Import to Copy Configuration Data
- Using Argus Safety to Configure Enterprises for Argus Insight
- Securing Sensitive Configuration and Operational Data

4.1 Logging In to Argus Insight for Configuration and Setup

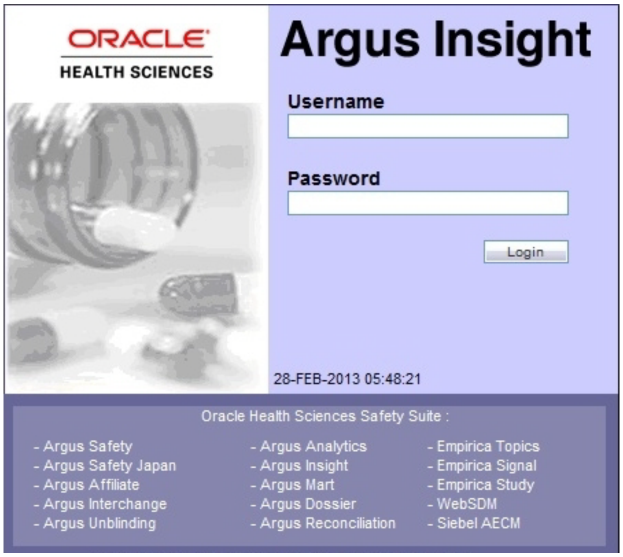
To log in to the Argus Insight application:

1. Log in with rights to a workstation from where you can access the Argus Insight application.
2. Start Internet Explorer.
3. In the Address bar, enter the following URL to start the Argus Insight:

   ```
   http://Argus_Insight_WebServer_Name:port_number/default.asp
   ```

4. Press **Enter.**

   The Argus Insight Login screen appears.



28-FEB-2013 05:48:21

Oracle Health Sciences Safety Suite :

- Argus Safety
- Argus Safety Japan
- Argus Affiliate
- Argus Interchange
- Argus Unblinding
- Argus Analytics
- Argus Insight
- Argus Mart
- Argus Dossier
- Argus Reconciliation
- Empirica Topics
- Empirica Signal
- Empirica Study
- WebSDM
- Siebel AECM

5. Log in to the Argus Insight application:

   a. In the **User Name** field, enter **admin.**

   b. In the **Password** field, enter the password for the admin user.

      This password is the same as the password of the admin user in Argus Safety.

   c. Click **Login.**

Note: If you are using a Single Sign On (SSO) environment, you must ensure that SSO tools such as OAM are disabled on the Argus Insight Web Server for initial configuration. The only administrator user in Argus Insight is a non-LDAP user. A non-LDAP user cannot log in to Argus Insight with SSO tools set to Enabled.

Note: In case of a multi-tenant setup, you must ensure that the entire configuration is done using the default enterprise.

- This will help in copying the configuration to a different enterprise
- All the global configuration is available in the default enterprise.

4.2 Configuring the Argus Insight Application Profile Switches

Profile switches are a collection of settings that let you configure the default behavior of the system. This section describes the profile switches that you must set to establish connectivity with your Business Intelligence tool and to run the initial ETL.

For detailed information about all the profile switches, see:

- *Oracle Argus Insight CMN Profile Enterprise Table Guide* (CMN_PROFILE_ENTERPRISE.pdf)
- *Oracle Argus Insight CMN Profile Global Table Guide* (CMN_PROFILE_GLOBAL.pdf)

4.2.1 Accessing and Modifying the Profile Switches

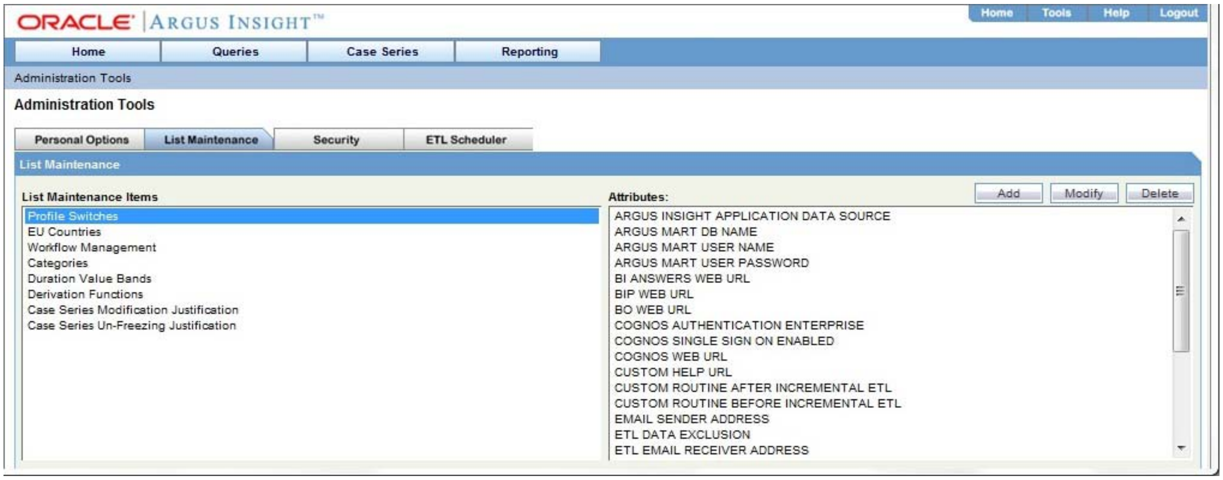
To access and modify the Argus Insight profile switches:

1. Log in to the Argus Insight application.
2. On the Argus Insight home page, from the upper-right corner, click the **Tools** tab.

   The Administration Tools screen appears.
3. Click the **List Maintenance** tab.
4. From the List Maintenance Items group, select **Profile Switches**.

   The Attributes group is updated with the profile switches that you may configure. See Figure 4–1.

Figure 4–1 List Maintenance Tab with the Profile Switches



List Maintenance Items

- Profile Switches
- EU Countries
- Workflow Management
- Categories
- Duration Value Bands
- Derivation Functions
- Case Series Modification Justification
- Case Series Un-Freezing Justification

Attributes:

- ARGUS INSIGHT APPLICATION DATA SOURCE
- ARGUS MART DB NAME
- ARGUS MART USER NAME
- ARGUS MART USER PASSWORD
- BI ANSWERS WEB URL
- BIP WEB URL
- BO WEB URL
- COGNOS AUTHENTICATION ENTERPRISE
- COGNOS SINGLE SIGN ON ENABLED
- COGNOS WEB URL
- CUSTOM HELP URL
- CUSTOM ROUTINE AFTER INCREMENTAL ETL
- CUSTOM ROUTINE BEFORE INCREMENTAL ETL
- EMAIL SENDER ADDRESS
- ETL DATA EXCLUSION
- ETL EMAIL RECEIVER ADDRESS

> **Note:** When the Argus Insight Database Source profile switch is set to **Argus Mart**, then in the List Maintenance section, only **Profile Switches** and **Case Series Modification Justification** list maintenance items are available.
>
> For more information on this profile switch, see Section 4.2.4, "Setting the Attributes Specific ONLY to Argus Mart".

4.2.2 Setting the Populate Data Attributes

You may control data population based on data attributes.

The following is the list of profile switch along with their value required to be set to populate data attributes.

Table 4–1 Populate Data Attribute-Value set

Attribute	Value
POPULATE AFFILIATE DATA	0 — Do not bring any affiliate data into the Insight data mart. 1 — Bring all affiliate data into the Insight data mart.

Table 4–1 (Cont.) Populate Data Attribute-Value set

Attribute	Value
POPULATE INTERCHANGE DATA	0 — Do not bring any interchange data into the Insight data mart. 1— Bring all interchange data into the Insight data mart. 2 — Bring only the SAFETYREPORT, MESSAGES, and EDI_INFO tables data into the Insight data mart.
POPULATE CASE/CONFIGURATION DATA	0 — Populate configuration data only. 1 — Populate all the data (both case and configuration data).
LEGACY REPORTS CONFIGURATION	0 — Configuration items are not visible. 1— Configuration items are visible. **Note**: If Legacy Reports Configuration switch is set to 1, then legacy reports switches becomes available for obsolete reports, and you must configure the following switches: ■ POPULATE NARRATIVE LANGUAGES TABLE ■ COMPANY LOGO PATH ■ DAYS TO LOCK ■ UDN COLUMN FOR SUPPLIER NAME ■ FOLLOW-UP ACTION CODE ■ POPULATE DLL SLL REPORTS TABLE DATA To configure these switches, refer to Argus Insight 7.0.2 Installation Guide.

To set the data attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   > **Note:** See Table 4–1, " Populate Data Attribute-Value set".

4. In the **Value** field, enter a numeric value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

4.2.3 Setting the Email Attributes

You may configure the profile switches that relate to sending and receiving email after an extract, transform, and load (ETL) operation has completed, as well as sending email for scheduled reports.

The following is the list of profile switch along with their value required to be set for email messages and delivery.

Table 4–2 Email Specific Attribute-Value set

Attribute	Value
ETL EMAIL SETUP	0 — Send no email message after an ETL operation. 1 — Send an email message only if an initial or incremental ETL fails. 2 — Send an email message only if an initial or incremental ETL succeeds. 3 — Send an email message after any initial or incremental ETL (failure or success).
ETL EMAIL RECEIVER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry. If the Value field blank, then no email messages are sent.
EMAIL SENDER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry. If the Value field blank, then no email messages are sent.
FAILED RECIPIENTS STATUS EMAIL ADDRESS	Specify the email address of the user who will receive information about undeliverable emails.

To configure the attributes related to email messages and delivery:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   > **Note:** See Table 4–2, " Email Specific Attribute-Value set".

4. In the **Value** field, enter a value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

4.2.4 Setting the Attributes Specific ONLY to Argus Mart

Argus Insight supports queries for analysis of the historical case data based on specific date/time through Argus Mart. To enable access to this data in Argus Mart, you need to set specific attributes.

The following is the list of profile switch along with their value required to be set to populate Argus Insight data into Argus Mart database.

Table 4–3 Argus Mart Specific Attribute-Value set

Attribute	Value
Argus Insight Application Data Source	Enables you to configure the data source for Argus Insight. You may run your queries for Argus Insight or Argus Mart depending on the value configured in this switch. **Argus Mart** — Enable queries on Argus Mart data source only. **Insight Mart** — Enable queries on Argus Insight data source only. **Both** (Insight Mart and Argus Mart) — You may choose between Insight Mart and Argus Mart data sources for creating and executing your queries. All the queries and case series created on these data sources can be identified in the application.
ARGUSMARTDBNAME	Specify the database instance name for the Argus Mart data mart. This information enables to connect Argus Insight with Argus Mart database.
ARGUS MART USER NAME	Specify the schema user created for Argus Insight in Argus Mart database. This user may perform all the background functions from Argus Insight application to Argus Mart database including querying and reporting.
ARGUS MART USER PASSWORD	Specify the password of the schema user created for Argus Insight in Argus Mart database that is, the password of user configured in ARGUS MART USER NAME.
ENABLE_AI_PROCESSING	**Note:** Use Argus Safety Console to enable this profile switch. This profile switch must be set to **Yes** to link Argus Insight database to Argus Mart database. Yes — Enable Argus Insight Processing for Argus Mart. No — Disable Argus Insight Processing for Argus Mart.

Note: These profile switches are optional and should be configured only if you want to run Advanced Conditions on Argus Mart database.

Argus Mart database TNS should be added in the Argus Insight Web Server TNS and Argus Insight Database Server TNS.

Argus Insight Database Server TNS should be added in the Argus Mart Database TNS.

To set these attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   Note: See Table 4–3, " Argus Mart Specific Attribute-Value set".

4. In the **Value** field, enter a value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

5. Log on to Argus Safety Console in separate window, and set ENABLE_AI_PROCESSING profile switch to **Yes**.

4.2.5 Setting the Attributes Specific ONLY to BIP

If you are using BIP as your Business Intelligence tool with Argus Insight, you need to set the following BIP-specific attributes:

- BIP WEB URL
- KEEP REPORT DATA

To define the attributes required for BIP:

1. On the Administration Tools page, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select **BIP WEB URL**.

   a. Click **Modify.**

      The Modify Attribute dialog box appears.

   b. In the **Value** field, enter the name of the BIP Web URL to open the BIP home page.

      This URL can be the BI Publisher URL for standalone BI Publisher server or the Load Balancer URL configured for multiple BI Publisher servers. If BI Publisher is configured for SSL, you must use https with the URL. For example:

      https://<server name>:<Port Number>/xmlpserver

   c. Click **OK** to save the changes and return to the List Maintenance tab.

4. From the Attributes group, select **KEEP REPORT DATA**.

   This attribute is used to determine if the report log tables needs to be populated or not.

   a. Click **Modify.**

      The Modify Attribute dialog box appears.

   b. In the **Value** field, enter **Yes** or **No**.

      The value **Yes** denotes that the Report Log tables should be populated. The value **No** denotes that the Report Log tables should not be populated

   c. Click **OK** to save the changes and return to the List Maintenance tab.

4.2.6 Setting the Attributes Specific ONLY to OBIEE

If you are using OBIEE with Argus Insight, you need to set the OBIEE specific attributes:

- BI ANSWERS WEB URL

To define the attributes required for OBIEE:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select BI ANSWERS WEB URL, and click **Modify**.

   The Modify Attributes dialog box appears.

4. In the **Value** field, enter the path for the BI ANSWERS WEB URL.

   For example, this path can be the OBIEE URL:

   https://<server name>:<Port Number>/analytics

5. Click **OK**.

   The profile switch is set and you return to List Maintenance tab.

4.2.7 Setting the Attributes Specific ONLY to BusinessObjects

If you are using BusinessObjects as your Business Intelligence tool with Argus Insight, you need to set the attributes for BusinessObjects Servers for **BusinessObjects configurations only**.

To define the attributes required for the **BusinessObjects Servers**:

1. On the Administration Tools page, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. Define the BusinessObjects Server Web URL that Argus Insight uses:

   a. From the Attributes group, select **BO WEB URL**.

   b. Click **Modify.**

      The Modify Attribute dialog box appears.

   c. In the **Value** field, enter either the IP address or the host name of the BusinessObjects Server.

      In addition, specify the cluster name if you are using the BusinessObjects clustering feature.

      > **Note:** In the case of a single-server environment (that is, Argus Insight and BusinessObjects are hosted on the same server), you must enter the IP address to avoid problems when accessing the BusinessObjects home page. These problems may be caused due to the session interference of Argus Insight and BusinessObjects web application.

   d. Click **OK** to save the changes and return to the List Maintenance tab.

4.2.8 Setting the Attributes Specific ONLY to Cognos

If you are using Cognos as your Business Intelligence tool with Argus Insight, you need to set the Cognos-specific attributes.

The following is the list of profile switch along with their value required to be set for Cognos.

Table 4–4 Cognos Specific Attribute-Value set

Attribute	Value
COGNOS AUTHENTICATION ENTERPRISE	Select the Enterprise Short Name from which all users are authenticated for Cognos login.

Table 4–4 (Cont.) Cognos Specific Attribute-Value set

Attribute	Value
COGNOS WEB URL	Specify the name of the Cognos Web URL for opening the Cognos home page. This URL can be the Cognos URL for standalone Cognos server or the Load Balancer URL configured for multiple Cognos servers. If Cognos is configured for SSL, you must use https with the URL. Example: http://<server name>/Cognos102
POPULATE DLL SLL REPORTS TABLE DATA	0 — Do not populate the RPT_CASE_EVENT_PRODUCT table, which is required for DLL and SLL reports 1 — Populate the RPT_CASE_EVENT_PRODUCT table, which is required for DLL and SLL reports **Note**: This attribute is obsolete in case of a fresh installation of Argus Insight 8.1. This attribute should be configured for the Detail Line Listing Report and the Simple Line Listing Report.
COGNOS SINGLE SIGN ON ENABLED	1 — Cognos single sign on enabled 0 — Cognos single sign on disabled

Note: You must configure the COGNOS AUTHENTICATION ENTERPRISE profile switch for Cognos integration. The default value of this switch is Null.

To define the attributes required for Cognos:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   Note: See Table 4–4, " Cognos Specific Attribute-Value set".

4. In the **Value** field, enter a value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

4.3 Configuring Duration Value Bands

In Argus Insight, you can map the following time values (entered in Argus Safety) to specific ranges called Duration Value Bands:

- Time to Onset from First Dose
- Time to Onset from Last Dose

You set the value of these fields in Argus Safety by navigating to Product tab, Drug Duration of Administration, and Events Tab.

By mapping the time values to Duration Value Bands in Argus Insight, you can specify query criteria based on ranges instead of specific values for the *Time to Onset* fields listed above.

Using the Duration Value Bands item on the List Maintenance tab, you can configure duration value bands in hours, days, weeks, months, and years. For each band, you can specify multiple ranges by entering minimum and maximum values for each range item. Any value that falls within a configured range will map to that range.

> **Note:** Duration Value Band configuration must be done before running the Initial ETL.
>
> If Duration Value Bands are modified after Initial ETL, you must re-run the Initial ETL.

To modify a duration value band:

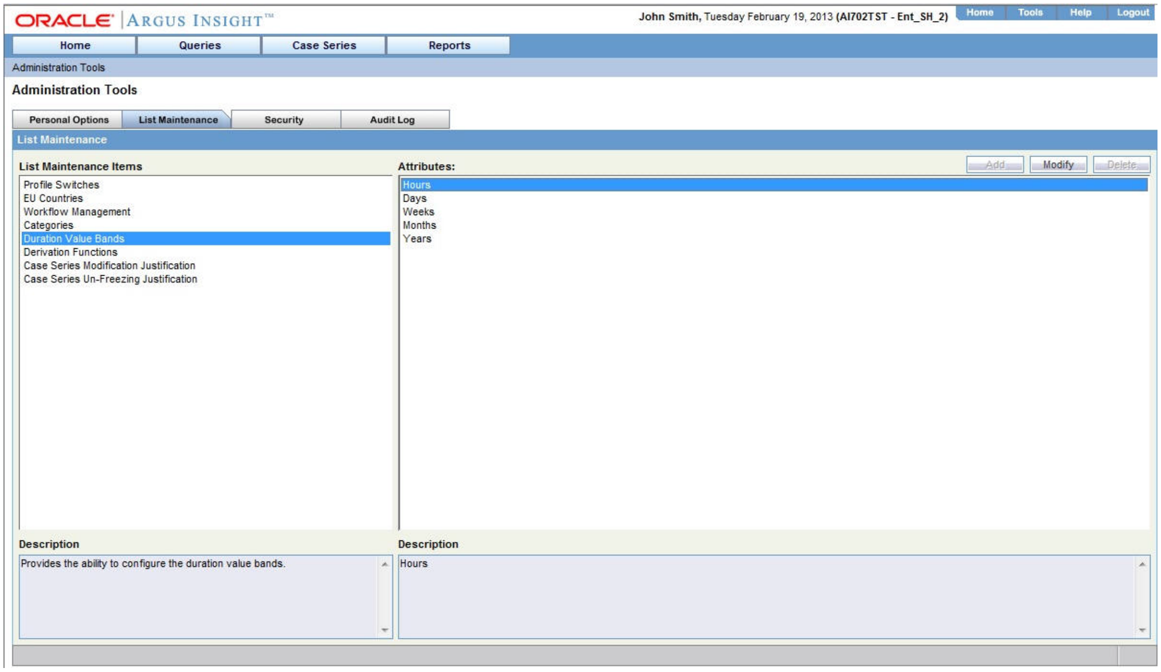
1. On the Argus Insight home page, click the **Tools** tab from the upper-right corner.

   The Administration Tools screen appears.

2. Click the **List Maintenance** tab.

3. From the List Maintenance Items group, select **Duration Value Bands**.

   The Attributes group displays the valid bands (Hours, Days, Weeks, Months, and Years). You can modify the values of these bands. You cannot, however, add more bands or delete an existing band.



List Maintenance Items:
- Profile Switches
- EU Countries
- Workflow Management
- Categories
- Duration Value Bands
- Derivation Functions
- Case Series Modification Justification
- Case Series Un-Freezing Justification

Attributes:
- Hours
- Days
- Weeks
- Months
- Years

Description: Provides the ability to configure the duration value bands.

Description: Hours

Note: When the Argus Insight Database Source profile switch is set to **Argus Mart**, then in the List Maintenance section, only **Profile Switches** and **Case Series Modification Justification** list maintenance items are available.

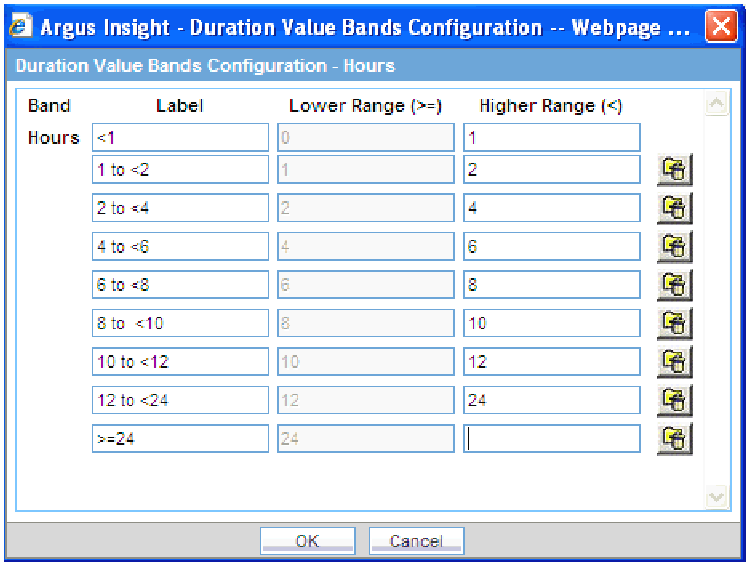
For more information on this profile switch, see Section 4.2.4, "Setting the Attributes Specific ONLY to Argus Mart".

4. Select the duration value band (Hours, Days, Weeks, Months, Years) you want to change, and click **Modify.**

   The Duration Value Bands Configuration dialog box appears with the factory-configured ranges.

   Note that:

   - The Label column represents the name of the range.
   - The Lower Range (>=) and Higher Range (<) columns contain the minimum and maximum values, respectively.
   - The highest value band includes all values that are greater than the highest range value specified.


Argus Insight - Duration Value Bands Configuration -- Webpage ...
Duration Value Bands Configuration - Hours
OK
Cancel

Band	Label	Lower Range (>=)	Higher Range (<)
Hours	<1	0	1
	1 to <2	1	2
	2 to <4	2	4
	4 to <6	4	6
	6 to <8	6	8
	8 to <10	8	10
	10 to <12	10	12
	12 to <24	12	24
	>=24	24	

5. Modify the values:

   - To modify an existing range, edit the values in the **Lower Range (>=)** and **Higher Range (<)** fields.
   - To add a range, scroll to the current highest range and click in the blank **Higher Range (<)** field.

     Enter a value greater than the current highest range, and press **Tab** to add a new row.
   - To delete an existing range, click the **Delete** icon next to the row.

     Note that you cannot delete the lowest band.

If you delete an intermediate range, the system automatically converts the highest value of the deleted range to the lowest value in the next range. However, the system does not change the range labels.

6. Click **OK** to save the changes.

4.4 Configuring Derivation Functions

You can create a new List Maintenance item and derive specific cases to this item based on case attributes. These attributes are supplied to the system as SQL.

For example:

1. Create a new List Maintenance item called **Report Type 1**, and derive all the cases with the **Report Type** attribute defined as **Spontaneous, Literature,** or **Compassionate Use.**

   The Report Type 1 appears as an option in the query tool interface corresponding to the Report Type attribute.

2. From the Report Type, select Report Type 1, and execute the query.

   Cases with the Report Type attribute specified as Spontaneous, Literature, or Compassionate Use are returned.

You can specify more than one attribute.

For example, create a further specialized List Maintenance item called **Report Type 1 US**, and derive all the cases that have the **Report Type** attribute defined as **Spontaneous, Literature,** or **Compassionate Use,** *and* the **Country of Incidence** attribute defined as **United States.**

> **Note:** There can be situations where two different List Maintenance items you create contain similar attributes in the SQL criteria. In this case, you can assign a priority level to individual List Maintenance items. The priority level determines which List Maintenance item SQL executes first.

4.4.1 Opening the Derivation Fields Dialog Box

To open the Derivation Fields dialog box and configure derivation functions:

1. On Argus Insight home page, click the **Tools** tab from the upper-right corner.

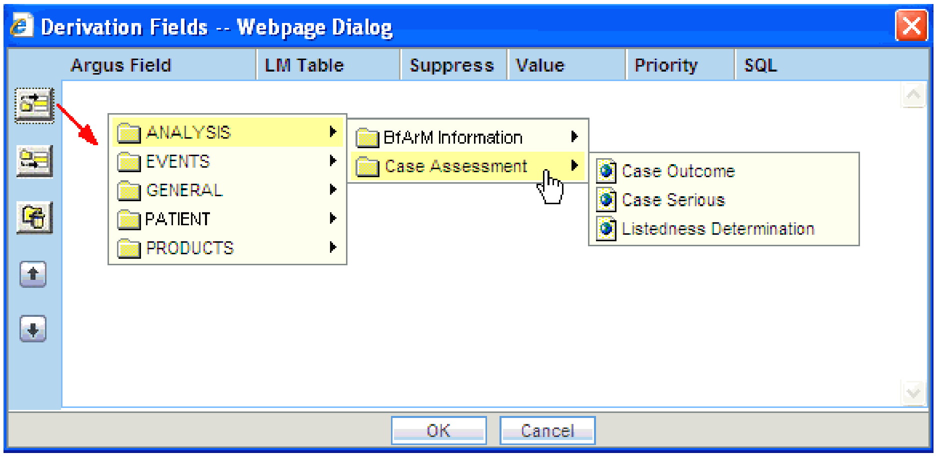
   The Administration Tools screen appears.

2. Click the **List Maintenance** tab.

3. From the List Maintenance Items group, select **Derivation Functions**.

4. From the Attributes group, select **All Derivations,** and click **Modify.**

   The Derivation Fields dialog box appears.



4.4.2 Icons in the Derivation Fields Dialog Box

Table 4–5 describes the icons in the Derivation Fields dialog box that you can use to add, delete, and reorder derivation field elements (rows).

Table 4–5 Icons in the Derivation Fields Dialog Box

Click...	To...
	Add a derivation field element (row) above the currently selected row
	Add a derivation field element (row) below the currently selected row
	Delete the currently selected derivation field element (row)
↑	Move the selected row up
↓	Move the selected row down

4.4.3 Field Mapping Derivation Rules

Table 4–6 lists the available field mapping derivation rules for Argus Insight.

Table 4–6 Field Mapping Derivation Rules

Function Category	Function Sub-category	Argus Insight Field
ANALYSIS	BfArM Information	Causality
ANALYSIS	Case Assessment	Case Outcome Case Serious Listedness Determination
EVENTS	Event Information	Lack of Efficacy
GENERAL	General Information	Report Type Derived Pregnancy
PATIENT	Patient Information	Age Group Gender Patient weight BMI desc

Table 4–6 (Cont.) Field Mapping Derivation Rules

Function Category	Function Sub-category	Argus Insight Field
PRODUCTS	Product Drug	Derived Drug Abuse Derived Drug Interaction Derived Overdose Last daily dose

Note: Causality, Report Type, Age Group, and Last daily dose are comma-separated derivation rules.

4.4.4 Fields and Check Boxes in the Derivation Fields Dialog Box

This section describes the fields and check boxes in the Derivation Fields dialog box.

4.4.4.1 LM Table

The LM Table field is the table name of the selected Argus field (that is, automatically populated).

4.4.4.2 Suppress

The Suppress check box is available for fields associated with the list maintenance data. When suppress is enabled for a field, the corresponding list maintenance values that are not present in any case are deleted and thus not available for querying.

Note: The Suppress check box is applicable *only if* the condition specified in the SQL text box covers all the cases having the selected List Maintenance field.

4.4.4.3 Value

The Value field captures the value for the new derivation field. For the following rules, you must enter the new value for the rule as a comma-separated value:

- Causality
- Report Type
- Age Group
- Last Daily Dose

Note: Make sure to enter the values for these rules as defined in the following sections. Unexpected results and/or ETL errors may result if the values are not entered as specified.

Causality Rule

Parameters: VALUE, REPORTABILITY

where:

VALUE = New value for the rule

REPORTABILITY = Lower value of the group

Example: NewCausality,1

Report Type Rule

Parameters: VALUE, INC_LIT, INC_TRIAL, ABRV

where:

VALUE = New value for the rule

INC_LIT = 1 if Literature Report Type else 0

INC_TRIAL = 1 if Clinical Trial Report Type else 0

ABRV = A 3-letter abbreviation for the Report Type

Example: NewReportType,0,1,NRT

Age Group Rule

Parameters: VALUE, GROUP_LOW, GROUP_HIGH

where:

VALUE = New value for the rule

GROUP_LOW = Lowest value of the age group

GROUP_HIGH = Highest value of the age group

Example: NewAgeGroup,25,50

If you do not want to specify the High Value, then the comma is mandatory in the end.

Example: Unknown,70,

Last Daily Dose Rule

Parameters: VALUE, DAILY_DOSE_SORTING_ORDER

where:

VALUE = New value for the rule

DAILY_DOSE_SORTING_ORDER = 1 or 2 or 3 and so on to define the sorting order if there is more than 1 rule for the Last Daily Dose field

Examples: 1 -> 0to1,1;   2 -> 2to3,2   3 -> 5to8,3

4.4.4.4 Priority

The Priority field captures the priority for a list of derivation rules applied to a single List Maintenance field. The value should be from 1 to 255.

Note: The priority for derivation rules applicable to a single List Maintenance field should be unique.

4.4.4.5 SQL

The SQL field specifies the SQL statement to capture the cases for which the derivation rule is applicable.

Note: The SQL statement must follow the correct syntax.

The system does not validate the length of the new values against the database. Make sure that new values being inserted into the Insight data mart do not exceed the limit defined in the database.

Guidelines for correct syntax:

- The SQL query configured against a rule should not contain the table name. It should contain only the primary key column name(s) of the field in the SELECT clause. For example:

  Correct: SELECT CASE_ID FROM RPT_CASE WHERE…

  Incorrect: SELECT RPT_CASE.CASE_ID FROM RPT_CASE WHERE…

- Make sure that there is only one space after the SELECT clause in the SQL query. For example:

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT   CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

- Make sure that no Oracle keyword (such as DISTINCT) is used after the SELECT clause in the SQL query. For example:

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT DISTINCT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

4.5 Configuring the Argus Insight Windows Service

To configure the Argus Insight Windows service:

1. Log in to the Argus Insight Web Server.
2. Click **Start**, and select **Run.**
3. In the text box, enter **services.msc**, and click **OK.**

   The Services screen appears.
4. Right-click **Argus Insight Service**, and select **Properties.**

   The Argus Insight Service Properties dialog box appears.
5. Set the value of the **Startup type** field to **Automatic.**
6. Click **Start** to start the Argus Insight Service.
7. Click **OK** to apply the changes.

> **Note:** To change the interval of different service tasks, modify the entries in the Service.config file located in the Bin folder of Argus Insight. All the timestamps in the Service.config file are specified in seconds.

IMPORTANT! Ensure that the user who runs this service has administrator privileges.

4.6 Configuring the IIS File Download Limit

To configure the IIS file download limit for Windows 2012:

1. Go to the Internet Information Services (IIS) Manager.
2. Double-click **ASP** in the right pane.

   The ASP dialog box appears.

3. Expand **Limit Properties** and change the **Response Buffering Limit** from 4 MB (default) to a large value such as 200000000 (200 MB).
4. From Actions in the left pane, click **Apply**.
5. Restart the IIS service.
   a. Click **Start**, and select **Run.**
   b. In the text box, enter **iisreset -start**.
   c. Click **OK.**

4.6.1 Configuring the Maximum Requesting Entity Body Limit

Defining a value for the **Maximum Requesting Entity Body Limit** setting is optional.

You may need to set this value only if you use custom SQL scripts in advanced conditions and only if the scripts have more than 70,000 characters.

If you receive AJAX errors when saving your custom SQL scripts that have more than 70,000 characters, you can increase the value of the **Maximum Requesting Entity Body Limit** setting in the IIS. Increasing the setting ensures that the ASP can post that much data onto the server.

To change the value of the **Maximum Requesting Entity Body Limit** setting:

1. Go to the Internet Information Services (IIS) Manager.
2. Double-click **ASP** in the right pane.

   The ASP dialog box appears.
3. Expand **Limit Properties** and change the **Maximum Requesting Entity Body Limit** from 200000 Bytes (default) to a large value (preferably 5000000 Bytes).
4. From Actions in the left pane, click **Apply**.
5. Restart the IIS service.
   a. Click **Start**, and select **Run.**
   b. In the text box, enter **iisreset -start**.
   c. Click **OK.**

4.7 Using Export and Import to Copy Configuration Data

Before configuring export and import functions, be aware of the following:

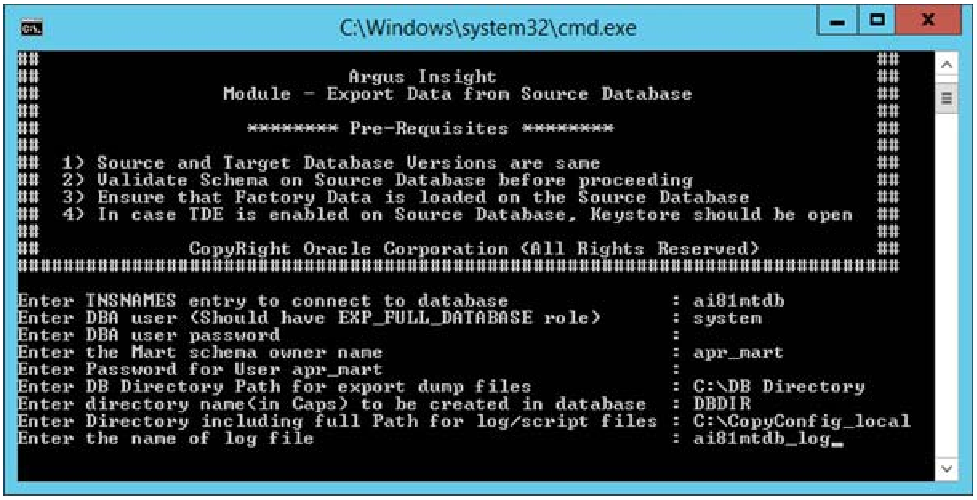
- Before importing or exporting to or from a network drive, verify that you have mapped the network drive. This tool does not support direct access to network drives.
- Before copying Argus Data, incremental ETL should be completed on Source Insight Database from Source Argus.
- It is assumed that the configuration of the instance of Argus used to run Initial and Incremental ETL on the source Argus Insight data mart will also be copied and applied on the new Argus Instance which will be associated with the new Argus Insight data mart.
- Data must be imported after loading Factory Data and before running Initial ETL on destination environment.

- In a multi-tenant environment, you must make sure that all the enterprises which are part of the source Argus Insight database, have been created in the Target Argus Insight database.

4.7.1 Exporting Data

1. Start the Argus Insight Schema Creation Tool.
2. Click **Export Data.**

   The Export Utility command prompt screen appears.



```
##                                                                         ##
##                           Argus Insight                                 ##
##                Module - Export Data from Source Database                ##
##                                                                         ##
##                  ********* Pre-Requisites *********                     ##
##                                                                         ##
##  1) Source and Target Database Versions are same                        ##
##  2) Validate Schema on Source Database before proceeding                ##
##  3) Ensure that Factory Data is loaded on the Source Database           ##
##  4) In case TDE is enabled on Source Database, Keystore should be open  ##
##                                                                         ##
##             CopyRight Oracle Corporation (All Rights Reserved)          ##
#############################################################################

Enter TNSNAMES entry to connect to database              : ai81mtdb
Enter DBA user (Should have EXP_FULL_DATABASE role)      : system
Enter DBA user password                                  :
Enter the Mart schema owner name                         : apr_mart
Enter Password for User apr_mart                         :
Enter DB Directory Path for export dump files            : C:\DB Directory
Enter directory name(in Caps) to be created in database  : DBDIR
Enter Directory including full Path for log/script files : C:\CopyConfig_local
Enter the name of log file                               : ai81mtdb_log_
```

3. Enter the following details when prompted, and press **Enter**:

   a. TNSNAMES entry of the Argus Insight Database

   b. DBA User

   c. DBA User Password

   d. Mart Schema Owner Name

   e. Mart Schema Owner Password

   f. DB Directory path for export dump files (database server file path)

      Enter a directory path specific to your database environment.

      The Export Dump file and Export log file will be placed here as INSIGHT.DMP and Export_log.log respectively.

   g. Directory Name (in capital letters) to be created in the database

      A database directory is created with this name at the path mentioned in the previous step.

   h. Directory including full path for log/script files (Local Machine)

      Enter a directory path specific to the machine where the Copy Configuration utility is being run.

      The user specified log file and files named application_type_check.sql, insight_export_tables.par, and truncate_delete_tables.sql will be generated here.

   i. Name of the log file

4. Verify that the script is successfully connected as <DBA User Name>@<Argus Insight Database Name>, and press **Enter**.

   The command prompt screen with the Encryption wallet verification status appears.

5. Verify the details mentioned on the command prompt screen, and press **Enter** if:

   - TDE is setup and Wallet is open
   - TDE is not setup and Wallet is not open

   The command prompt screen with Directory creation status appears.

6. Press **Enter** if the Directory Path is valid.

7. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name>, and press **Enter**.

   The command prompt screen with list of parameters appears.

8. Press **Enter** to resume if the parameters are valid.

   Verify the details mentioned on the command prompt screen, and press **Enter**.

9. Enter the password for the **APR_MART** user, and press **Enter**.

   A data export completed screen appears with a list of all the output files.

10. Verify the location of files, and press **Enter** to Exit.

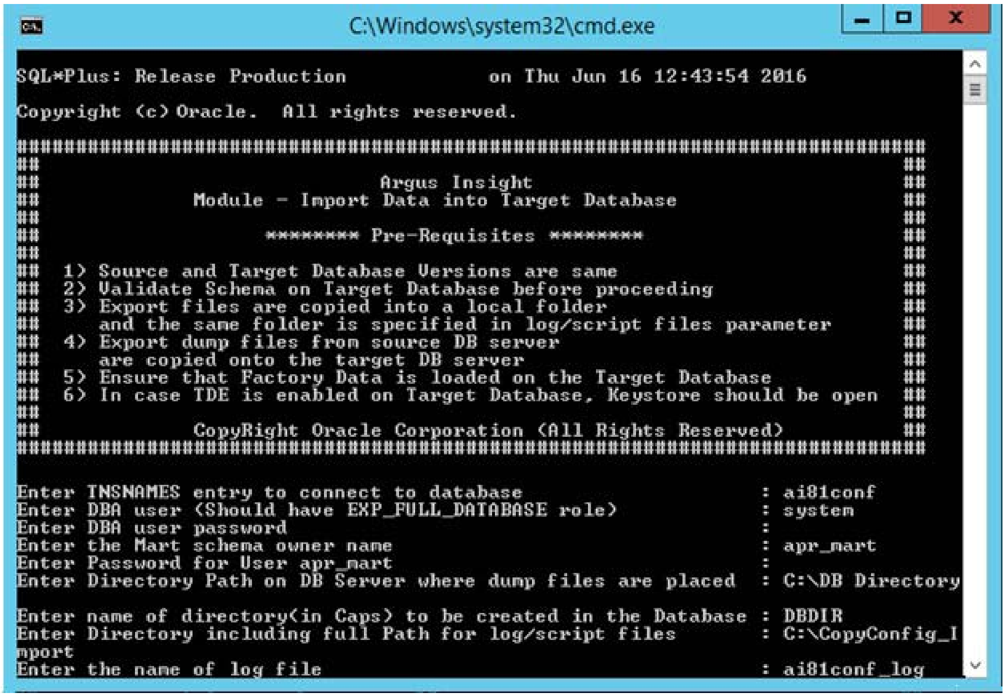
    Make sure to review the all the log files for information about the export and export errors.

4.7.2 Importing Data

1. Start the Argus Insight Schema Creation Tool.

2. Click **Import Data.**

   The Import Utility command prompt screen appears.



```
SQL*Plus: Release Production            on Thu Jun 16 12:43:54 2016

Copyright (c) Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                          Argus Insight                                   ##
##              Module - Import Data into Target Database                   ##
##                                                                          ##
##                    ******** Pre-Requisites ********                      ##
##                                                                          ##
##   1) Source and Target Database Versions are same                        ##
##   2) Validate Schema on Target Database before proceeding                ##
##   3) Export files are copied into a local folder                         ##
##      and the same folder is specified in log/script files parameter      ##
##   4) Export dump files from source DB server                             ##
##      are copied onto the target DB server                                ##
##   5) Ensure that Factory Data is loaded on the Target Database           ##
##   6) In case TDE is enabled on Target Database, Keystore should be open  ##
##                                                                          ##
##              CopyRight Oracle Corporation (All Rights Reserved)          ##
##############################################################################

Enter TNSNAMES entry to connect to database                 : ai81conf
Enter DBA user (Should have EXP_FULL_DATABASE role)         : system
Enter DBA user password                                     :
Enter the Mart schema owner name                            : apr_mart
Enter Password for User apr_mart                            :
Enter Directory Path on DB Server where dump files are placed  : C:\DB Directory

Enter name of directory(in Caps) to be created in the Database : DBDIR
Enter Directory including full Path for log/script files       : C:\CopyConfig_I
mport
Enter the name of log file                                  : ai81conf_log
```

3. Press **Enter** if all prerequisites are satisfied.
4. Enter the following details when prompted, and press **Enter**:
   a. TNSNAMES entry of the Argus Insight Database
   b. DBA User
   c. DBA User Password
   d. Mart Schema Owner Name
   e. Mart Schema Owner Password
   f. DB Directory path for import dump files (database server file path)

      Enter a directory path specific to your database environment.

      INSIGHT.DMP created in the export process is copied here. Beside, Import_log.log is also created here.
   g. Directory Name (in capital letters) to be created in the database

      A database directory is created with this name at the path mentioned in the previous step.
   h. Directory including full path for log/script files (Local Machine)

      Enter a directory path specific to the machine where the Copy Configuration utility is being run.

      The user specified log files are generated here.

      Besides, make sure that the files named application_type_check.sql, insight_export_tables.par, and truncate_delete_tables.sql that were generated during export process are also copied here.
   i. Name of the log file
5. Verify that the script is successfully connected as <DBA User Name>@<Argus Insight Database Name>, and press **Enter**.

   The command prompt screen with the Encryption Wallet Verification status appears.
6. Verify the details mentioned on the command prompt screen, and press **Enter** if:
   - TDE is setup and Wallet is open
   - TDE is not setup and Wallet is not open

   The command prompt screen with Directory Creation status appears.
7. Press **Enter** if the Directory Path is valid.
8. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name>, and press **Enter**.

   The command prompt screen with list of parameters appears.
9. Press **Enter** to resume if the parameters are valid.

   Verify the details mentioned on the command prompt screen, and press **Enter**.
10. Enter the password for the **APR_MART** user, and press **Enter**.

    A data import completed screen appears.
11. Press **Enter** to Exit.

Make sure to review the all the log files for information about the import and import errors.

4.8 Using Argus Safety to Configure Enterprises for Argus Insight

Using Argus Safety to configure enterprises for Argus Insight is supported in multi-tenant installations only.

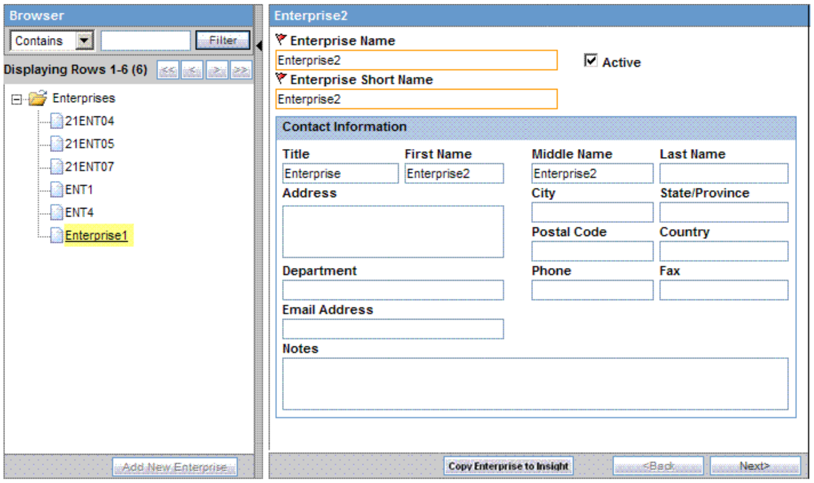
In addition, you must be a valid LDAP user and you must have access to the Argus Safety global home page.

See the Global Enterprise Management section of the *Argus Safety Installation Guide* for detailed steps on logging and accessing Argus Safety global home page.

To create an enterprise in Argus Insight:

1. Log in to the Global Enterprise Management portlet.
2. From the Enterprises folder, select an enterprise from the left pane.

   The Enterprises folder includes enterprises as per you access privileges.



Browser

Displaying Rows 1-6 (6)

Enterprise2

Enterprise Name: Enterprise2

☑ Active

Enterprise Short Name: Enterprise2

Contact Information

Title: Enterprise

First Name: Enterprise2

Middle Name: Enterprise2

Last Name:

Address:

City:

State/Province:

Postal Code:

Country:

Department:

Phone:

Fax:

Email Address:

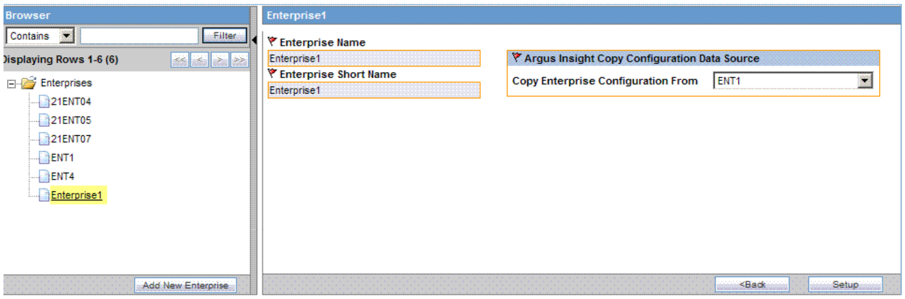
Notes:

3. Click **Copy Enterprise to Insight** to initiate the creation of the selected enterprise in Argus Insight.

   Note that the Copy Enterprise to Insight button:

   - Is disabled if the selected enterprise already exists in Argus Insight.
   - Is enabled if you have Copy Configuration role in any of the listed enterprises.

   The following screen appears.



Browser

Displaying Rows 1-6 (6)

Enterprise1

Enterprise Name: Enterprise1

Enterprise Short Name: Enterprise1

Argus Insight Copy Configuration Data Source

Copy Enterprise Configuration From: ENT1

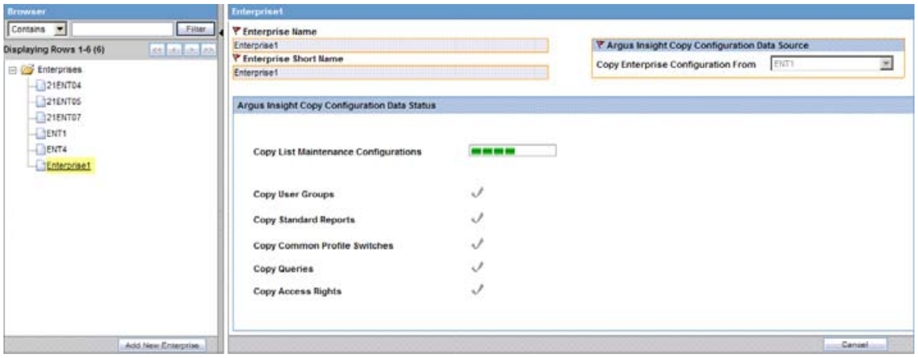
4. In the **Copy Enterprise Configuration From** field, select the source enterprise from which the information will be copied.

   Note that the drop-down list includes only those enterprises that meet the following two conditions:

   - The enterprise has already been created in Argus Insight.
   - You have been assigned Copy Configuration privileges for the enterprise.

5. Click **Setup.**

   The process to copy the configuration begins and a status information appears throughout the process.

   Enterprise Name: Enterprise1

   Enterprise Short Name: Enterprise1

   Argus Insight Copy Configuration Data Source

   Copy Enterprise Configuration From: ENT1

   Argus Insight Copy Configuration Data Status

Copy List Maintenance Configurations	🟩🟩🟩🟩
Copy User Groups	✓
Copy Standard Reports	✓
Copy Common Profile Switches	✓
Copy Queries	✓
Copy Access Rights	✓

6. Click **Finish** to complete the creation of the enterprise in Argus Insight.

4.9 Securing Sensitive Configuration and Operational Data

For security reasons, you should configure permission settings for certain files and folders on the Argus Insight Web Server. The permission settings ensure that only the IIS user can access these files. Local system login accounts that are not part of the Administrators group cannot make changes to the files.

Windows Directory File

For the user under which IIS is running, the **ai.ini** file requires a permission of **Full Control.**

Shared Folders

For the user under which IIS is running, the following folders require a permission of **Full Control:**

- CacheTemp
- ScheduledReports
- PDFReports
- ASP
- Bin

5

Extracting, Transforming, and Loading Data

This chapter describes the steps required to run and work with the initial extract, transform, and load (ETL) process.

This chapter includes the following topics:

- Prerequisites, Cautions, and Warnings
- Running the Initial ETL
- Running the Initial ETL Again
- Processing a Failed ETL
- Restarting the Initial ETL Process

5.1 Prerequisites, Cautions, and Warnings

Before running the Initial ETL, ensure:

- The Auto extend is set to ON for all the data files in the database that are related to staging and Insight Mart.
- The POPULATE CASE/CONFIGURATION DATA profile switch is configured to the desired value.

In addition, note that:

- Since the initial ETL requires a huge amount of temporary space, set the temporary space to 100 GB to prevent data errors. After completing the Initial ETL, reduce the temporary space to 30 GB.
- After the Initial ETL completes, the balancing log may show differences between the Argus (Stage) and Insight Mart table counts. This is because of the derivation rules applied to the Insight data mart.
- The system may display the following message:

  ```
  Warning !!! - Could not locate MedDRA-J User in the Argus Database.
  ```

  Ignore this warning for all MedDRA tables.
- **Do not** run incremental ETL for more than 50,000 cases. Run the Initial ETL again if the number of cases exceeds 50,000.
- The Argus Insight ETL will not populate the Argus Mart database.

  Refer to the *Oracle Argus Mart Installation and Administration Guide* for more information on the Argus Mart ETL.

5.2 Running the Initial ETL

To run the initial ETL:

1. Log in to the Argus Insight Web Server as a user with administrator privileges.
2. Click **Start.**
3. Navigate to **Programs > Oracle > Argus Insight,** and then select **Schema Creation Tool.**
4. Click **Initial ETL.**

   The Oracle Database Connect dialog box appears.
5. To connect to the Oracle Database:

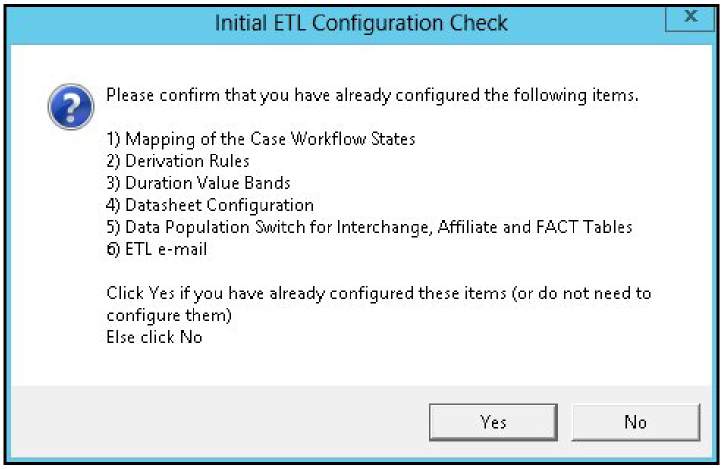
   a. In the **Password** field, enter the password for the APR_MART user.

   b. In the **Database** field, enter the name of your Argus Insight database.

   c. Click **OK.**

   The Initial ETL Status dialog box opens.
6. Click **Start ETL**.

   The initial process of extracting, transforming, and loading data begins. A message confirming that you have completed the required configuration steps appears.



Please confirm that you have already configured the following items.

1) Mapping of the Case Workflow States
2) Derivation Rules
3) Duration Value Bands
4) Datasheet Configuration
5) Data Population Switch for Interchange, Affiliate and FACT Tables
6) ETL e-mail

Click Yes if you have already configured these items (or do not need to configure them)
Else click No

7. Click **Yes** if these items have already been configured.

   The Initial ETL Status dialog box appears stating the ETL start time, the progress bar, and the current process in execution.

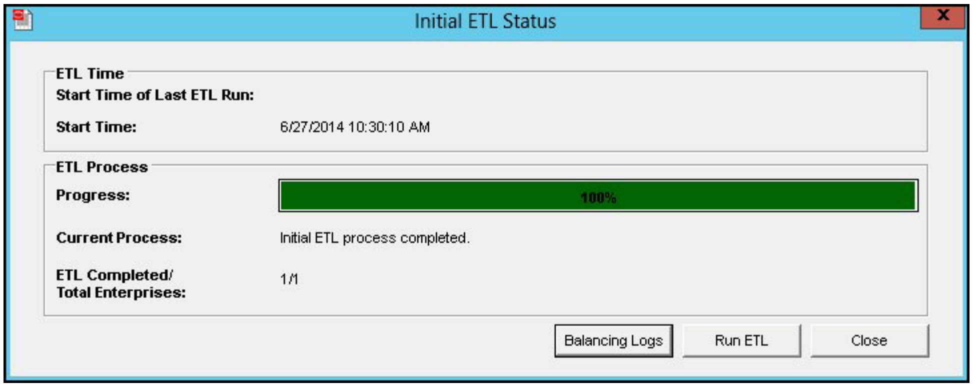
   While the ETL is in progress, you can:

   - To close the dialog box, and exit from the Schema Creation Tool, click **Close**.

     Closing the dialog box does not affect the execution of the ETL process.
   - To halt the ETL process, click **Stop ETL**.

     For more information about this option, see Section 5.2.3, "Stopping the Execution of ETL."

   A status message appears when the initial ETL process is completed.



Initial ETL Status

ETL Time

Start Time of Last ETL Run:

Start Time: 6/27/2014 10:30:10 AM

ETL Process

Progress: 100%

Current Process: Initial ETL process completed.

ETL Completed/ Total Enterprises: 1/1

5.2.1 Generating the Balance Logs

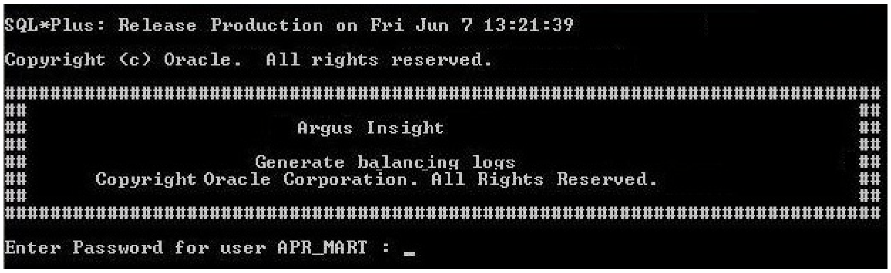
When the system successfully completes the Initial ETL process, you should generate and check the logs.

To generate the balance logs:

1. Wait until the dialog box that reports the initial ETL completed successfully appears.
2. Click **Balancing Logs.**

   A dialog box appears to confirm that you want to generate balancing logs for the completed Initial ETL appears.
3. Click **OK**.

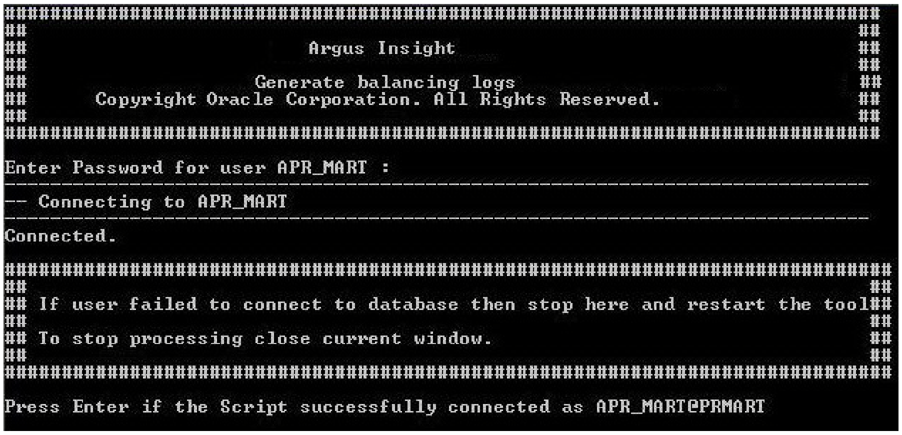
   The command prompt screen appears.



```
SQL*Plus: Release Production on Fri Jun 7 13:21:39

Copyright (c) Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                            Argus Insight                                 ##
##                                                                          ##
##                         Generate balancing logs                          ##
##       Copyright Oracle Corporation. All Rights Reserved.                 ##
##                                                                          ##
##############################################################################

Enter Password for user APR_MART : _
```

4. Enter the password for the **APR_MART** user, and press **Enter**.

   This following command prompt screen appears:



```
##############################################################################
##                                                                          ##
##                             Argus Insight                                ##
##                                                                          ##
##                         Generate balancing logs                          ##
##       Copyright Oracle Corporation. All Rights Reserved.                 ##
##                                                                          ##
##############################################################################

Enter Password for user APR_MART :
-----------------------------------------------------------------------------
-- Connecting to APR_MART
-----------------------------------------------------------------------------
Connected.

###############################################################################
##                                                                           ##
## If user failed to connect to database then stop here and restart the tool##
##                                                                           ##
## To stop processing close current window.                                  ##
##                                                                           ##
###############################################################################

Press Enter if the Script successfully connected as APR_MART@PRMART
```

5. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name>, and press **Enter**.

   The command prompt screen appears and the balancing logs are generated.

   When the logs are generated, a dialog box with the location and name of the log files appears.

6. Click **OK** to close the dialog box.

7. Open and verify the contents of each Balancing Report.

   The Balancing Reports are located at:

   drive:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller

   The log files are named as:

   - etl_ini_atos_bal_lm_cfg_rep.log
   - etl_ini_atos_bal_rep.log
   - etl_ini_stom_bal_lm_cfg_rep.log
   - etl_ini_stom_bal_rep.log

5.2.2 Closing the Initial ETL Status Dialog Box

To close the Initial ETL Status dialog box and exit from the Schema Creation Tool:

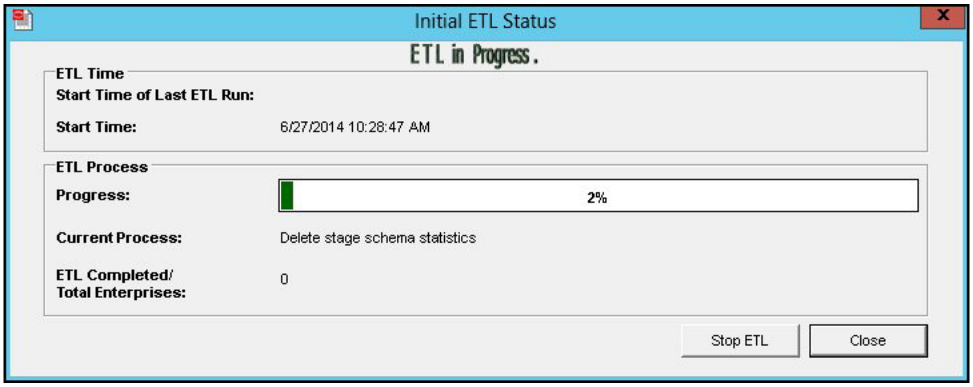
1. Click **Close.**

   A message to confirm that you want to close the Schema Creation Tool application appears.

2. Click **OK.**

5.2.3 Stopping the Execution of ETL

You can choose to stop an ETL in progress.



Start Time of Last ETL Run:

Start Time: 6/27/2014 10:28:47 AM

Progress: 2%

Current Process: Delete stage schema statistics

ETL Completed/ Total Enterprises: 0

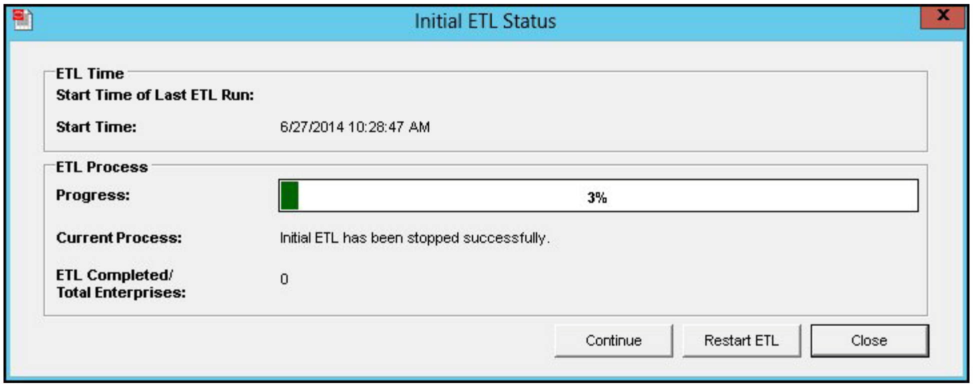
To halt the execution of the initial ETL process:

1. Click **Stop ETL.**

   A message to confirm that you want to stop the ETL currently in progress appears.

2. Click **OK.**

   The ETL process is stopped and returns to the Initial ETL Status dialog box.



ETL Time

Start Time of Last ETL Run:

Start Time: 6/27/2014 10:28:47 AM

ETL Process

Progress: 3%

Current Process: Initial ETL has been stopped successfully.

ETL Completed/ Total Enterprises: 0

At this point, you can select one of the following options:

- To continue extracting, transforming, and loading the data that was in progress, click **Continue.**
- To start the initial ETL from the beginning, click **Restart ETL.**
- To exit from the Schema Creation Tool application, click **Close.**

5.3 Running the Initial ETL Again

To start the ETL process from the beginning:

1. Click **Run ETL.**

   A message to confirm whether you want to start the initial ETL from the beginning appears.

2. Click **OK.**

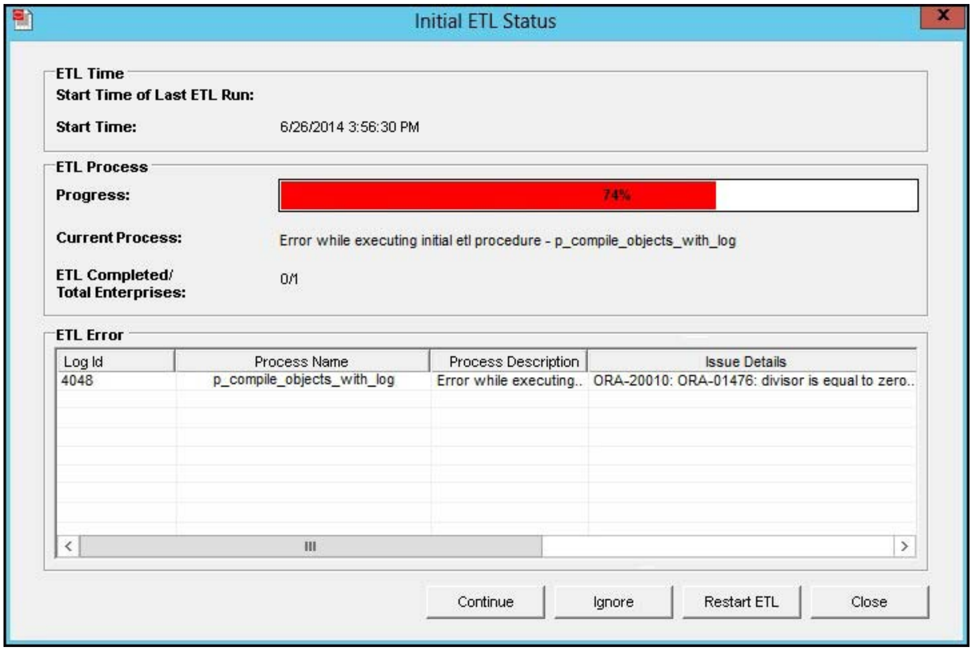
   The Oracle Database Connect dialog box appears.

3. Enter the password for the APR_MART user, and then click **OK.**

   The initial ETL process starts from the beginning.

5.4 Processing a Failed ETL

The initial ETL may fail due to an error. If an error occurs, the system stops processing the ETL and displays the following screen:



Start Time of Last ETL Run:

Start Time: 6/26/2014 3:56:30 PM

Progress: 74%

Current Process: Error while executing initial etl procedure - p_compile_objects_with_log

ETL Completed/ Total Enterprises: 0/1

Log Id	Process Name	Process Description	Issue Details
4048	p_compile_objects_with_log	Error while executing..	ORA-20010: ORA-01476: divisor is equal to zero..

You may choose any of the following options for the failed Initial ETL process:

- To continue the failed Initial ETL process, click **Continue**.
- To ignore the failed Initial ETL process, click **Ignore**.
- For ETL Data Exclusion, click **Modify Attributes**, if PRE_REQ_CHECK_FLAG switch is set to ABORT.

> **Note:** These modifications must be done before running the Initial ETL process.

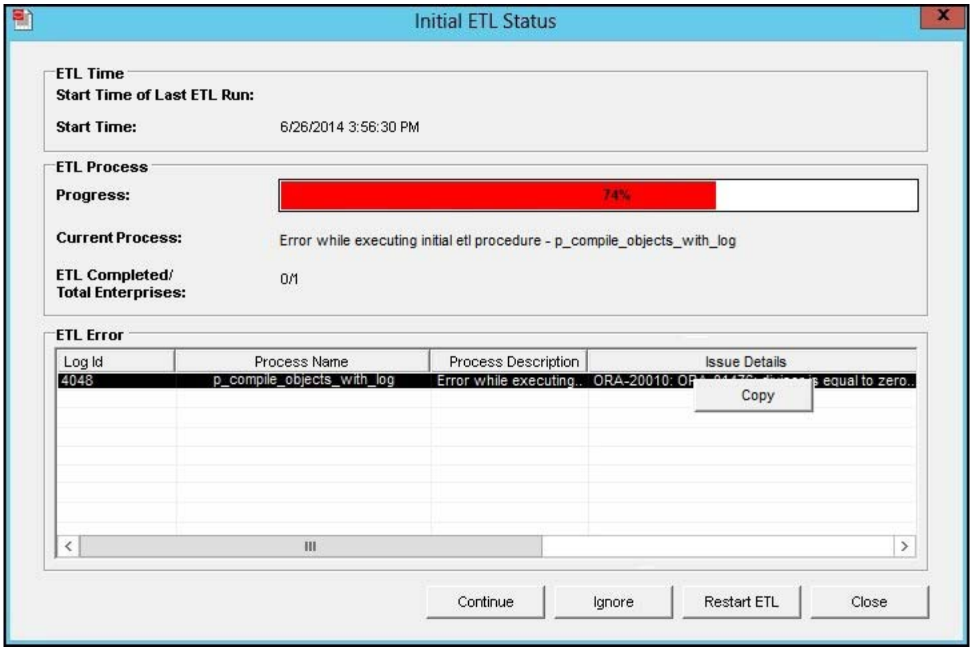
5.4.1 Continuing the Failed Initial ETL Process

To continue the Initial ETL process from the failed ETL procedure:

1. Double-click on the ETL error.

   The Error Data dialog box appears with details of the error.

2. Review the error information, and then click **OK.**
3. Right-click on the ETL Error, and click **Copy** to copy the error data.



Initial ETL Status

ETL Time

Start Time of Last ETL Run:

Start Time: 6/26/2014 3:56:30 PM

ETL Process

Progress: 74%

Current Process: Error while executing initial etl procedure - p_compile_objects_with_log

ETL Completed/ Total Enterprises: 0/1

ETL Error

Log Id	Process Name	Process Description	Issue Details
4048	p_compile_objects_with_log	Error while executing..	ORA-20010: OR [illegible] s equal to zero..

4. Click **Continue** to continue the failed ETL process.

   A message to confirm that you want to start the initial ETL from the stopped process appears.

5. Click **OK.**

   The ETL process continues (if no errors are found).

5.4.2 Ignoring the Failed Initial ETL Process

To ignore a failed ETL process and continue with the next process in the ETL:

1. Click **Ignore**.

   A message to confirm that you want to skip the failed process and continue executing the Initial ETL with the next process appears.

2. Click **OK.**

   The Initial ETL begins from the next process and continues with the ETL process (if no errors are found).

5.4.3 Modifying the Attributes of ETL Data Exclusion

You must modify these attributes before ETL execution.

To modify ETL Data Exclusion attributes:

1. Log in to the Argus Insight application as a user with administrator privileges.
2. On Argus Insight home page, from the upper-right corner, click the **Tools** tab.

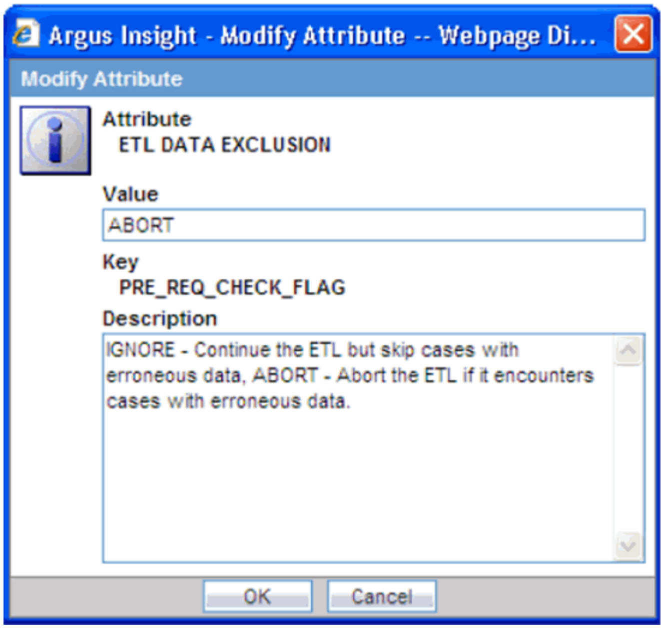
   The Administration Tools screen appears.

3. Click the **List Maintenance** tab.
4. Select **Profile Switches** from the List Maintenance Items group.

   The Attributes group is updated with the profile switches that you can modify.

5. Select **ETL Data Exclusion**, and click **Modify.**

   The Modify Attribute dialog box appears.



Attribute
ETL DATA EXCLUSION

Value
ABORT

Key
PRE_REQ_CHECK_FLAG

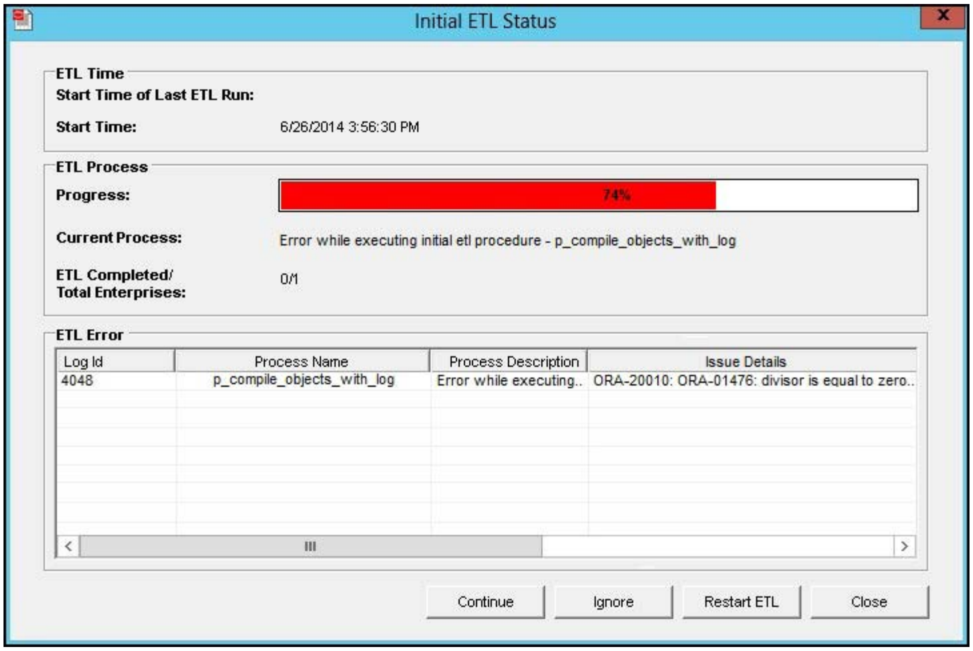
Description
IGNORE - Continue the ETL but skip cases with erroneous data, ABORT - Abort the ETL if it encounters cases with erroneous data.

6. Click the **Value** field, and enter one of the following values:

   - If you want the ETL process to skip cases with erroneous data and continue processing all other cases, enter **IGNORE.**
   - If you want the ETL process to abort when it encounters cases with erroneous data, enter **ABORT.**

7. Click **OK** to save the changes and return to the List Maintenance tab.

5.5 Restarting the Initial ETL Process



ETL Time
Start Time of Last ETL Run:
Start Time: 6/26/2014 3:56:30 PM

ETL Process
Progress: 74%
Current Process: Error while executing initial etl procedure - p_compile_objects_with_log
ETL Completed/ Total Enterprises: 0/1

ETL Error

Log Id	Process Name	Process Description	Issue Details
4048	p_compile_objects_with_log	Error while executing..	ORA-20010: ORA-01476: divisor is equal to zero..

To restart the Initial ETL process starting from after the confirmation message and APR_MART password input:

1. Click **Restart ETL.**

   A message to confirm that you want to start the initial ETL from the beginning appears.

2. Click **OK.**

   The Oracle Database Connect dialog box appears.

3. Connect to the Oracle Database:

   a. In the **Password** field, enter the password for the APR_MART user.

   b. In the **Database** field, enter the name of your Argus Insight database.

   c. Click **OK.**

4. Click **Start ETL** to start the initial process of extracting, transforming, and loading data.

   A message to confirm that you have completed the required configuration steps appears. See Section 5.2 > Step 6.

5. Click **Yes** if these items have already been configured.

   The Initial ETL Status dialog appears with the ETL start time, the progress bar, and the current process in execution.

   When the system finishes the ETL process, click **Close.**

6 Configuring the BIP Environment

Once you have installed the BI Publisher (BIP), you need to configure certain settings to be able to view the available reports in BIP. This chapter introduces you with the steps to make those configuration changes using BIP.

This chapter includes the following topics:

- Creating PRMART JDBC Connection
- Managing Users and Roles: BI Publisher Standalone Installation with BI Publisher Security
- Managing Users and Roles: BI Publisher Standalone Installation with OFM Security
- Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model

6.1 Creating PRMART JDBC Connection

If you are installing BIP on a Windows machine, the TNS entry of Argus Insight must be added in **TNSNAMES.ora** file of the BIP Web Server.

If BIP is installed on a Linux machine, no modifications to the **TNSNAMES.ora** file are required.

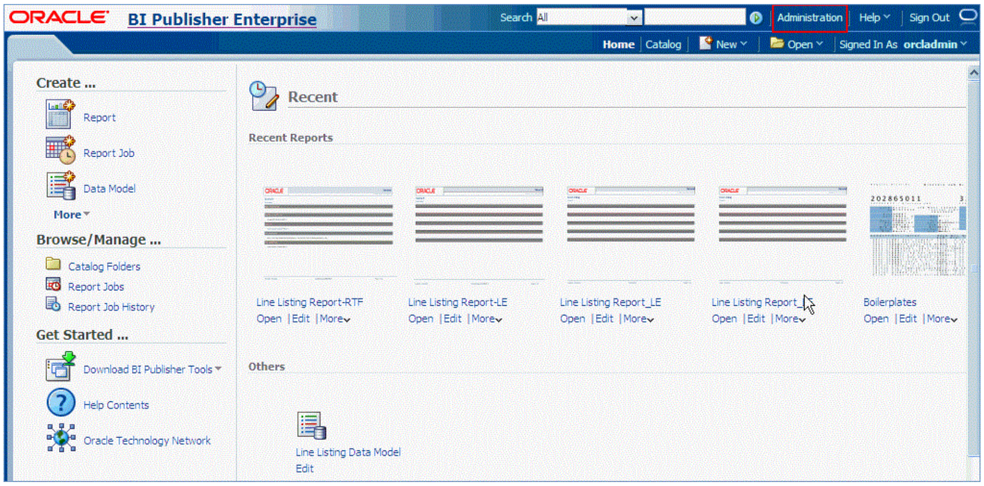
When you have uploaded the **Argus Insight.xdrz** file to BIP, you also need to create a connection between the BIP and the database.

To connect the BIP and the database, execute the following steps:

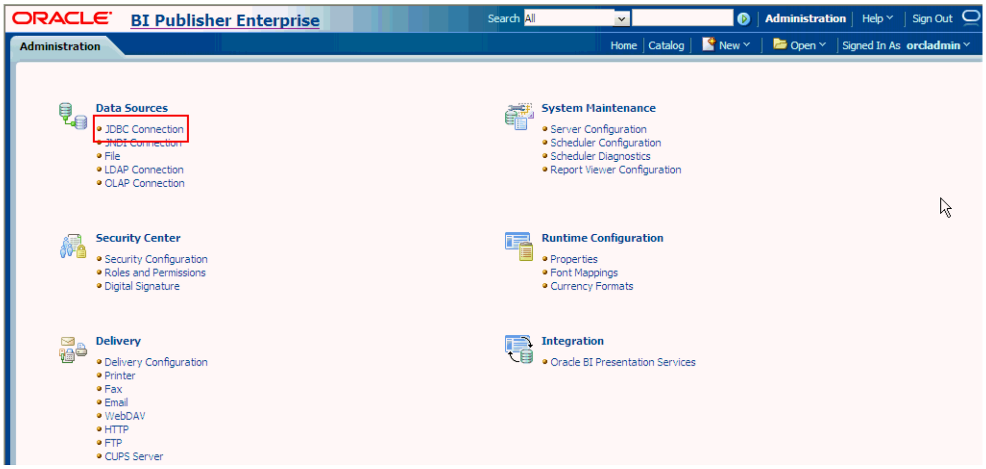
1. Log on to BIP using the administrator credentials.

   The BIP home page appears.

2. From top-menu, click **Administration**.

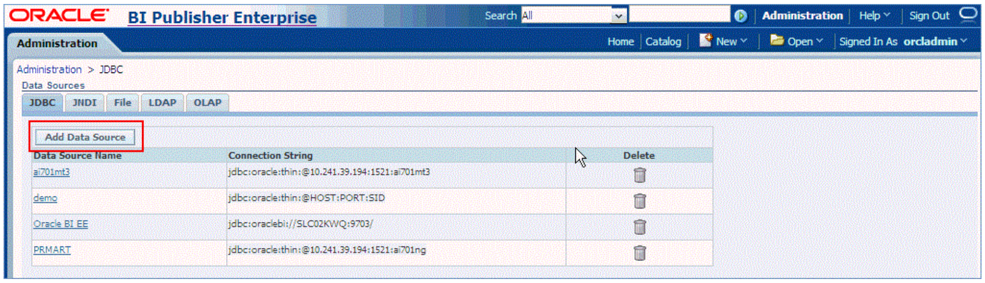


3. In the Data Sources section, click **JDBC Connection**.



The Data Sources screen appears.

4. Click **Add Data Source**.



Data Source Name	Connection String	Delete
ai701mt3	jdbc:oracle:thin:@10.241.39.194:1521:ai701mt3	🗑
demo	jdbc:oracle:thin:@HOST:PORT:SID	🗑
Oracle BI EE	jdbc:oraclebi://SLC02KWQ:9703/	🗑
PRMART	jdbc:oracle:thin:@10.241.39.194:1521:ai701ng	🗑

5. In the **Add Data Source** section:

   a. In the **Data Source Name** field, enter **PRMART**.

   b. From the **Driver Type** drop-down list, select the database.

      The **Database Driver Class** field is auto-populated based on the selected Driver Type.

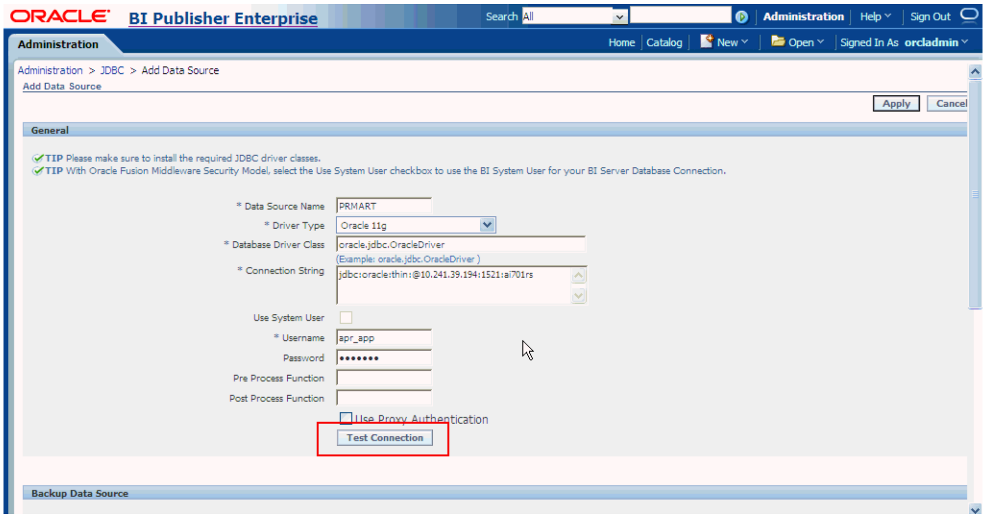
   c. In the **Connection String** field, enter the connection string.

      You must enter all the details in lower case in this field.

d. In the **Username** field, enter the username (Argus Insight application DB user, for example, apr_app) to connect to the database.

e. In the **Password** field, enter the password for the user.

f. Click **Test Connection**.


ORACLE BI Publisher Enterprise
Search All
Administration | Help | Sign Out
Administration
Home | Catalog | New | Open | Signed In As orcladmin
Administration > JDBC > Add Data Source
Add Data Source
Apply
Cancel
General
Backup Data Source

TIP Please make sure to install the required JDBC driver classes.
TIP With Oracle Fusion Middleware Security Model, select the Use System User checkbox to use the BI System User for your BI Server Database Connection.

* Data Source Name	PRMART
* Driver Type	Oracle 11g
* Database Driver Class	oracle.jdbc.OracleDriver (Example: oracle.jdbc.OracleDriver)
* Connection String	jdbc:oracle:thin:@10.241.39.194:1521:ai701rs
Use System User	□
* Username	apr_app
Password	•••••••
Pre Process Function	
Post Process Function	

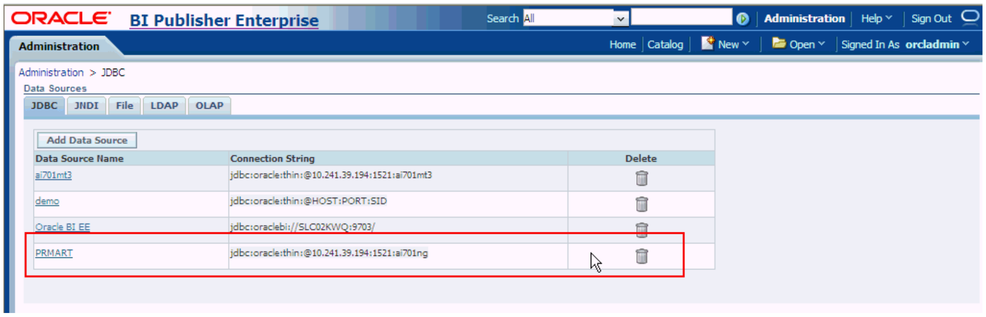
□ Use Proxy Authentication

Test Connection

If successful, a confirmation message appears.

6. Click **Apply**.

The **PRMART** Data Source in the list of already existing data source names appears.


ORACLE BI Publisher Enterprise
Search All
Administration | Help | Sign Out
Administration
Home | Catalog | New | Open | Signed In As orcladmin
Administration > JDBC
Data Sources
JDBC
JNDI
File
LDAP
OLAP
Add Data Source

Data Source Name	Connection String	Delete
ai701mt3	jdbc:oracle:thin:@10.241.39.194:1521:ai701mt3	🗑
demo	jdbc:oracle:thin:@HOST:PORT:SID	🗑
Oracle BI EE	jdbc:oraclebi://SLC02KWQ:9703/	🗑
PRMART	jdbc:oracle:thin:@10.241.39.194:1521:ai701ng	🗑

A connection between BIP and the database is successfully created.

6.2 Managing Users and Roles: BI Publisher Standalone Installation with BI Publisher Security

When you have uploaded the **Argus Insight.xdrz** file to BIP and created the JDBC connection, you can start creating the users for the BI Publisher Security Model.

This section introduces you to the steps that you need to execute to create users, assign the roles and permissions to those users, and configure server settings for the BI Publisher Security Model.

This section comprises the following sub-sections:

- Creating Users and Assigning Roles to Users
- Creating Roles, Adding Data Sources, and Assigning Roles

6.2.1 Creating Users and Assigning Roles to Users

To create users and assign the required roles to the users in the BIP Security Model, execute the following steps:

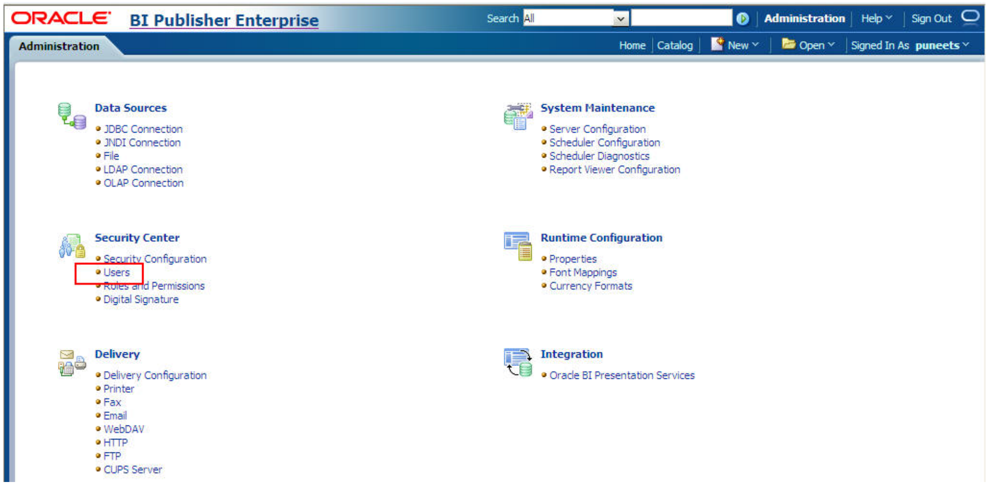
1. Log on to BIP using the administrator credentials.

   The BIP home page appears.

2. From top-menu, click **Administration**.

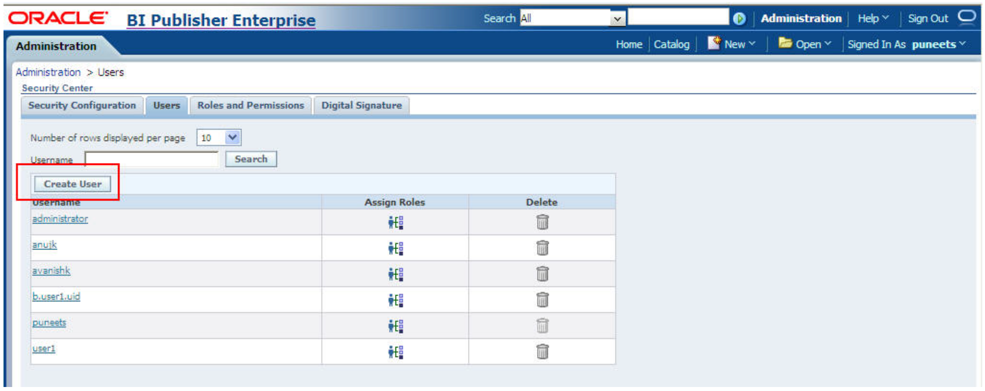
   Refer to Section 6.2 > Step 2.

3. In the Security Center section, click **Users**.



   The Users screen appears.

4. Click **Create User**.



Username	Assign Roles	Delete
administrator	👥	🗑
anuik	👥	🗑
avanishk	👥	🗑
b.user1.uid	👥	🗑
puneets	👥	🗑
user1	👥	🗑

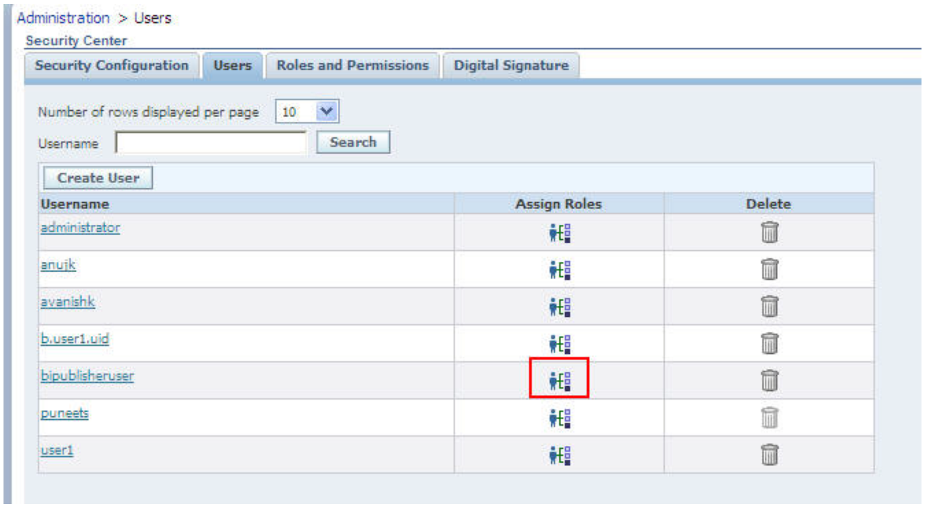
   The Create User screen appears.

5. In the **Username** field, enter the name of the user.
6. In the **Password** field, enter the password.
7. Click **Apply**.

   The name of the user appears in the list of existing users.

   When you have created the user, you need to assign the required roles to the user.

8. Click the Assign Roles icon corresponding to the user that you have created.



Number of rows displayed per page: 10

Username:

Username	Assign Roles	Delete
administrator		
anuik		
avanishk		
b.user1.uid		
bipublisheruser		
puneets		
user1		

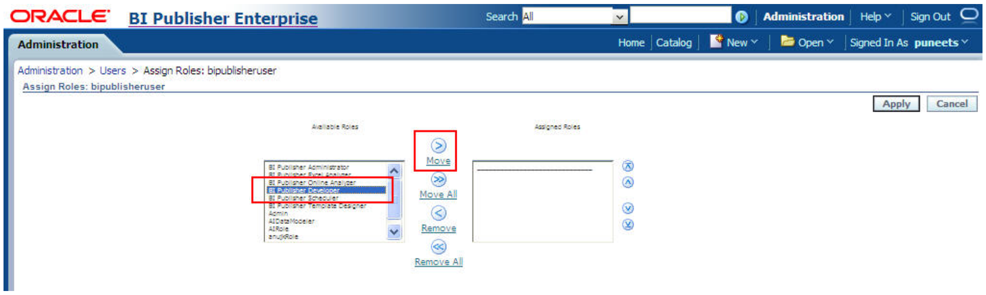
The Assign Roles screen appears.

The BIP system roles such as BI Publisher Administrator, BI Publisher Excel Analyzer, BI Publisher Online Analyzer, BI Publisher Developer, BI Publisher Scheduler, and BI Publisher Template Designer are available by default along with the custom roles (if any) that have been created by you.

See Section 6.2.2, "Creating Roles, Adding Data Sources, and Assigning Roles" for the steps to create custom roles.

For more information on system roles, refer to Understanding BI Publisher's Users, Roles, and Permissions in Administrator's Guide for Oracle Business Intelligence Publisher.

9. From the Available Roles section, select the role that you want to assign to the user, and click **Move(>)** to move the selected role to the Assigned Roles section.



Available Roles:

- BI Publisher Administrator
- BI Publisher Excel Analyzer
- BI Publisher Online Analyzer
- BI Publisher Developer
- BI Publisher Scheduler
- BI Publisher Template Designer
- Admin
- AIDataModeler
- AIRole
- anujkRole

10. Click **Apply**.

The selected roles are assigned to the user.

For the list of users that you need to configure using BIP, refer to Section 6.4, "Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model".

6.2.2 Creating Roles, Adding Data Sources, and Assigning Roles

In addition to creating users and assigning them the required roles, you also need to create certain roles, add data sources, and assign them the required roles.

To create roles, add data sources, and assign them the required roles, execute the following steps:

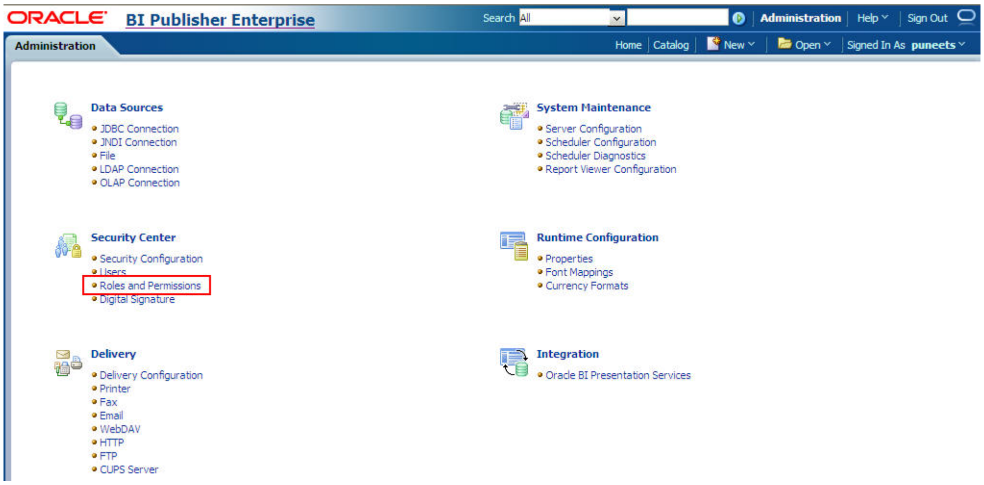
1. Log on to BIP using the administrator credentials.

The BIP home page appears.

2. From the top-menu, click **Administration**.

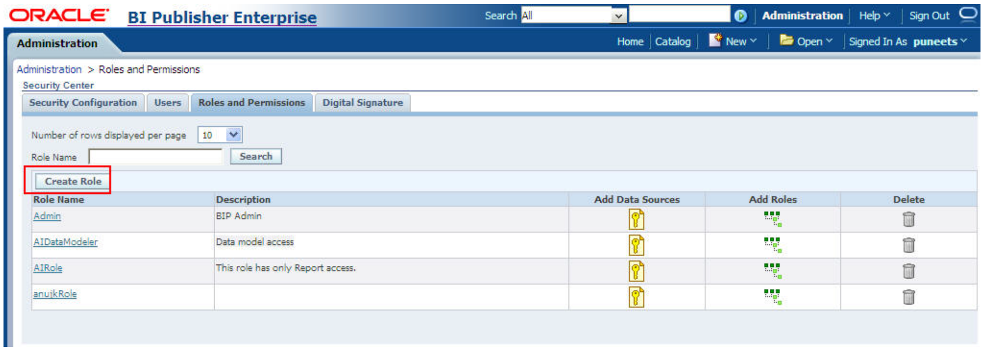
   Refer to Section 6.2 > Step 2.

3. In the Security Center section, click **Roles and Permissions**.



The Roles and Permissions screen appears.

4. Click **Create Role**.



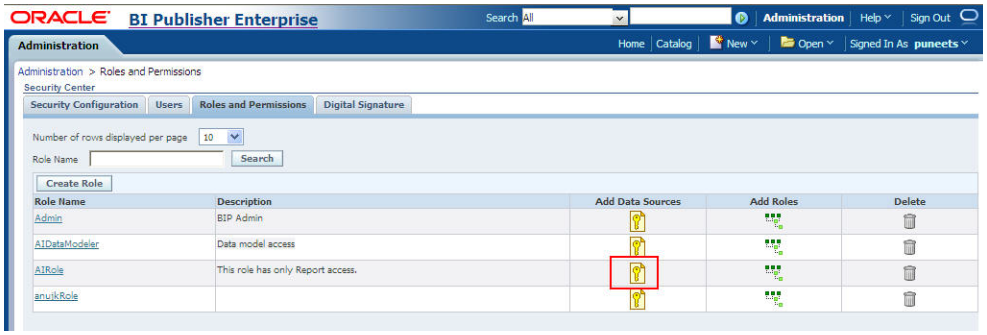
Role Name	Description	Add Data Sources	Add Roles	Delete
Admin	BIP Admin			
AIDataModeler	Data model access			
AIRole	This role has only Report access.			
anujkRole				

The Create Role screen appears.

5. Enter the **Name** and **Description** of the role, and click **Apply**.

   The new role is created and appears in the list of existing roles in the Roles and Permissions screen.

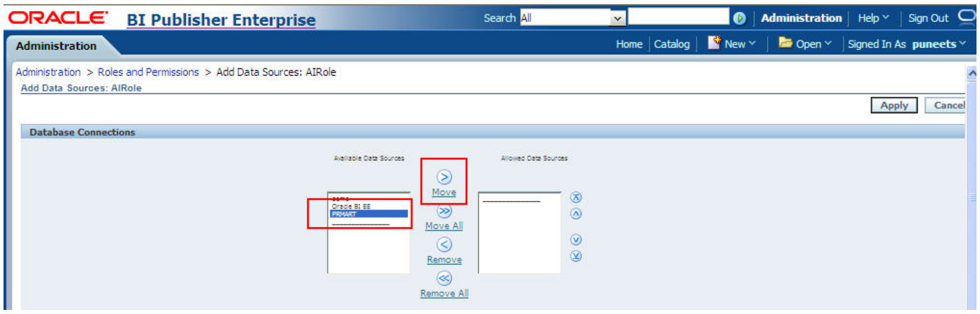
6. Click **Add Data Sources** icon, corresponding to the role which you have just created.



Role Name	Description	Add Data Sources	Add Roles	Delete
Admin	BIP Admin			
AIDataModeler	Data model access			
AIRole	This role has only Report access.			
anujkRole				

The Add Data Sources screen appears.

7. Form Available Data Sources section, select **PRMART**, and click **Move(>)** to move it to the Allowed Data Sources section.



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

   The Roles and Permissions screen appears.

   See Section 6.1, "Creating PRMART JDBC Connection" for the steps to create the JDBC connection.

9. Click the **Add Roles** icon, corresponding to the role which you have just created to add the required roles.

   The Add Roles screen appears.

10. From the Available Roles section, select the roles that you want to include, and click **Move(>)** to move the selected roles to the Included Roles section.

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

    For more information, refer to the Configuring Users, Roles, and Data Access section in the Oracle BIP Administrator's Guide.

    For the list of roles that you need to configure using BIP, refer to Section 6.4, "Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model".

6.3 Managing Users and Roles: BI Publisher Standalone Installation with OFM Security

This section introduces you with the steps that you need to execute to create users, assign the roles and permissions to those users, and configure server settings for the Oracle Fusion Middleware (OFM) Security Model.

This section comprises the following sub-sections:

- Creating Users and Assigning Roles to Users
- Creating Roles, Adding Data Sources, and Assigning Roles in WebLogic Enterprise Manager
- Creating Application Policy
- Uploading the Argus Insight.xdrz file to BIP

6.3.1 Creating Users and Assigning Roles to Users

Creating users for LDAP or SSO users is done using the LDAP servers which is beyond the scope of this manual.

For the list of users that need to be configured, refer to the Section 6.4, "Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model".

6.3.2 BI Publisher Standalone Installation in OFM Security

This section provides the steps to create roles, policies, users, and groups in OFM (Oracle Fusion Middleware) Security for BIP Standalone Installation.

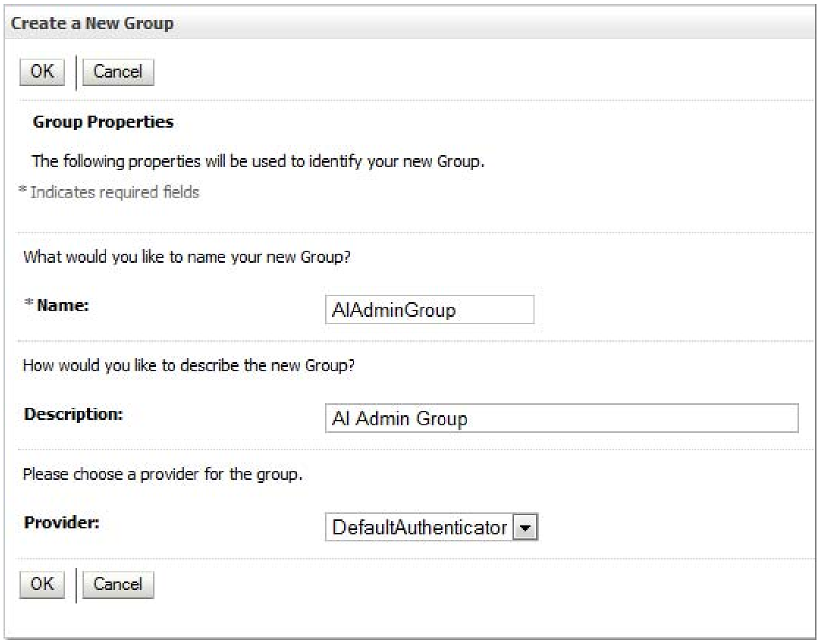
- Creating Users and Groups
- Creating Roles and Policies

6.3.2.1 Creating Users and Groups

To create users and assigning groups:

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

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



Create a New Group

Group Properties

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

* Indicates required fields

What would you like to name your new Group?

* Name: AIAdminGroup

How would you like to describe the new Group?

Description: AI Admin Group

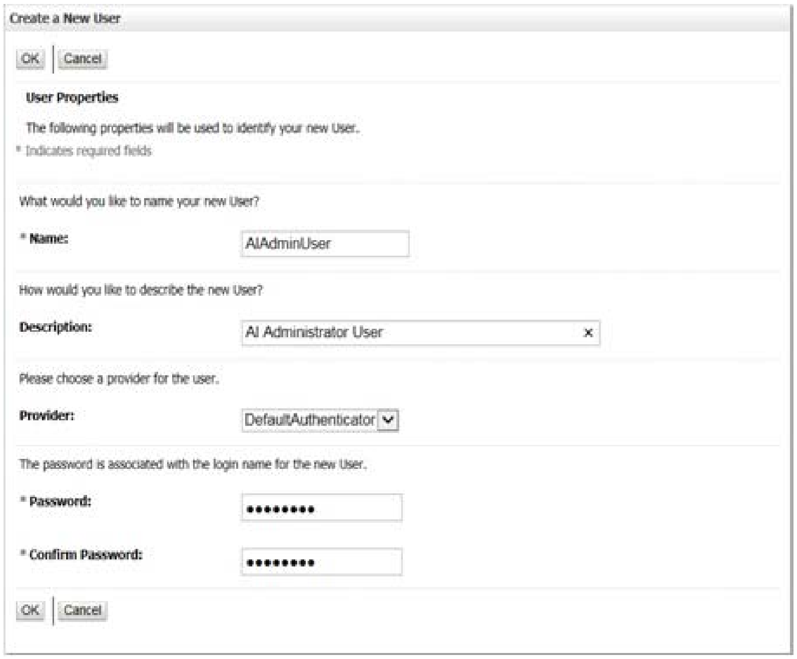
Please choose a provider for the group.

Provider: DefaultAuthenticator

To create users in the Fusion Middleware Control:

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

   The Create a New User dialog box appears.



Create a New User

User Properties

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

* Indicates required fields

What would you like to name your new User?

* Name: AIAdminUser

How would you like to describe the new User?

Description: AI Administrator User

Please choose a provider for the user.

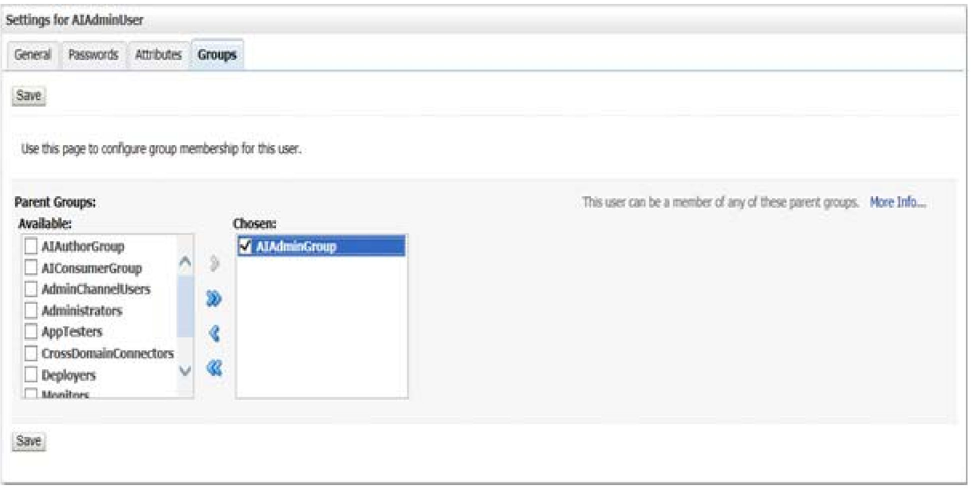
Provider: DefaultAuthenticator

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

* Password: ••••••••

* Confirm Password: ••••••••

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**.



Settings for AIAdminUser

Use this page to configure group membership for this user.

Parent Groups:

This user can be a member of any of these parent groups. More Info...

Available:

- □ AIAuthorGroup
- □ AIConsumerGroup
- □ AdminChannelUsers
- □ Administrators
- □ AppTesters
- □ CrossDomainConnectors
- □ Deployers
- □ Monitors

Chosen:

- ☑ AIAdminGroup

Note: For more details, refer to *Section 2.5.2 Managing Users and Groups Using the Default Authentication Provider* in *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*.

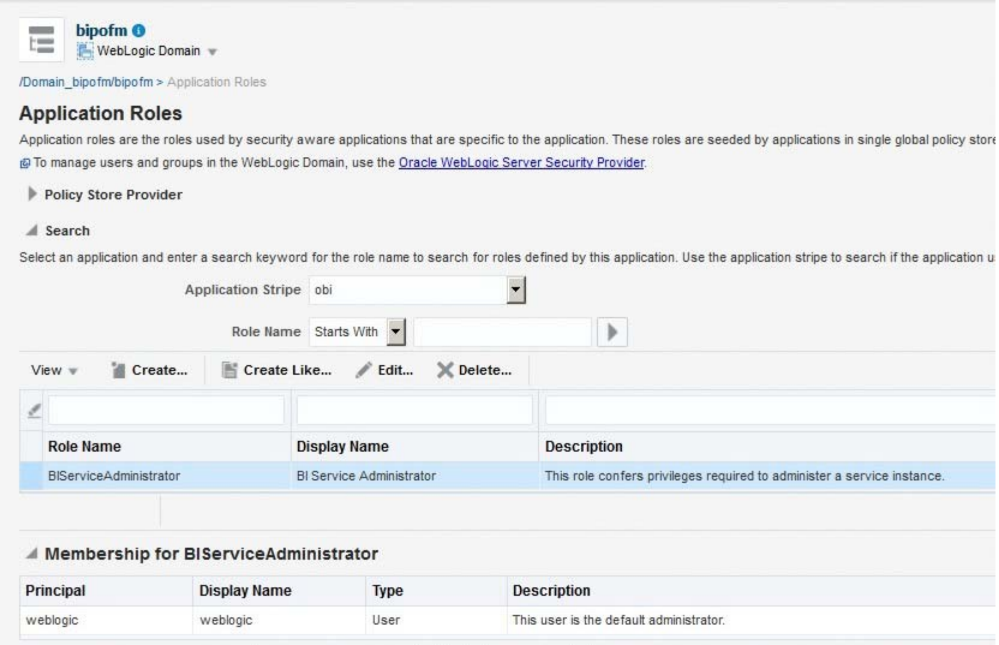
6.3.2.2 Creating Roles and Policies

To create new application roles:

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

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

   The default role available in clean slate installation appears.



Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Select an application and enter a search keyword for the role name to search for roles defined by this application. Use the application stripe to search if the application u

Application Stripe obi

Role Name Starts With

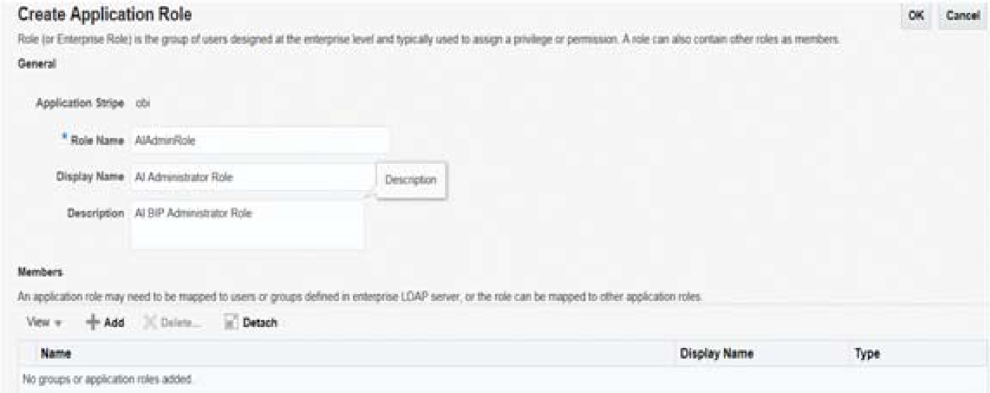
Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.

Membership for BIServiceAdministrator

Principal	Display Name	Type	Description
weblogic	weblogic	User	This user is the default administrator.

4. Click **Create**.

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



Create Application Role

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically used to assign a privilege or permission. A role can also contain other roles as members.

General

Application Stripe obi

* Role Name AIAdminRole

Display Name AI Administrator Role

Description AI BIP Administrator Role

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

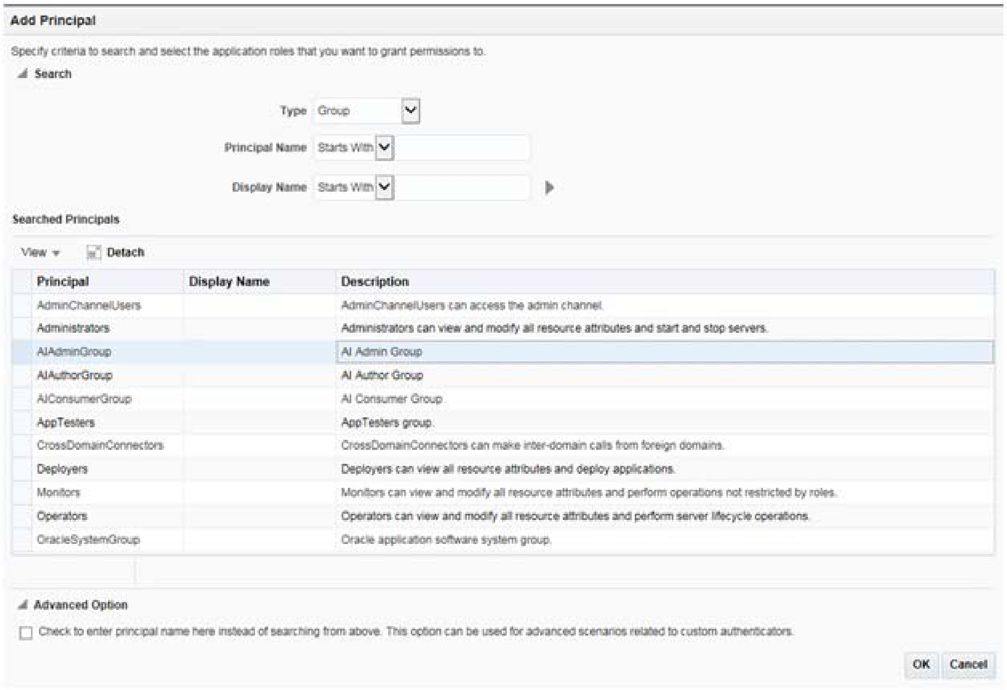
Name	Display Name	Type
No groups or application roles added		

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

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

A list of principals appears.

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



Add Principal

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

Search

Type: Group

Principal Name: Starts With

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
AdminChannelUsers		AdminChannelUsers can access the admin channel.
Administrators		Administrators can view and modify all resource attributes and start and stop servers.
AIAdminGroup		AI Admin Group
AIAuthorGroup		AI Author Group
AIConsumerGroup		AI Consumer Group
AppTesters		AppTesters group.
CrossDomainConnectors		CrossDomainConnectors can make inter-domain calls from foreign domains.
Deployers		Deployers can view all resource attributes and deploy applications.
Monitors		Monitors can view and modify all resource attributes and perform operations not restricted by roles.
Operators		Operators can view and modify all resource attributes and perform server lifecycle operations.
OracleSystemGroup		Oracle application software system group.

Advanced Option

□ Check to enter principal name here instead of searching from above. This option can be used for advanced scenarios related to custom authenticators.

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

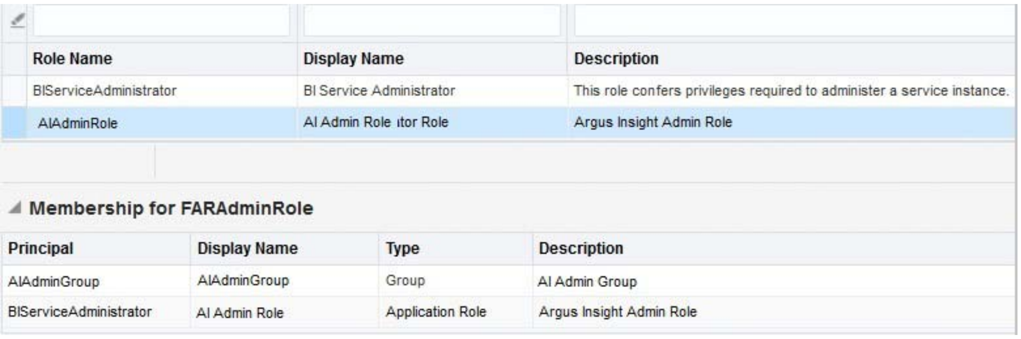
The Add Principal dialog box appears.

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

A list of principals appears.

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

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

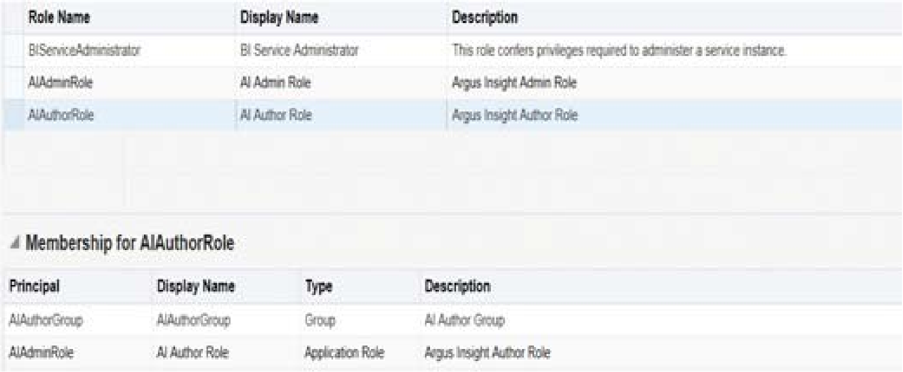


Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role ıtor Role	Argus Insight Admin Role

Membership for FARAdminRole

Principal	Display Name	Type	Description
AIAdminGroup	AIAdminGroup	Group	AI Admin Group
BIServiceAdministrator	AI Admin Role	Application Role	Argus Insight Admin Role

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

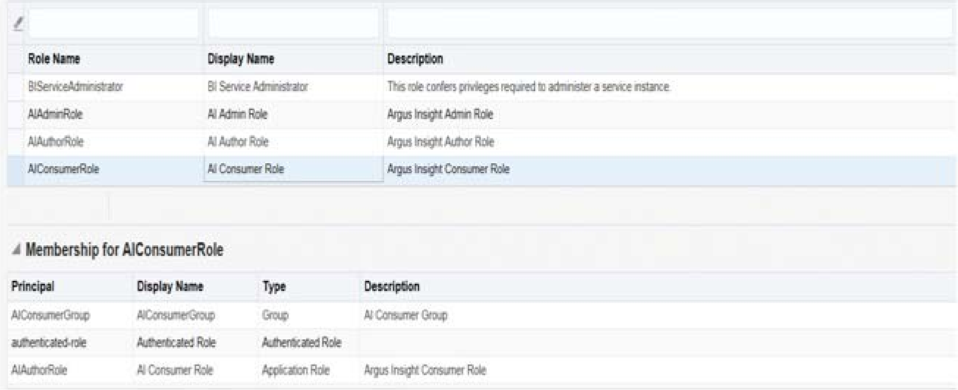


Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role	Argus Insight Admin Role
AIAuthorRole	AI Author Role	Argus Insight Author Role

Membership for AIAuthorRole

Principal	Display Name	Type	Description
AIAuthorGroup	AIAuthorGroup	Group	AI Author Group
AIAdminRole	AI Author Role	Application Role	Argus Insight Author Role

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



Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role	Argus Insight Admin Role
AIAuthorRole	AI Author Role	Argus Insight Author Role
AIConsumerRole	AI Consumer Role	Argus Insight Consumer Role

Membership for AIConsumerRole

Principal	Display Name	Type	Description
AIConsumerGroup	AIConsumerGroup	Group	AI Consumer Group
authenticated-role	Authenticated Role	Authenticated Role	
AIAuthorRole	AI Consumer Role	Application Role	Argus Insight Consumer Role

---

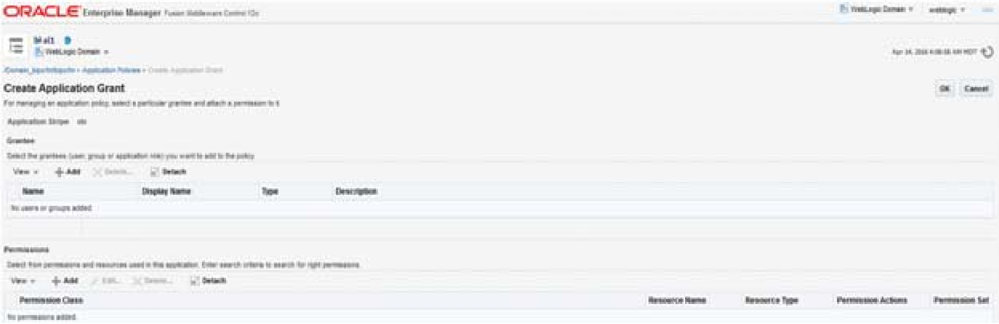
Note: For more details, refer *Section 2.8.3.1 Creating Application Roles Using Fusion Middleware Control* in *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*

To create new application policy:

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

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

   The Create Application Grant dialog box appears.



Create Application Grant

For managing an application policy, select a particular grantee and attach a permission to it

Application Stripe obi

Grantee

Select the grantees (user, group or application role) you want to add to the policy

Name	Display Name	Type	Description
No users or groups added			

Permissions

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

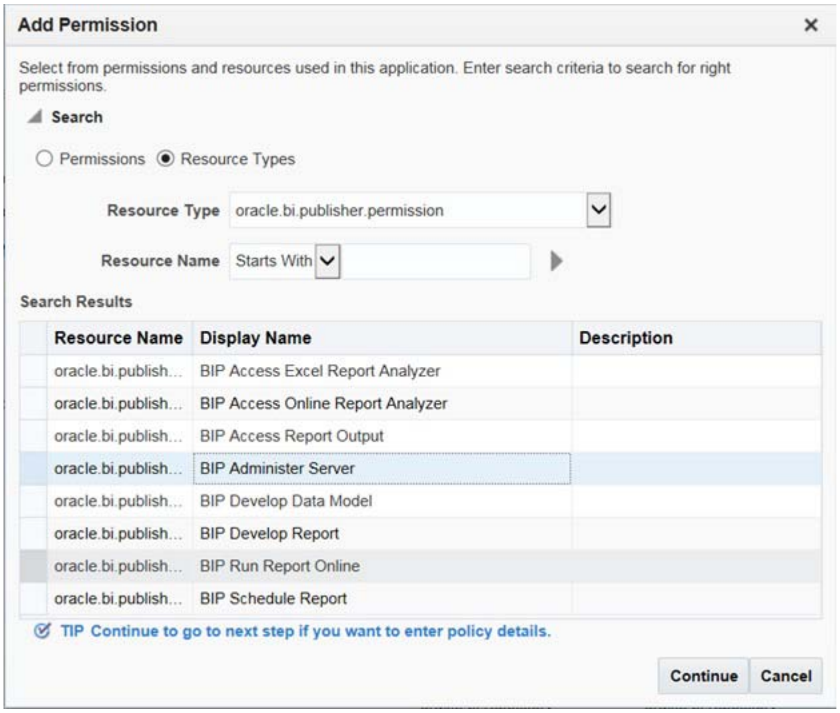
Permission Class	Resource Name	Resource Type	Permission Actions	Permission Set
No permissions added				

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 **AIAdminRole**, and click **OK**.
7. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.



Add Permission ×

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

◢ Search

○ Permissions ● Resource Types

Resource Type: oracle.bi.publisher.permission

Resource Name: Starts With ▶

Search Results

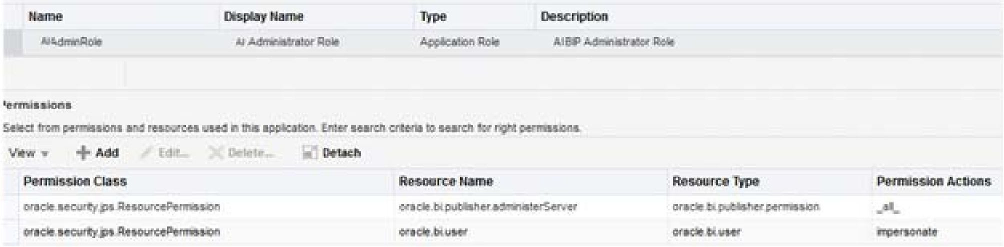
Resource Name	Display Name	Description
oracle.bi.publish...	BIP Access Excel Report Analyzer	
oracle.bi.publish...	BIP Access Online Report Analyzer	
oracle.bi.publish...	BIP Access Report Output	
oracle.bi.publish...	BIP Administer Server	
oracle.bi.publish...	BIP Develop Data Model	
oracle.bi.publish...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

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

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. Add Resource Name as **oracle.bi.user** with **Impersonate** permission.

    The new AI Admin policy has all the permissions.



Name	Display Name	Type	Description
AIAdminRole	AI Administrator Role	Application Role	AIBIP Administrator Role

'ermissions

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

Permission Class	Resource Name	Resource Type	Permission Actions
oracle.security.jps.ResourcePermission	oracle.bi.publisher.administerServer	oracle.bi.publisher.permission	_all_
oracle.security.jps.ResourcePermission	oracle.bi.user	oracle.bi.user	impersonate

---

Note: Make sure all the fields are either selected or entered manually.

---

13. Repeat from Step 4 to Step 12, to add the following:

Name	Grantee	Resource Permissions
AI Author	AIAuthorRole	BIP Develop Report BIP Develop Data Model
AI Consumer	AIConsumerRole	BIP Access Excel Report Analyzer BIP Access Online Report Analyzer BIP Access Report Output BIP Schedule Report

> **Note:** For more details, refer to *Section 2.8.3.2 Creating Application Policies Using Fusion Middleware Control* from *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*.

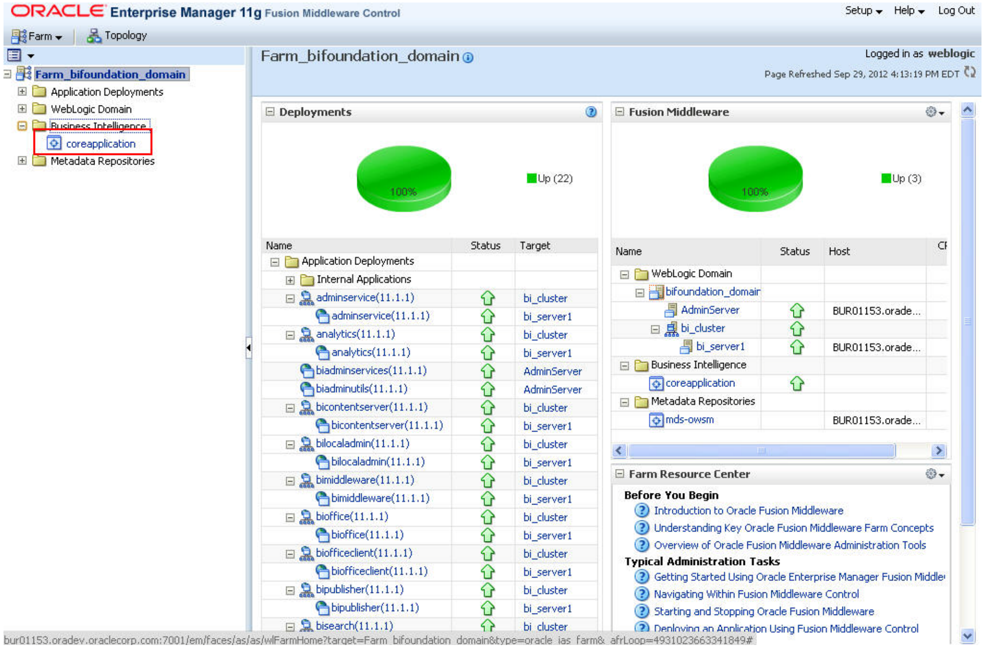
6.3.3 Creating Roles, Adding Data Sources, and Assigning Roles in WebLogic Enterprise Manager

To create roles, add data sources, and assign roles in WebLogic Enterprise Manager, execute the following procedure:

1. Log on to the Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.

2. In the left pane, expand the **Business Intelligence** folder, and click **coreapplication**.



Farm_bifoundation_domain

Deployments

Name	Status	Target
Application Deployments		
Internal Applications		
adminservice(11.1.1)	⇧	bi_cluster
adminservice(11.1.1)	⇧	bi_server1
analytics(11.1.1)	⇧	bi_cluster
analytics(11.1.1)	⇧	bi_server1
biadminservices(11.1.1)	⇧	AdminServer
biadminutils(11.1.1)	⇧	AdminServer
bicontentserver(11.1.1)	⇧	bi_cluster
bicontentserver(11.1.1)	⇧	bi_server1
bilocaladmin(11.1.1)	⇧	bi_cluster
bilocaladmin(11.1.1)	⇧	bi_server1
bimiddleware(11.1.1)	⇧	bi_cluster
bimiddleware(11.1.1)	⇧	bi_server1
bioffice(11.1.1)	⇧	bi_cluster
bioffice(11.1.1)	⇧	bi_server1
biofficeclient(11.1.1)	⇧	bi_cluster
biofficeclient(11.1.1)	⇧	bi_server1
bipublisher(11.1.1)	⇧	bi_cluster
bipublisher(11.1.1)	⇧	bi_server1
bisearch(11.1.1)	⇧	bi_cluster

Fusion Middleware

Name	Status	Host	CI
WebLogic Domain			
bifoundation_domair			
AdminServer	⇧	BUR01153.oracle...	
bi_cluster	⇧		
bi_server1	⇧	BUR01153.oracle...	
Business Intelligence			
coreapplication	⇧		
Metadata Repositories			
mds-owsm		BUR01153.oracle...	

Farm Resource Center

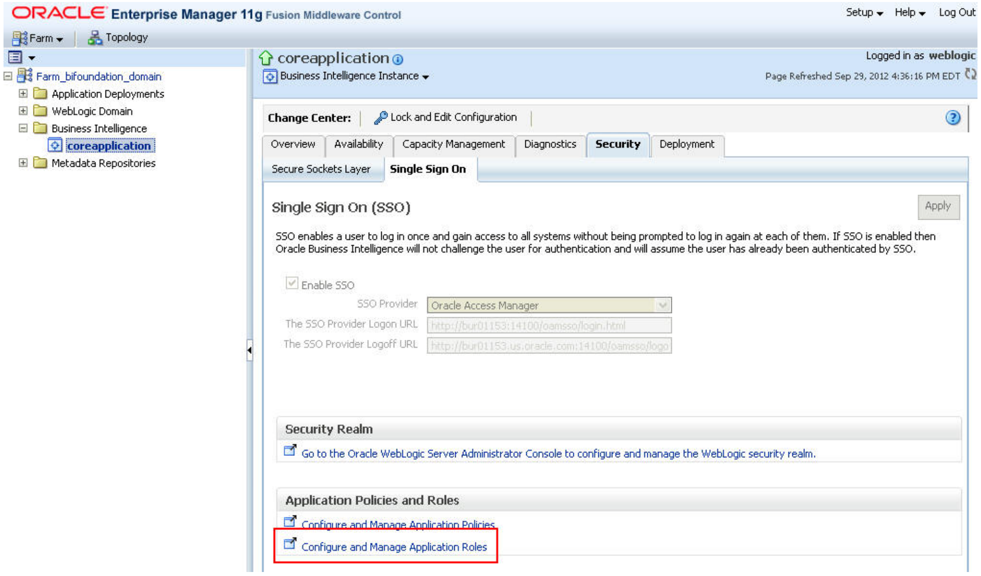
Before You Begin
- Introduction to Oracle Fusion Middleware
- Understanding Key Oracle Fusion Middleware Farm Concepts
- Overview of Oracle Fusion Middleware Administration Tools

Typical Administration Tasks
- Getting Started Using Oracle Enterprise Manager Fusion Middle
- Navigating Within Fusion Middleware Control
- Starting and Stopping Oracle Fusion Middleware
- Deploying an Application Using Fusion Middleware Control

bur01153.oradev.oraclecorp.com:7001/em/faces/as/as/wlFarmHome?target=Farm_bifoundation_domain&type=oracle_ias_farm&_afrLoop=4931023663341849#

   The Coreapplication screen appears in the right pane.

3. In the Application Policies and Roles section, click **Configure and Manage Application Roles**.



Logged in as weblogic

Page Refreshed Sep 29, 2012 4:36:16 PM EDT

Single Sign On (SSO)

SSO enables a user to log in once and gain access to all systems without being prompted to log in again at each of them. If SSO is enabled then Oracle Business Intelligence will not challenge the user for authentication and will assume the user has already been authenticated by SSO.

☑ Enable SSO

SSO Provider: Oracle Access Manager

The SSO Provider Logon URL: http://bur01153:14100/oamsso/login.html

The SSO Provider Logoff URL: http://bur01153.us.oracle.com:14100/oamsso/logo

Go to the Oracle WebLogic Server Administrator Console to configure and manage the WebLogic security realm.

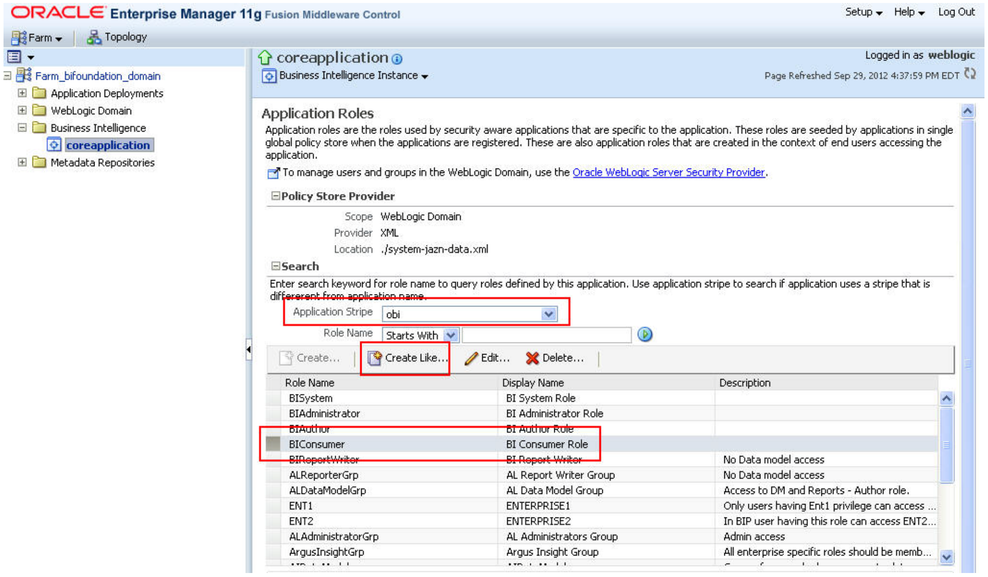
Configure and Manage Application Policies

Configure and Manage Application Roles

The Application Roles screen appears.

4. From the **Application Stripe** drop-down list, select the required application stripe.

5. Select any existing role (for example, BIConsumer), and click **Create Like**.



Logged in as weblogic

Page Refreshed Sep 29, 2012 4:37:59 PM EDT

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Scope: WebLogic Domain

Provider: XML

Location: ./system-jazn-data.xml

Search

Enter search keyword for role name to query roles defined by this application. Use application stripe to search if application uses a stripe that is differerent from application name.

Application Stripe: obi

Role Name: Starts With

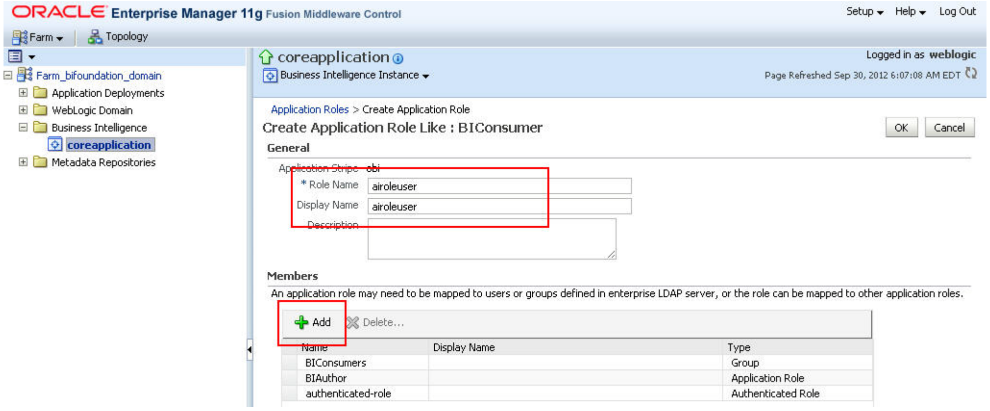
Role Name	Display Name	Description
BISystem	BI System Role	
BIAdministrator	BI Administrator Role	
BIAuthor	BI Author Role	
BIConsumer	BI Consumer Role	
BIReportWriter	BI Report Writer	No Data model access
ALReporterGrp	AL Report Writer Group	No Data model access
ALDataModelGrp	AL Data Model Group	Access to DM and Reports - Author role.
ENT1	ENTERPRISE1	Only users having Ent1 privilege can access ...
ENT2	ENTERPRISE2	In BIP user having this role can access ENT2...
ALAdministratorGrp	AL Administrators Group	Admin access
ArgusInsightGrp	Argus Insight Group	All enterprise specific roles should be memb...

The Create Application Role screen appears.

6. In **Role Name** field, enter the name of the role.

7. Optionally, enter the **Display Name** and **Description** for the role.

8. To add any existing application role/group/user to the new role, click **Add**.



Create Application Role Like : BIConsumer

General

Application Stripe obi

* Role Name airoleuser

Display Name airoleuser

Description

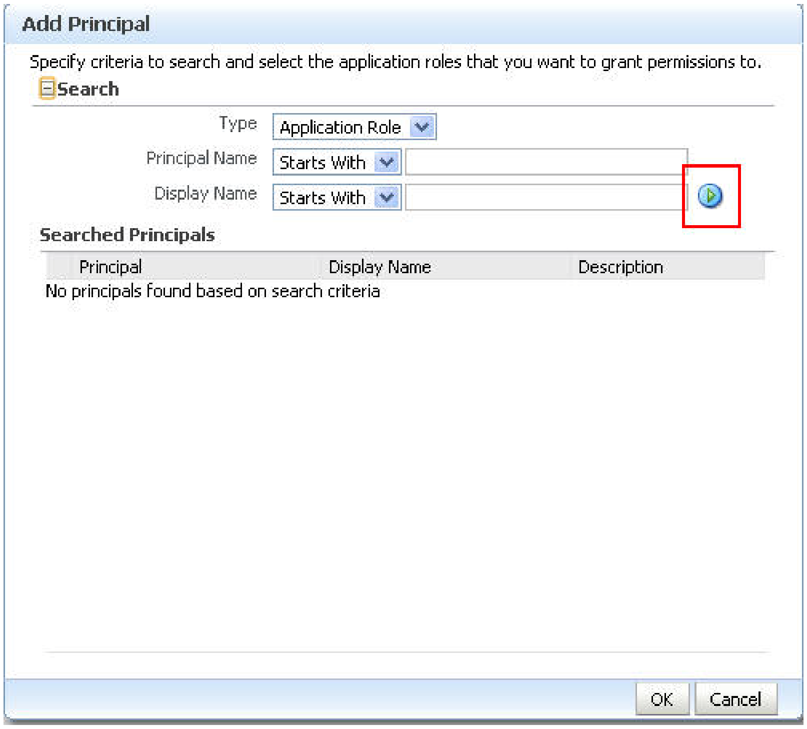
Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Name	Display Name	Type
BIConsumers		Group
BIAuthor		Application Role
authenticated-role		Authenticated Role

The Add Principal screen appears.

9. To display the list of all the roles, groups, and users that are created in LDAP server, click the > icon next to the **Display Name** field.



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

Type Application Role

Principal Name Starts With

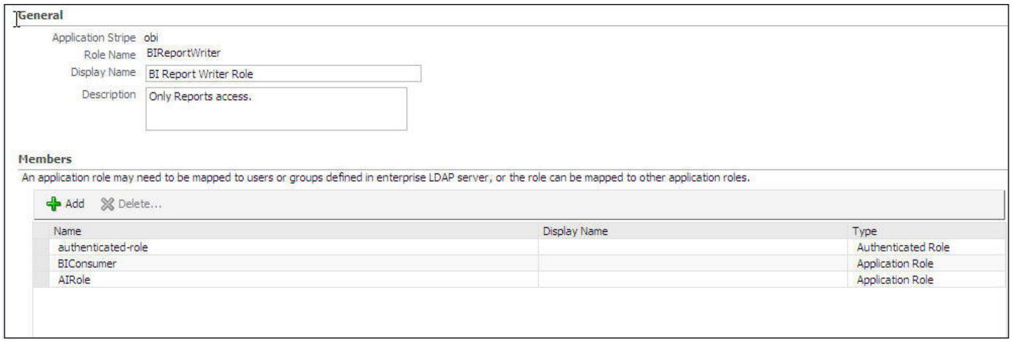
Display Name Starts With

Searched Principals

Principal	Display Name	Description
No principals found based on search criteria		

10. Select the name of the role, group, or user that you want to add to the new role, and click **OK**.

    For example, for the **BIReportWriter** role, **BIConsumer** and **authenticated-role** are mandatory members. Besides that, the **AIRole** must also be a part of the **BIReportWriter** Role. These roles are displayed in the Members section of the Create Application screen.



General

Application Stripe obi

Role Name BIReportWriter

Display Name BI Report Writer Role

Description Only Reports access.

Members

An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Name	Display Name	Type
authenticated-role		Authenticated Role
BIConsumer		Application Role
AIRole		Application Role

Note: The **BIReportWriter** role must be added to the **BIReportWriter** application policy. Refer to Section 6.3.4, "Creating Application Policy" for the steps to create the application policy for the **BIReportWriter** role.

11. Repeat steps 8 to 10 to add more roles, users, and groups to the new role.
12. On Create Application Role screen, click **OK** to save the changes.

    When you have created the role and added the required list of users, roles, and groups to the new role, you must add the **PRMART** data source to the new role.
13. Log on to BIP using the administrator credentials.

    The BIP home page appears.
14. From top-menu, click **Administration**.

    Refer to Section 6.2 > Step 2.
15. In Security Center section, click **Roles and Permissions**.

    The Roles and Permission screen appears.

    You can view the name of the new role which you have just created in the list of role names.
16. Click the **Add Data Sources** icon corresponding to the name of the new role.

    The Add Data Sources screen appears.
17. From the Available Data Sources section, select **PRMART**, and click the **Move (>)** icon to move the PRMART data source to the Allowed Data Sources section.
18. Click **Apply** to save the changes.

    For more information, refer to the Oracle BIP Administrator's Guide > Creating Application Roles Using Fusion Middleware Control section.

    For the list of roles that need to be configured, refer to the Section 6.4, "Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model".

6.3.4 Creating Application Policy

Once you have created the new role and assigned the required roles, users, and data sources to the role, you also need to create the application policy for the new role.

Before creating a BI Publisher policy, you must have created an empty role in the Enterprise Manager.

Note: The steps mentioned in this section are valid for creating **BIReportWriter** application policy.

To create the application policy for the new role, execute the following steps:

1. Log on to the Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.

2. In the left pane, expand the **Business Intelligence** folder, and click **coreapplication**.

   The Coreapplication screen appears in the right pane.

3. In the Application Policies and Roles section, click **Configure and Manage Application Policies**.

   The Application Policies screen appears.

4. From the **Application Stripe** drop-down list, select **obi**.

5. Select the **BIAuthor** policy, and click **Create Like**.

   The Create Application Grant Like screen appears with the **Grantee** and **Permissions** sections.

6. In the Grantee section, click **Add**.

   This displays the **Add Principal** Screen.

7. To retrieve the list of all the available application roles, click the **>** icon next to the **Principal Name** field.

8. From the Searched Principals section, select the name of the role (for example, BIReportWriter), and click **OK**.

   The Create Application Grant Like screen appears.

9. From the list of Permission Classes, select the **developDataModel** resource name, and click **Delete.**

10. Click **OK** to apply the changes.

6.3.5 Uploading the Argus Insight.xdrz file to BIP

Note: You must be logged in to BIP with the BI Admin User credentials to be able to upload the **Argus Insight.xdrz** file.

To upload the **Argus Insight.xdrz** file to BIP, execute the following steps:

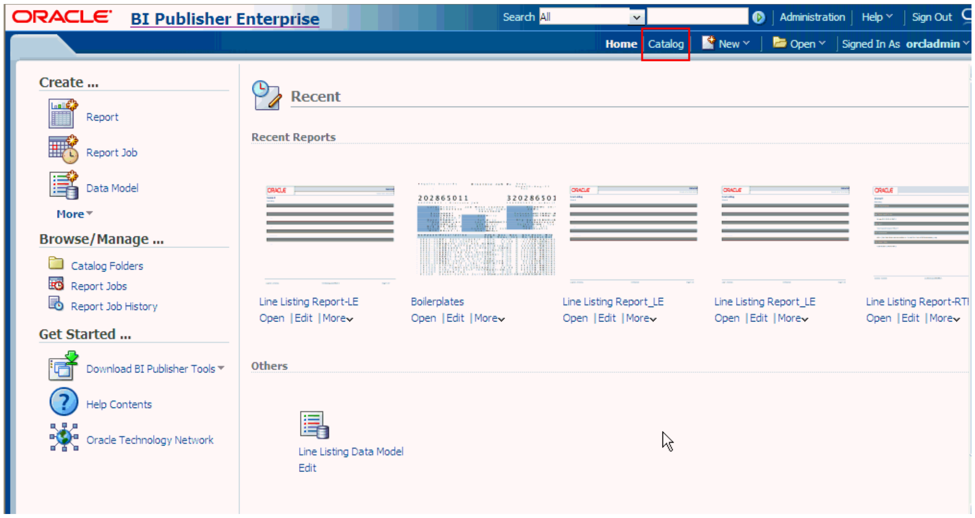
1. Copy the **Argus Insight.xdrz** file from the following location on the Argus Insight Web Server to the local file system:

   Drive:\<Argus Insight Installation Folder>\ArgusInsight\BIP\Repository

2. Log on to BIP using the BI Admin User credentials.

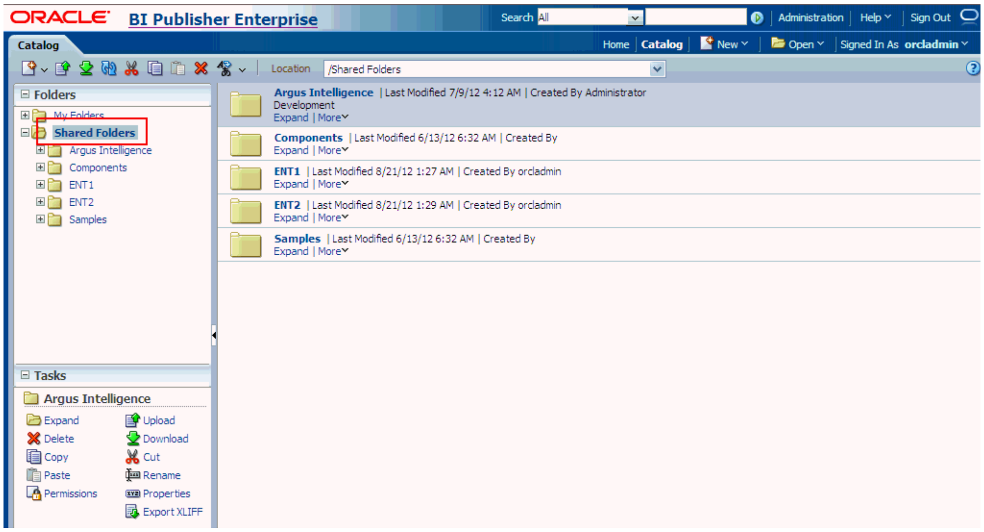
   The BIP home page appears.

3. From the menu bar, click **Catalog**.



The Catalog screen with the **Folders** and **Tasks** sections appears.

4. From Folders section in the left pane, click **Shared Folders**.



Argus Intelligence | Last Modified 7/9/12 4:12 AM | Created By Administrator
Development
Expand | More

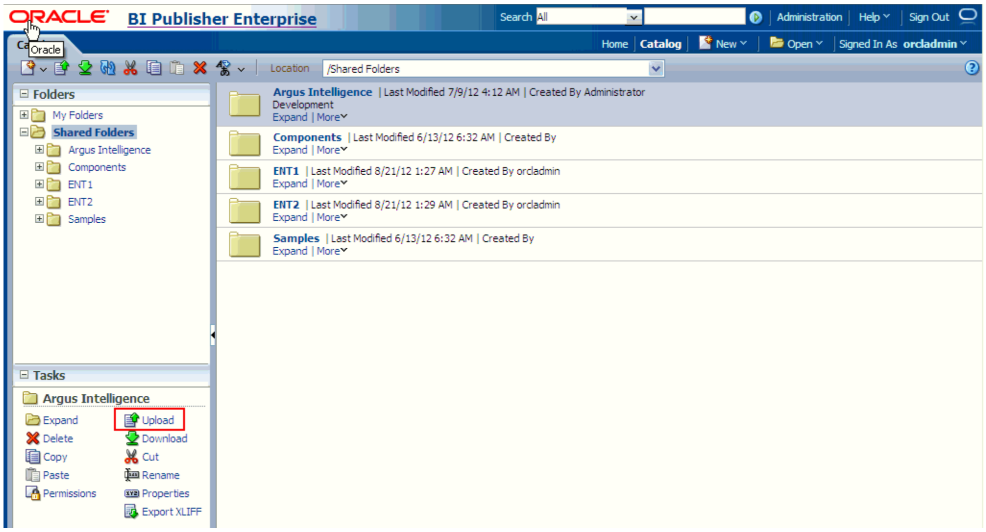
Components | Last Modified 6/13/12 6:32 AM | Created By
Expand | More

ENT1 | Last Modified 8/21/12 1:27 AM | Created By orcladmin
Expand | More

ENT2 | Last Modified 8/21/12 1:29 AM | Created By orcladmin
Expand | More

Samples | Last Modified 6/13/12 6:32 AM | Created By
Expand | More

5. From Tasks section in the left pane, click **Upload**.



Argus Intelligence | Last Modified 7/9/12 4:12 AM | Created By Administrator
Development
Expand | More

Components | Last Modified 6/13/12 6:32 AM | Created By
Expand | More

ENT1 | Last Modified 8/21/12 1:27 AM | Created By orcladmin
Expand | More

ENT2 | Last Modified 8/21/12 1:29 AM | Created By orcladmin
Expand | More

Samples | Last Modified 6/13/12 6:32 AM | Created By
Expand | More

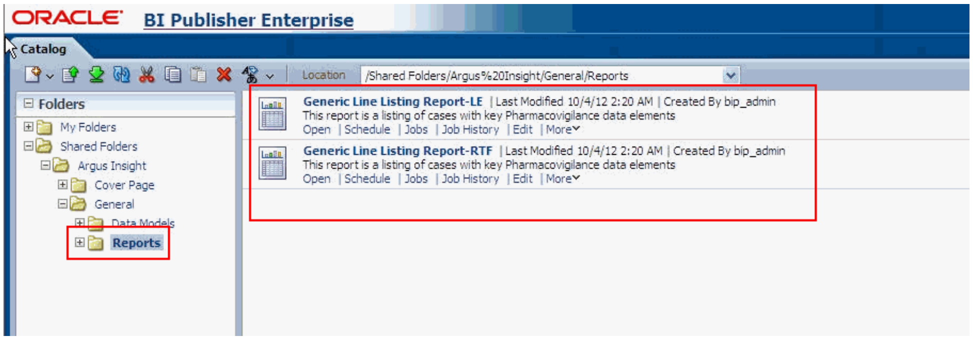
The Upload dialog box appears.

6. Click **Browse** and navigate to the location where you have saved the **Argus Insight.xdrz** file on the local file system.

7. Click **Upload**.

   After successful upload, an **Argus Insight** folder is created in **Shared Folders**.

8. Expand the **Argus Insight** folder to verify that the **Generic Line Listing Data Model** exists in the **Data Models** sub-folder and the **Generic Line Listing Report** in **LE** and **RTF** formats exists in the **Reports** sub-folder.


ORACLE BI Publisher Enterprise
Catalog
Location /Shared Folders/Argus%20Insight/General/Reports
Folders
My Folders
Shared Folders
Argus Insight
Cover Page
General
Data Models
Reports

Generic Line Listing Report-LE | Last Modified 10/4/12 2:20 AM | Created By bip_admin
This report is a listing of cases with key Pharmacovigilance data elements
Open | Schedule | Jobs | Job History | Edit | More

Generic Line Listing Report-RTF | Last Modified 10/4/12 2:20 AM | Created By bip_admin
This report is a listing of cases with key Pharmacovigilance data elements
Open | Schedule | Jobs | Job History | Edit | More

6.4 Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model

This section lists the names of the <Admin Users> and roles that you need to configure using the steps given in Section 6.2, "Managing Users and Roles: BI Publisher Standalone Installation with BI Publisher Security" and Section 6.3, "Managing Users and Roles: BI Publisher Standalone Installation with OFM Security".

Table 6–1 Configuring BIP Users: Oracle Fusion Middleware Security Model

User	Description
BI Admin User	An Admin user refers to the user who has BI Publisher administrative rights. This user should belong to the **BIAdministration** functional role.

Table 6–1 (Cont.) Configuring BIP Users: Oracle Fusion Middleware Security Model

User	Description
Data Modeler Users	An Argus Insight Data Model user refers to the user who should have access to both **Data Models** and **Reports** in the **Argus Insight** folder. This user should belong to **AIDataModeler** custom role. There are Enterprise specific Modeler users, who have access to **Data Models** and **Reports** in Enterprise specific folders and **Argus Insight** folder. These users should have Enterprise specific Modeler roles assigned to them. This user should belong to Enterprise specific Modeler roles.
Users	An Argus Insight Role (AIRole) user refers to the user who should have access to **Reports** only, and should have Read-only access to the Data Model which is required to create the reports. This user should belong to **AIRole**. There can be users who have access to reports of specific Enterprises. These users can Read/Write reports in **Enterprise specific Report** folder and **Argus Insight Report** folder. However, these users have Read-only access to the Data Models in the Enterprise specific **Data Model** and Argus Insight **Data Model** folder. This user should belong to Enterprise specific Report roles.
Global Admin Users	An AI Admin Role user should have full access to the **Argus Insight** folder (Read/Write/Delete). An Enterprise specific Admin user should have full access to the Enterprise specific folders (Read/Write/Delete) and **Argus Insight folder** (Read/Write/Delete).

6.4.1 Configuring BIP Roles

The following table illustrates the roles that you need to configure using BIP:

Table 6–2 Configuring BIP Roles

Role	Users/Roles to be added
BIAdministration (Functional Role)	Super user who has full access to any folder and BIP Administration access
AIRole	All Argus Insight role users, **AIDataModelerRole**, and All Enterprise Report Roles (for specific enterprises)
AIDataModelerRole	All AI Data Modeler Users, All Enterprise Modeler Roles, and **AIAdminRole**
Enterprise Report Role	Users that belong to a specific Enterprise with **Reports** access and Enterprise Modeler Role
Enterprise Modeler Role	Users that belong to a particular Enterprise with both **Data Models** and **Reports** access
Enterprise Admin Role	Enterprise specific Admin users. These users should have full access to the Enterprise specific folders.
AIAdminRole	Any User with this role should have full access to the Argus Insight Folder. The Enterprise Admin Role should be added to this role.
BIAdministrator (Functional Role)	BI Admin User
BIAuthor (Functional Role)	**AIDataModelerRole**

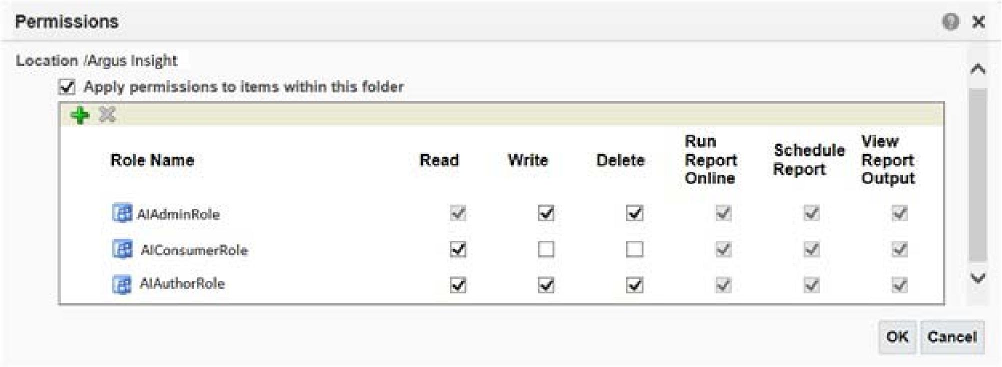
Table 6–2 (Cont.) Configuring BIP Roles

Role	Users/Roles to be added
BIReportWriter (create this role using the steps given in section 8.4.3 and create an Application Policy for this role using the steps given in section 8.4.4)	**AIRole**

6.4.2 Folder Level Permissions

Viewing folder level permissions for BI Publisher Standalone Installation:

You cannot see the permissions of shared folder for BIP Stand-Alone installation. Besides, the Argus Insight folder permissions appears as below:



Permissions

Location /Argus Insight

☑ Apply permissions to items within this folder

Role Name	Read	Write	Delete	Run Report Online	Schedule Report	View Report Output
AIAdminRole	☑	☑	☑	☑	☑	☑
AIConsumerRole	☑	☐	☐	☑	☑	☑
AIAuthorRole	☑	☑	☑	☑	☑	☑

To assign folder level permissions for BIP Integrated Installation (OBIEE+BIP):

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

   The Permissions dialog box appears.

2. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
AI Admin Role	Open (Read, and Traverse)
AI Author Role	Open (Read, and Traverse)
AI Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

3. Go to Shared Folders > Argus Insight > Permissions.

   The Permissions dialog box appears.

4. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control

Accounts	Permissions
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

7 Configuring the BusinessObjects XI Environment

This chapter describes how to configure the BusinessObjects XI (BOXI) environment. You must configure the BusinessObjects XI environment in the order specified in this guide.

This chapter includes the following topics:

- Checking Requirements
- Configuring the BusinessObjects Server
- Configuring the Argus Insight Web Server

If you are using Cognos 10 instead of BusinessObjects XI, see Chapter 8 for information about configuring the Cognos 10 environment for Argus Insight.

7.1 Checking Requirements

Before configuring the BusinessObjects environment, verify that you have installed all required hardware and software. For more information, see Section 1.2, "Software and Hardware Requirements."

In addition, if you are using the 64-bit version of Internet Information Services 7 (IIS 7), you must ensure that:

- ASP.NET is enabled.
- The IIS advanced setting **Enable 32-bit Applications** is set to **True.**
- The IIS advanced setting **.NET Application Pool** is set to **Classic** mode.

> **Note:** Argus Insight 8.1 does not support multi-tenancy with its reporting framework for BusinessObjects. There are no restrictions in the multi-tenant Argus Insight database for the functioning of BusinessObjects. The users can enhance the Argus Insight Reporting framework or tweak BusinessObjects to support multi-tenancy in BO reports.

7.2 Configuring the BusinessObjects Server

If the BusinessObjects application uses a different server from the Argus Insight application, you must update the TNSNAMES.ora file as follows:

1. Copy the PRMART TNS entry from the Argus Insight Web Server.

2. Paste the entry into the TNSNAMES.ora file on the BusinessObjects Server.

> **Note:** PRMART TNS entry must be mentioned in the TNSNAMES.ora file for both 32-bit and 64-bit Oracle Client.

If both applications use the same server and Oracle client, no modifications to the TNSNAMES.ora file are required.

7.3 Configuring the Argus Insight Web Server

The following profile switches are available only when the BO WEB URL profile switch is configured and Legacy Report profile switch is set to 1:

- Holiday Schedule Management
- Product Designated Medical Event Configuration
- Measurable Suppliers
- Site Configuration
- Acceptable Delay Justification Configuration

To configure these profile switches, refer to Argus Insight 7.0.2 Installation Guide.

8

Configuring the Cognos 10 Environment

This chapter describes how to configure the Cognos 10 environment. You must configure the Cognos 10 environment in the order specified in this guide.

This chapter includes the following topic:

- Setting Up Cognos Server and Configuration for New Installation

Before configuring the environment, verify that you have installed all required hardware and software. For more information, see Section 1.2, "Software and Hardware Requirements."

8.1 Setting Up Cognos Server and Configuration for New Installation

This section describes how to set up Cognos Server and configure your environment for a new installation of Argus Insight.

This section comprises the following sub-section:

- Configuring IIS 7.0 on the Cognos 10 Server
- Configuring the Java Database Components
- Configuring Custom Java Authentication
- Configuring the Cognos 10 Environment
- Creating Cognos Data Source (PRMART)
- Configuring Cognos Security
- Configuring Roles and Permissions

8.1.1 Configuring IIS 7.0 on the Cognos 10 Server

This section describes the following tasks that you must complete to configure Internet Information Services 7.0 (IIS 7.0) on the Cognos 10 Server:

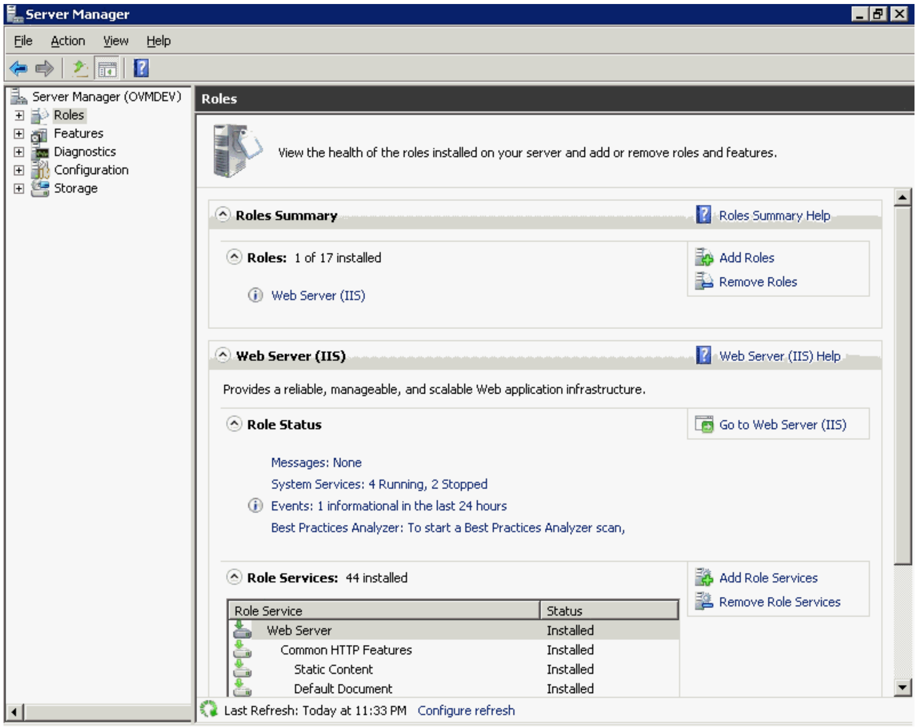
- Checking that CGI or ISAPI Is Enabled in IIS
- Creating the Cognos 10 Virtual Directories
- Editing ISAPI or CGI Extensions
- Adding the Module Mapping
- Editing the Module Mapping
- Allowing CGI Application to Use Execute

8.1.1.1 Checking that CGI or ISAPI Is Enabled in IIS

To check that CGI or ISAPI is enabled in IIS:

1. Click **Start.**
2. Navigate to **Administrative Tools**, and select **Server Manager.**

   The Server Manager screen appears.



View the health of the roles installed on your server and add or remove roles and features.

Roles: 1 of 17 installed

Web Server (IIS)

Provides a reliable, manageable, and scalable Web application infrastructure.

Messages: None

System Services: 4 Running, 2 Stopped

Events: 1 informational in the last 24 hours

Best Practices Analyzer: To start a Best Practices Analyzer scan,

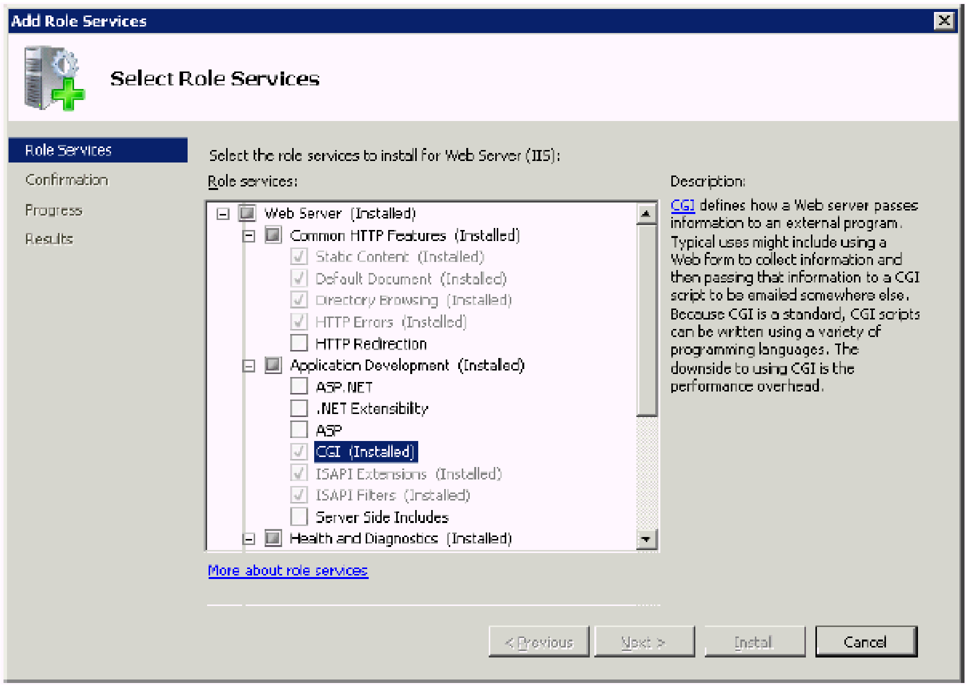
Role Services: 44 installed

Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed

Last Refresh: Today at 11:33 PM

3. In the Role Services section, click the **Add Role Services** link.

   The Add Role Services dialog box appears.



Add Role Services

Select Role Services

Select the role services to install for Web Server (IIS):

Role services:

- Web Server (Installed)
  - Common HTTP Features (Installed)
    - ☑ Static Content (Installed)
    - ☑ Default Document (Installed)
    - ☑ Directory Browsing (Installed)
    - ☑ HTTP Errors (Installed)
    - □ HTTP Redirection
  - Application Development (Installed)
    - □ ASP.NET
    - □ .NET Extensibility
    - □ ASP
    - ☑ CGI (Installed)
    - ☑ ISAPI Extensions (Installed)
    - ☑ ISAPI Filters (Installed)
    - □ Server Side Includes
  - Health and Diagnostics (Installed)

Description:

CGI defines how a Web server passes information to an external program. Typical uses might include using a Web form to collect information and then passing that information to a CGI script to be emailed somewhere else. Because CGI is a standard, CGI scripts can be written using a variety of programming languages. The downside to using CGI is the performance overhead.

4. Expand **Application Development (Installed).**

5. Verify that the CGI and ISAPI Extensions are listed as **(Installed).**

   - If these role services are not installed, select the appropriate check box, and then click **Install.** Follow the instructions on the screen to complete the installation.

   - If these role services are already installed, click **Cancel.** The system returns to the Server Manager screen.

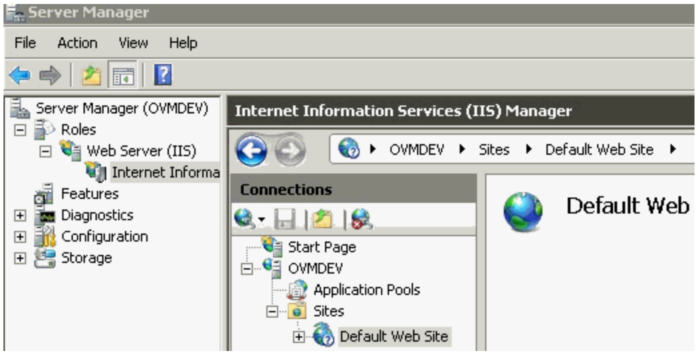
8.1.1.2 Creating the Cognos 10 Virtual Directories

To create the Cognos 10 virtual directories:

1. Navigate to **Roles > Web Server (IIS),** and select **Internet Information Services (IIS) Manager.**

2. In Connections pane, expand the server node.

3. Expand **Sites.**



4. Right-click **Default Web Site,** and select **Add Virtual Directory.**

   The Add Virtual Directory dialog box appears.

a. In the **Alias** field, enter **Cognos 10.**

b. In the **Physical path** field, enter the complete path to the Cognos 10 Web content directory. The default path is:

   drive:\Program Files\ibm\cognos\c10\webcontent

c. Click **OK.**

5. Right-click your newly-created Cognos 10 virtual directory, and select **Add Virtual Directory.**

   The Add Virtual Directory dialog box appears.

   a. In the **Alias** field, enter **cgi-bin.**

   b. In the **Physical path** field, enter the complete path to the Cognos 10 cgi-bin directory. The default path is:

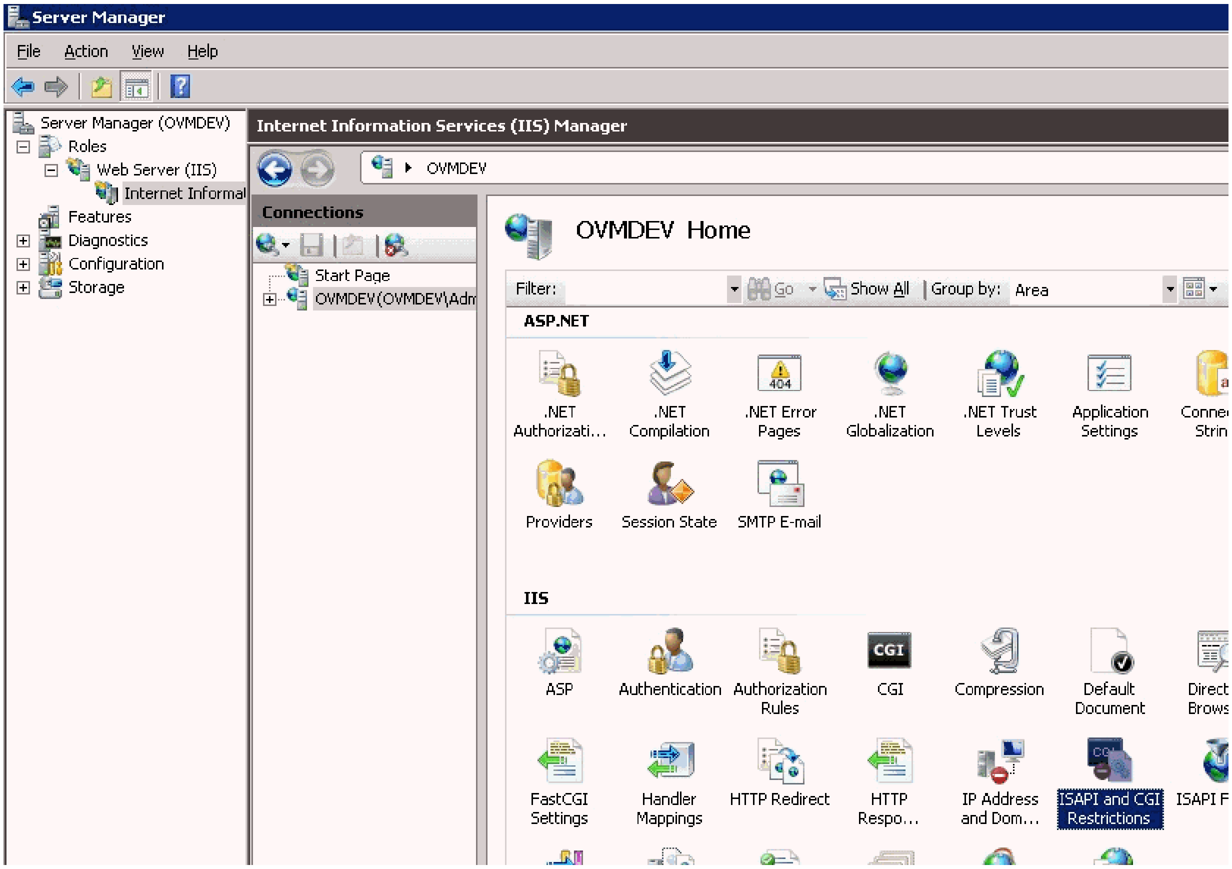
      drive:\Program Files\ibm\cognos\c10\cgi-bin

   c. Click **OK.**

8.1.1.3 Editing ISAPI or CGI Extensions

To edit the ISAPI or CGI extensions:

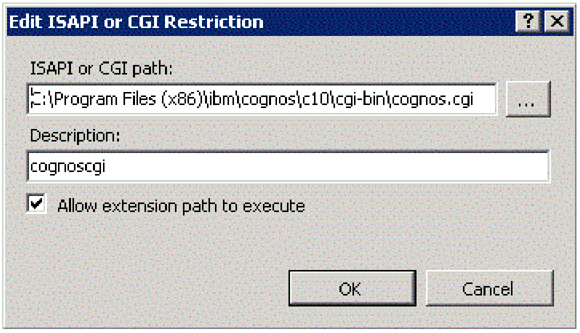
1. On Server Manager screen, in the Connections pane, select the server node.



2. Double-click the **ISAPI and CGI Restrictions** icon.

3. In the Actions pane, click the **Add**.

   The Edit ISAPI or CGI Restriction dialog box appears.



ISAPI or CGI path: C:\Program Files (x86)\ibm\cognos\c10\cgi-bin\cognos.cgi

Description: cognoscgi

☑ Allow extension path to execute

a. In the **ISAPI or CGI path** field, enter the path to either the cognos.cgi file or the cognosisapi.dll file depending on which one you will use.

> **Note:** For Argus Insight, Oracle recommends that you use cognos.cgi. In addition, you may need to surround the path in double quotes if it contains any spaces.

The default path for each file is as follows:

drive:\Program Files\ibm\cognos\c10\cgi-bin\cognosisapi.dll

drive:\Program Files\ibm\cognos\c10\cgi-bin\cognos.cgi

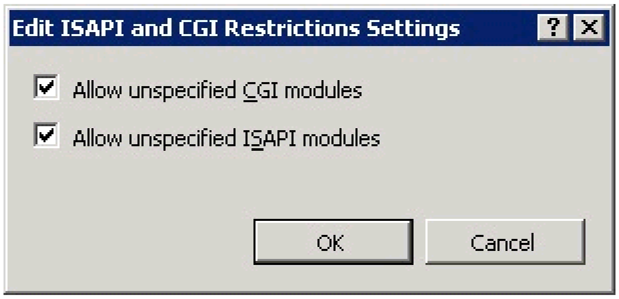
b. Select **Allow extension path to execute** check box.

c. Click **OK.**

Alternative Method

1. In Connections pane, select the server node.
2. Double-click the **ISAPI and CGI Restrictions** icon.
3. In Actions pane, click the **Edit Feature Settings**.

   The Edit ISAPI and CGI Restriction Settings dialog box appears.



☑ Allow unspecified CGI modules

☑ Allow unspecified ISAPI modules

4. Select the **Allow unspecified CGI Modules** check box.
5. Click **OK.**

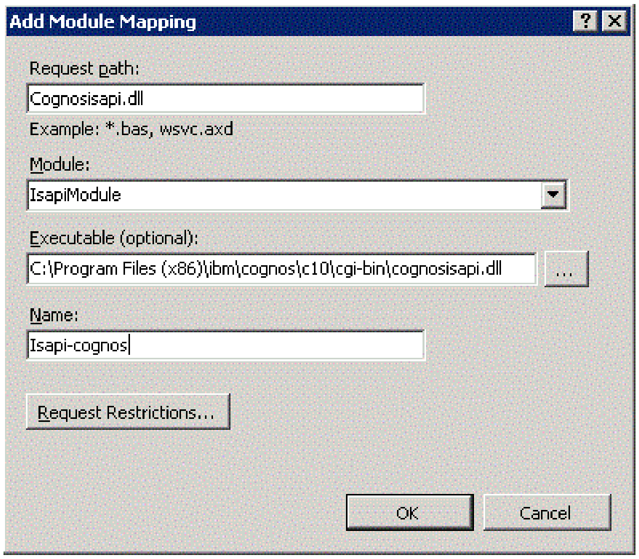
8.1.1.4 Adding the Module Mapping

To add the module mapping:

1. Open the Internet Information Services (IIS) Manager.
2. Expand the virtual directory folder, and click **cgi-bin**.

3. Double-click the **Handler Mappings** icon.
4. In the Actions pane, click the **Add Module Mapping**.

   The Add Module Mapping dialog box appears.



Add Module Mapping

Request path: Cognosisapi.dll

Example: *.bas, wsvc.axd

Module: IsapiModule

Executable (optional): C:\Program Files (x86)\ibm\cognos\c10\cgi-bin\cognosisapi.dll

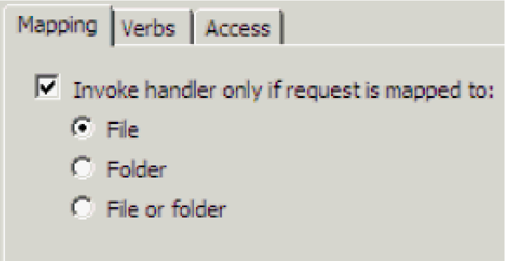
Name: Isapi-cognos

   a. In the **Request path** field, enter either *.cgi or *.dll as you need.
   b. In the **Module** field, select either **CGIModule** or **IsapiModule** from the list.
   c. In the **Executable** field, enter a value depending on the module you are using.

      If you are using an ISAPI Module, you must enter the complete path to the cognosisapi.dll. You can click the ellipsis icon to browse to the file location.

      If you are using a CGI Module, you do not need to enter a value in the Executable field.
   d. In the **Name** field, enter a realistic name for this mapping. For example, ISAPI-Cognos.

5. Click **Request Restrictions.**
   a. Click the **Mapping** tab, and select **Invoke handler only if request is mapped to: File.**



☑ Invoke handler only if request is mapped to:

● File

○ Folder

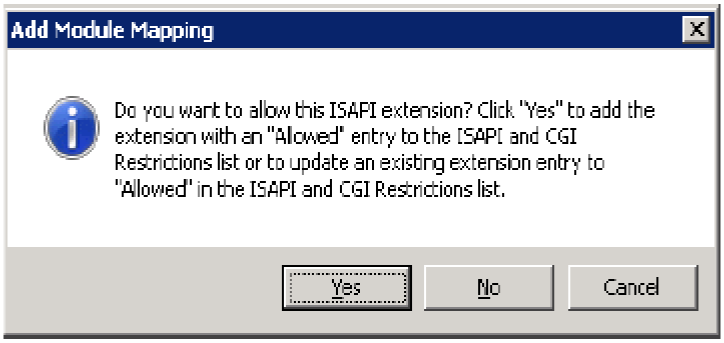
○ File or folder

   b. Click the **Verbs** tab, and select **All verbs.**
   c. Click the **Access** tab, select **Execute**.
   d. Click **OK** to save changes.

      You return to the Add Module Mapping dialog box.

6. Click **OK.**

A message appears depending on the method used in Section 8.1.1.3, "Editing ISAPI or CGI Extensions,".



Do you want to allow this ISAPI extension? Click "Yes" to add the extension with an "Allowed" entry to the ISAPI and CGI Restrictions list or to update an existing extension entry to "Allowed" in the ISAPI and CGI Restrictions list.

7. Click **Yes.**

   The new module mapping is added to the Module Mapping list.

8.1.1.5 Editing the Module Mapping

For Cognos Administration to function properly, you must manually edit the directive that you added to the IIS configuration file in the previous step (see Section 8.1.1.4, "Adding the Module Mapping").

To edit the module mapping:

1. Navigate to the following folder:

   COGNOS_HOME/c10/cgi-bin

   > **Note:** Ensure that you have access permissions on the cgi-bin folder so you can save the changes you make to the web.config file.

2. Open the **web.config** file for editing.
3. Locate the appropriate **add name** statement in the web.config file.

   For CGI, locate this statement:

```
<add name="CGI-cognos" path="*.cgi" verb="*" modules="CgiModule"
resourceType="Unspecified" />
```

   For ISAPI, locate this statement:

```
<add name="ISAPI-Cognos" path="cognosisapi.dll" verb="*"
modules="IsapiModule" scriptProcessor="E:\Program Files\ibm\Cognos\C10\
cgi-bin\cognosisapi.dll" resourceType="Unspecified"
requireAccess="Execute" preCondition="bitness32" />
```

4. Add **allowPathInfo="true"** to the end of the statement.

   For CGI:

```
<add name="CGI-cognos" path="*.cgi" verb="*" modules="CgiModule"
resourceType="Unspecified" allowPathInfo="true" />
```

   For ISAPI:

```
<add name="ISAPI-Cognos" path="cognosisapi.dll" verb="*"
modules="IsapiModule" scriptProcessor="E:\Program Files\ibm\Cognos\C10\
cgi-bin\cognosisapi.dll" resourceType="Unspecified"
requireAccess="Execute" preCondition="bitness32" allowPathInfo="true"/>
```

5. Save changes and close the web.config file.

8.1.1.6 Allowing CGI Application to Use Execute

To allow the CGI application to use execute:

1. Open the Internet Information Services (IIS) Manager.
2. Expand the virtual directory folder, and click the **cgi-bin**.
3. Double-click the **Handler Mappings** icon.
4. In the Actions pane, click the **Edit Feature Permissions**.

   The Edit Features Permissions dialog box appears.
5. Select the **Execute** check box.
6. Click **OK.**

8.1.2 Configuring the Java Database Components

To configure the Java Database Components (JDBC) in the Cognos 10 environment:

1. Navigate to the following Oracle installation path:

   Oracle_Installation_Path\product*Oracle_Version*\client_1\sqldeveloper\jdbc\lib
2. For Oracle 11g client, copy the **ojdbc5.jar** file, and for Oracle 12c client, copy **ojdbc6.jar** to the following location on the Cognos 10 environment:

   Cognos_Installation_Path\c10\webapps\p2pd\web-inf\lib

8.1.3 Configuring Custom Java Authentication

This section comprises the following sub-sections:

- Configuring Custom Java Authentication for Windows
- Configuring Custom Java Authentication for Linux

8.1.3.1 Configuring Custom Java Authentication for Windows

To configure custom Java authentication for Windows:

1. Go to IBM Cognos Administration and stop the Cognos services.
2. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Authentication\JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\webapps\p2pd\WEB-INF\lib
3. Copy the **JDBC_Config_PowerReports.properties** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\Configuration

4. Define the configuration parameters:

   a. Navigate to the following folder:

      \\Cognos_10_Install_Path\ c10\Configuration

   b. Open the **JDBC_Config_PowerReports.properties** file for editing.

   c. Modify the existing values of the following parameters only if the database changed from the 7.0 database:

Parameter	Value to Enter
Server	Enter the IP address or the name of the Database Server.
SID	Enter the instance/service name of the Argus Insight data mart.
Port	Enter the database port number.
COGNOS_ SINGLE_SIGN_ ON_HEADER	Enter the header name in which Single Sign On user name will be populated by SSO solution, that is, HEADER_OAM_ REMOTE_USER.

   d. Save and close the file.

5. Copy **AI.ini** and **ArgusSecureKey.ini** from the following location:

   \\<Argus_Insight_Server>\Windows

   To the following location:

   \\Cognos_10_Install_Path\C10\configuration

6. Navigate to the following folder:

   Program Files\ibm\cognos\c10\bin\jre\6.0\lib\security

7. Backup **local_policy.jar** and **US_export_policy.jar** files.

8. Download the policy files corresponding to the version of installed JRE.

   Note: To find the version of installed JRE:

   - For Cognos 32 bit, go to bin/jre/version
   - For Cognos 64 bit, go to bin64/jre/version

   For example, to install policy files of JRE version 6, execute the following steps:

   a. Go to the following URL:

      https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   b. Log in to the IBM site.

   c. Select the files for *Java 5.0 SR16, Java 6 SR13, Java 6 SR5 (J9 VM2.6), Java 7 SR4*, and all later releases option, and click **Continue**.

   d. Click **I agree**, to agree to the license terms, and then select **I confirm**.

   e. Click **Download Now**.

   f. Download the files and extract into a folder.

   g. Locate **local_policy.jar** and **US_export_policy.jar** files in the extracted folder.

   h. Copy these jar files into the following folder:

      drive:\Program Files\ibm\cognos\c10\bin(bin64 in case Cognos is 64 bit)\jre\6.0\lib\security

9. Go to IBM Cognos Administration, and restart the Cognos services.

8.1.3.2 Configuring Custom Java Authentication for Linux

To configure custom Java authentication for Linux:

1. Go to IBM Cognos Administration and stop the Cognos services.
2. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\webapps\p2pd\WEB-INF\lib
3. Copy the **JDBC_Config_PowerReports.properties** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\Configuration
4. Define the configuration parameters:

   a. Navigate to the following folder:

      \\Cognos_10_Install_Path\ c10\Configuration

   b. Open the **JDBC_Config_PowerReports.properties** file for editing.

   c. Modify the existing values of the following parameters only if the database changed from the 7.0 database:

Parameter	Value to Enter
Server	Enter the IP address or the name of the Database Server.
SID	Enter the instance/service name of the Argus Insight data mart.
Port	Enter the database port number.
COGNOS_SINGLE_SIGN_ON_HEADER	Enter the header name in which Single Sign On user name will be populated by SSO solution, that is, HEADER_OAM_REMOTE_USER.

   d. Save and close the file.

5. Copy **AI.ini** and **ArgusSecureKey.ini** from the following location:

   \\<Argus_Insight_Server>\Windows

   To the following location:

   \\Cognos_10_Install_Path\C10\configuration
6. Navigate to the following folder:

   JAVA_HOME\jre\6.0\lib\security

7. Backup **local_policy.jar** and **US_export_policy.jar** files.

8. Download the policy files corresponding to the version of installed JRE.

   > **Note:** To find the version of installed JRE, go to the JAVA_HOME and check the folder name under the JRE folder.

   For example, to install policy files of JRE version 6, execute the following steps:

   a. Go to the following URL:

      http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

   b. Download **local_policy.jar** and **US_export_policy.jar** files in the extracted folder.

   c. Copy these jar files into the following folder:

      JAVA_HOME\jre\6.0\lib\security

   d. If the Replace Files dialog box appears, click **Yes**.

9. Go to IBM Cognos Administration, and restart the Cognos services.

8.1.4 Configuring the Cognos 10 Environment

This section describes the following tasks that you must complete to configure the Cognos 10 environment:

- Opening the IBM Cognos 10 Configuration Window
- Setting the Security Properties for Cognos 10
- Setting the Data Access Properties for Cognos 10
- Creating the Namespace for Argus Insight Authentication
- Saving the Configuration and Starting the Cognos 10 Service

8.1.4.1 Opening the IBM Cognos 10 Configuration Window

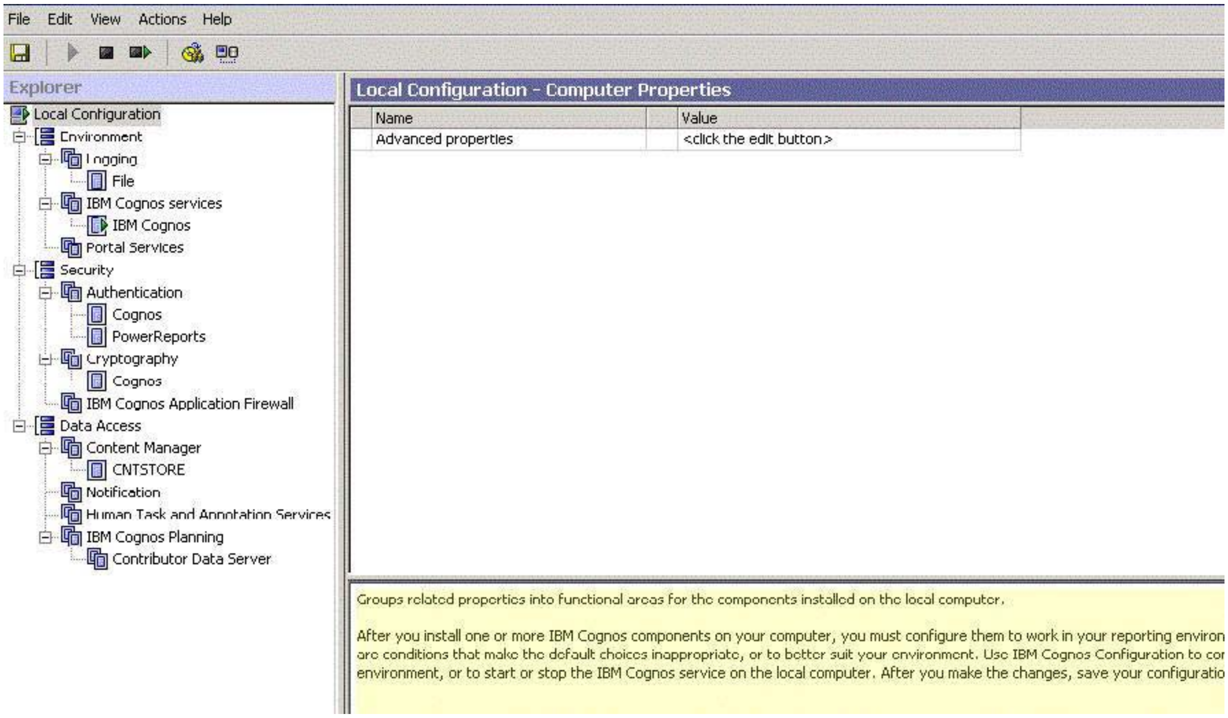
You use the options in the IBM Cognos 10 Configuration screen to define environment group and logging properties, security properties, and data access properties.

To open the IBM Cognos 10 Configuration screen:

1. Click **Start.**

2. Navigate to **All Programs > IBM Cognos 10,** and then select **IBM Cognos Configuration.**

   The IBM Cognos Configuration screen appears.



Local Configuration - Computer Properties

Name	Value
Advanced properties	<click the edit button>

Groups related properties into functional areas for the components installed on the local computer.

After you install one or more IBM Cognos components on your computer, you must configure them to work in your reporting environ
are conditions that make the default choices inappropriate, or to better suit your environment. Use IBM Cognos Configuration to cor
environment, or to start or stop the IBM Cognos service on the local computer. After you make the changes, save your configuratio

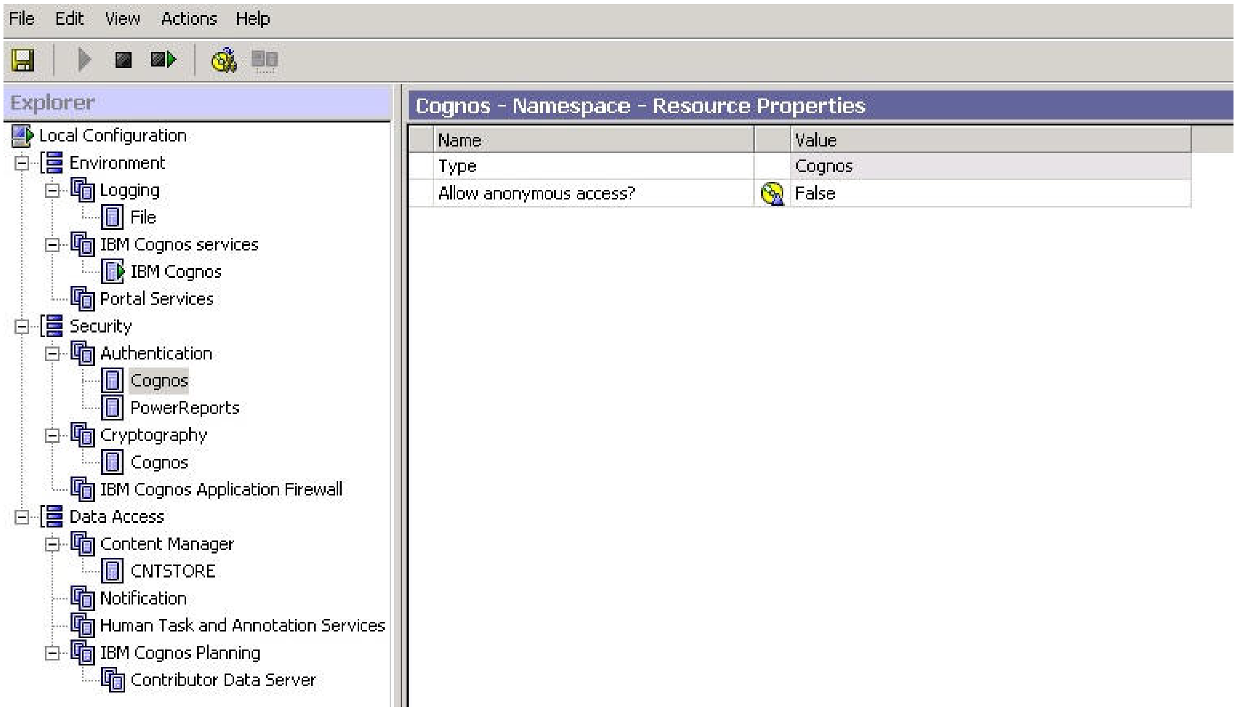
---

Note: The screens displayed during the Cognos 10 configuration are labeled either IBM Cognos 10 or Cognos 10. Both labels refer to the same Cognos configuration.

8.1.4.2 Setting the Security Properties for Cognos 10

To define the security properties:

1. Open the IBM Cognos 10 Configuration screen.
2. Navigate to **Security > Authentication,** and select **Cognos.**

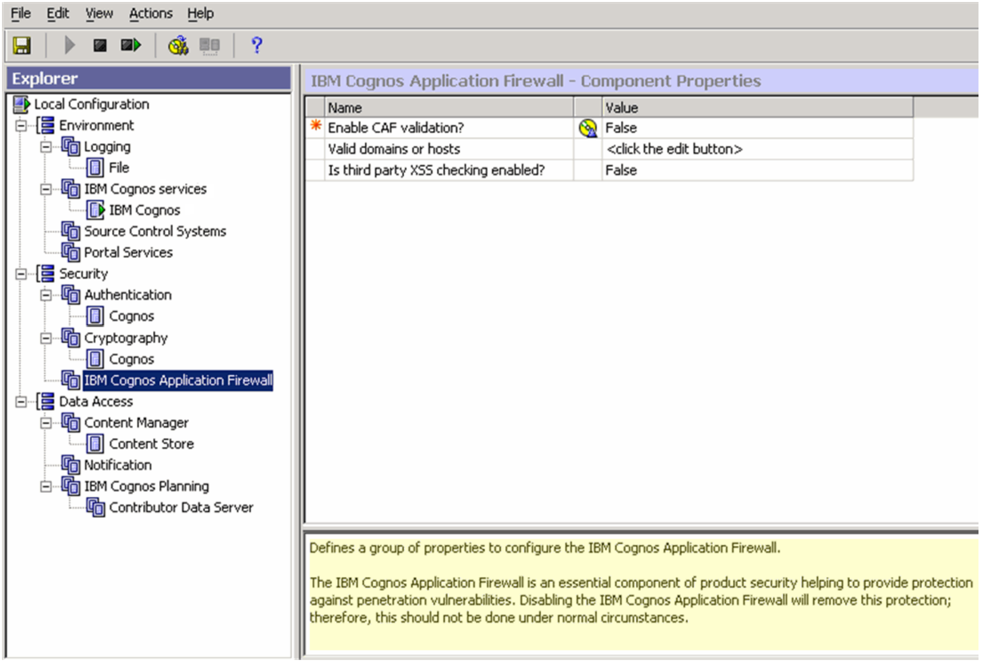


Cognos - Namespace - Resource Properties

Name	Value
Type	Cognos
Allow anonymous access?	False

3. Set the **Allow anonymous access?** property to **True.**

4. Navigate to **Security**, and select **IBM Cognos Application Firewall.**



IBM Cognos Application Firewall - Component Properties

Name	Value
* Enable CAF validation?	False
Valid domains or hosts	<click the edit button>
Is third party XSS checking enabled?	False

Defines a group of properties to configure the IBM Cognos Application Firewall.

The IBM Cognos Application Firewall is an essential component of product security helping to provide protection against penetration vulnerabilities. Disabling the IBM Cognos Application Firewall will remove this protection; therefore, this should not be done under normal circumstances.

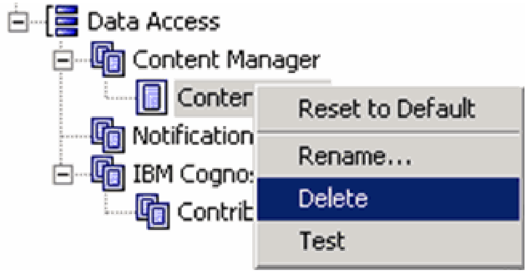
5. Set the **Enable CAF validation?** property to **False.**

8.1.4.3 Setting the Data Access Properties for Cognos 10

To define the data access properties:

1. Open the IBM Cognos 10 Configuration screen.

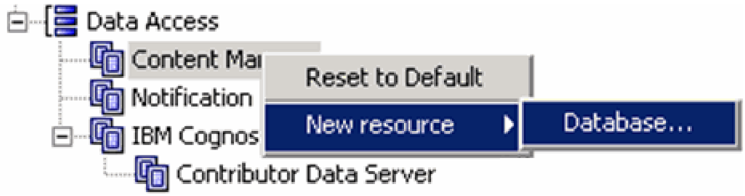
2. Navigate to **Data Access > Content Manager,** right-click **Content Store,** and then select **Delete** from the menu.



A confirmation messages appears.

3. Click **Yes.**

4. Navigate to **Data Access,** right-click **Content Manager,** select **New resource,** and then select **Database.**



5. Complete the New Resource - Database dialog box as follows:

   - In the **Name** field, enter **CNTSTORE.**

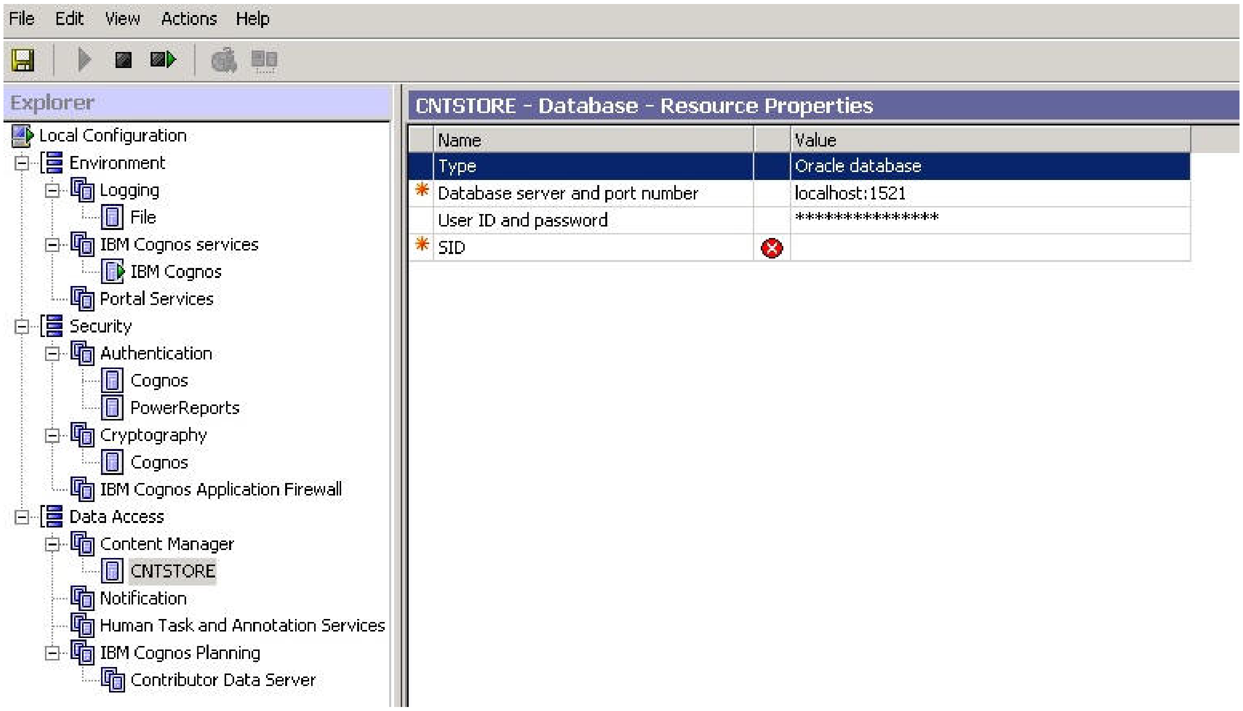
     This is the name of the database resource.

   - In the **Type** field, select **Oracle database.**

   - Click **OK.**

   You return to the IBM Cognos Configuration screen.

   The resource property for the database of the newly-created CNTSTORE resource database appears.



CNTSTORE - Database - Resource Properties

	Name		Value
	Type		Oracle database
*	Database server and port number		localhost:1521
	User ID and password		***************
*	SID	⊗	

6. Enter the value for the **Database server and port number** as:

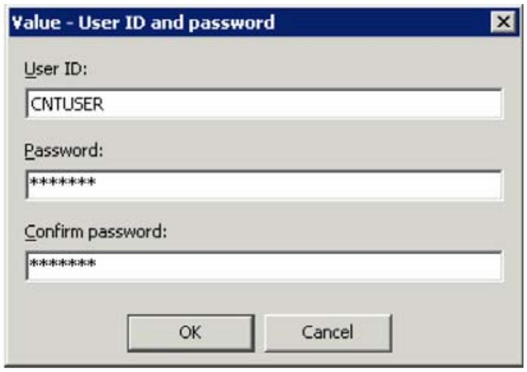
   Database_Server_Name:1521

   where:

   Database_Server_Name is the name of the server where your content store database is stored.

7. Select **User ID and password,** and click the icon next to it.

   The Value - User ID and password dialog box appears.



Value - User ID and password

User ID: CNTUSER

Password: *******

Confirm password: *******

   a. In the **User ID** field, enter the ID for the content store database user.

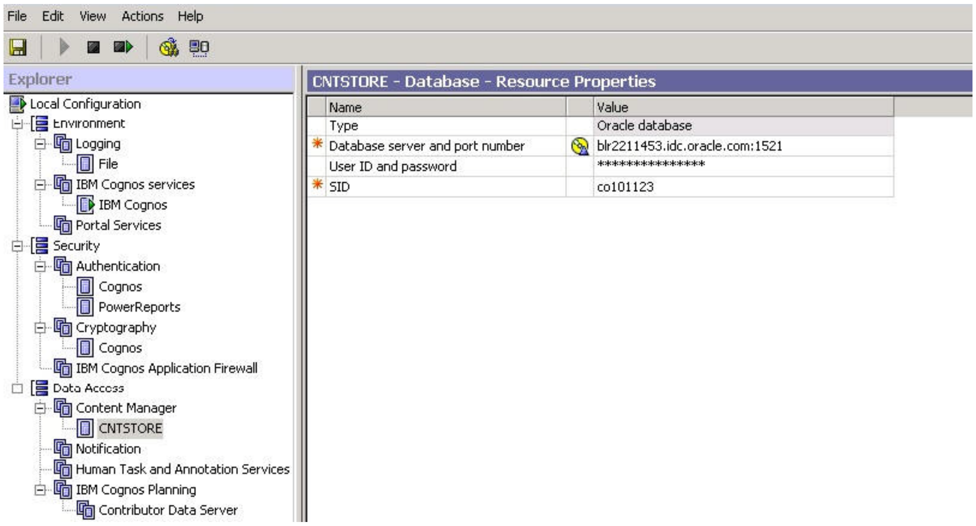
   b. In the **Password** field, enter the password for the content store database user.

   c. In the **Confirm password** field, re-enter the password for verification.

   d. Click **OK.**

> **Note:** The contents store database user is created in the Cognos content store database. This user is given grants of Connect, Resource, and Create View, along with Unlimited Tablespace Grant.
>
> The character set of the Cognos content store database should only be UTF.
>
> Make sure that the content store database entry is added in the TNSNames.ora file on the Cognos 10 server.

8. In the **Service name** field, enter the database instance name for the Cognos 10 repository.



CNTSTORE - Database - Resource Properties

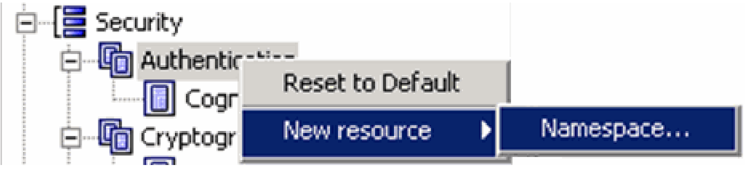
	Name		Value
	Type		Oracle database
*	Database server and port number		blr2211453.idc.oracle.com:1521
	User ID and password		****************
*	SID		co101123

8.1.4.4 Creating the Namespace for Argus Insight Authentication

To create the namespace for Argus Insight authentication:

1. Open the IBM Cognos 10 Configuration screen.

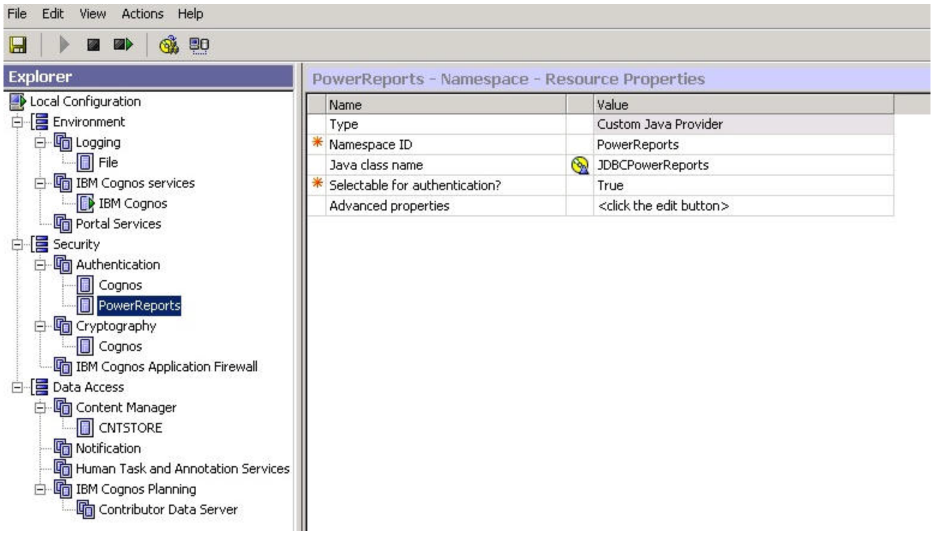
2. Navigate to **Security,** right-click **Authentication,** click **New resource,** and then select **Namespace.**



3. Complete the New Resource – Namespace dialog box as follows:

   - In the **Name** field, enter **PowerReports.**
   - In the **Type** field, enter **Custom Java Provider.**
   - Click **OK.**

   The PowerReports - Namespace - Resource Properties screen appears.



PowerReports - Namespace - Resource Properties

Name	Value
Type	Custom Java Provider
* Namespace ID	PowerReports
Java class name	JDBCPowerReports
* Selectable for authentication?	True
Advanced properties	<click the edit button>

4. Set the **Namespace ID** property to **PowerReports.**

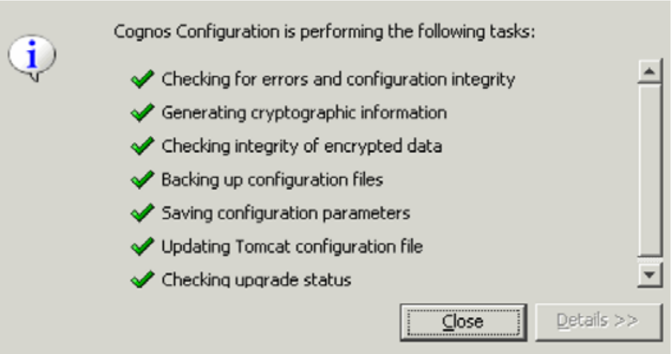
5. Set the **Java class name** property to **JDBCPowerReports.**

8.1.4.5 Saving the Configuration and Starting the Cognos 10 Service

To save the configuration and start the Cognos 10 service:

1. Open the File menu, and select **Save** to save changes to the configuration settings.

   An information dialog box appears and lists each task as it is performed.

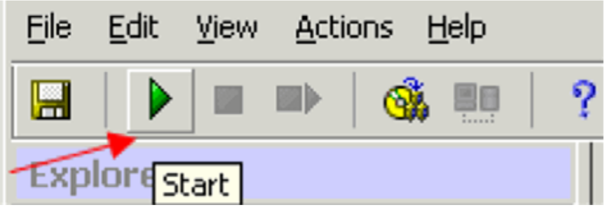


Cognos Configuration is performing the following tasks:

✓ Checking for errors and configuration integrity
✓ Generating cryptographic information
✓ Checking integrity of encrypted data
✓ Backing up configuration files
✓ Saving configuration parameters
✓ Updating Tomcat configuration file
✓ Checking upgrade status

2. Click **Close** when the system completes all the configuration tasks.

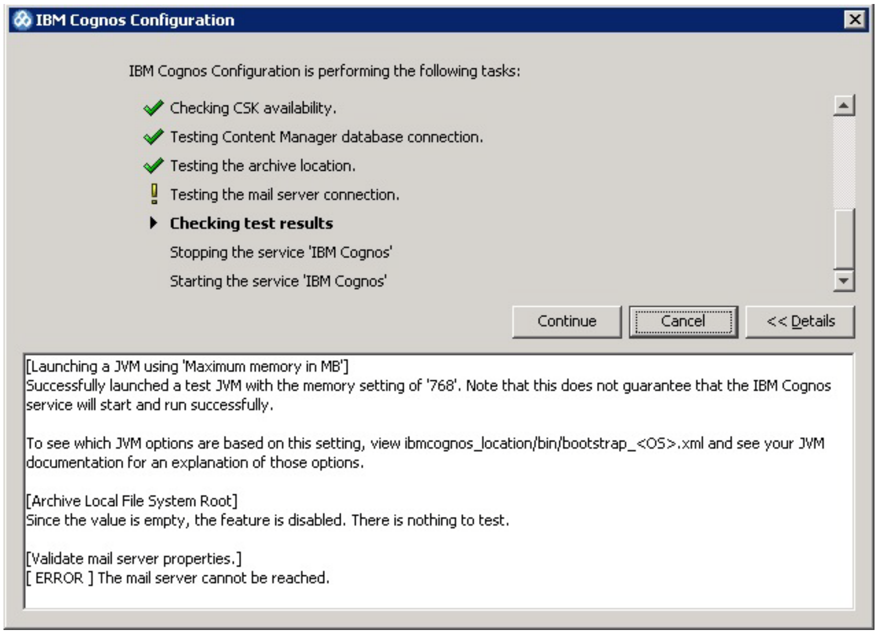
3. In the IBM Cognos Configuration screen, click the **Start** icon to run the Cognos 10 service.



The system begins to run the IBM Cognos 10 service.

- If there are no problems with the configuration, the system completes the test phase and starts the IBM Cognos 10 service successfully.

- If there are possible problems with the configuration, the system stops running the service and displays a warning message. When you click **OK** to acknowledge the warning message, the system opens another dialog box with more information. For example:



IBM Cognos Configuration is performing the following tasks:

✓ Checking CSK availability.
✓ Testing Content Manager database connection.
✓ Testing the archive location.
! Testing the mail server connection.
▶ **Checking test results**
Stopping the service 'IBM Cognos'
Starting the service 'IBM Cognos'

```
[Launching a JVM using 'Maximum memory in MB']
Successfully launched a test JVM with the memory setting of '768'. Note that this does not guarantee that the IBM Cognos
service will start and run successfully.

To see which JVM options are based on this setting, view ibmcognos_location/bin/bootstrap_<OS>.xml and see your JVM
documentation for an explanation of those options.

[Archive Local File System Root]
Since the value is empty, the feature is disabled. There is nothing to test.

[Validate mail server properties.]
[ ERROR ] The mail server cannot be reached.
```

At this point:

- For more information about the warnings and errors, click **Details**.
- To stop the process, click **Cancel**.

  If the warnings or errors are due to reasons other than mail server connection failure, cancel the process and check your configuration again.
- To ignore the warnings and errors, and complete the process of starting the IBM Cognos 10 service, click **Continue**.

  For example, you may ignore warnings that the mail server cannot be reached (see the previous illustration).

4. Click **Close** to exit.
5. Open the **File** menu, and select **Exit** to exit from the IBM Cognos 10 configuration.

8.1.5 Creating Cognos Data Source (PRMART)

To create Cognos Data Source (PRMART):

1. Log in to the Cognos 10.

   The IBM Cognos 10 home page appears.

   > **Note:** If your security settings on the server do not permit you to view the Cognos connection, add the site URL (http://*Cognos_10_Server*/cognos10) to the list of local intranet sites.

2. Under Administration section, click **Administer IBM Cognos content.**

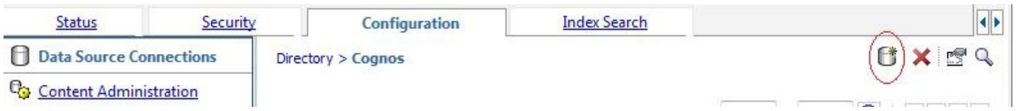
   The IBM Cognos Administration screen appears.

3. Click the **Configuration** tab.

4. Click **Data Source Connections**.

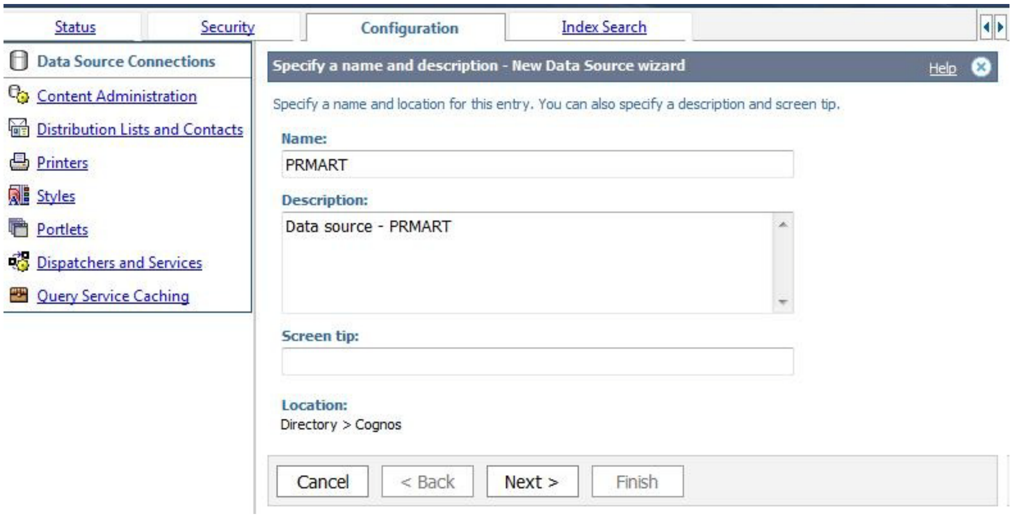
5. Click **New Data Source** icon.

   The Specify a name and description - New Data Source Wizard screen appears.



6. Enter the **Name** and **Description** of the data source, and click **Next**.

   The Specify the connection - New Data Source Wizard screen appears.



Specify a name and description - New Data Source wizard

Specify a name and location for this entry. You can also specify a description and screen tip.

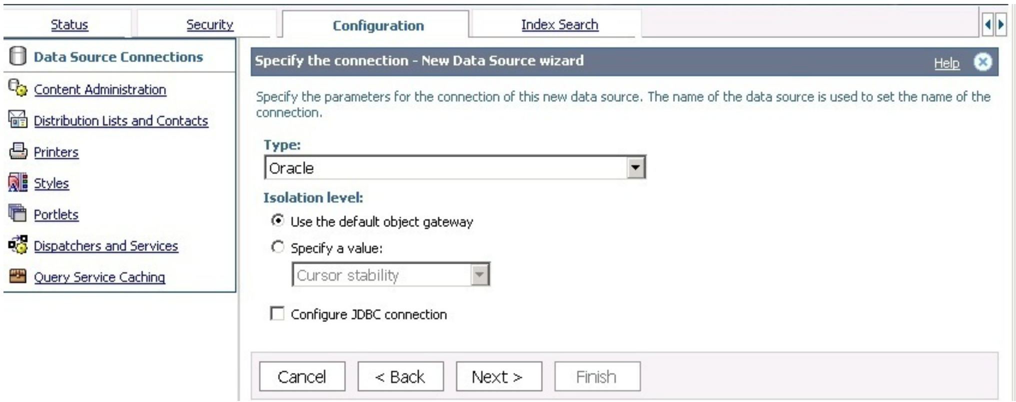
Name: PRMART

Description: Data source - PRMART

Screen tip:

Location: Directory > Cognos

7. Specify parameters for the connection, and click **Next**.



Specify the connection - New Data Source wizard

Specify the parameters for the connection of this new data source. The name of the data source is used to set the name of the connection.

Type: Oracle

Isolation level:

● Use the default object gateway

○ Specify a value: Cursor stability

□ Configure JDBC connection

8. On the Configuration tab:

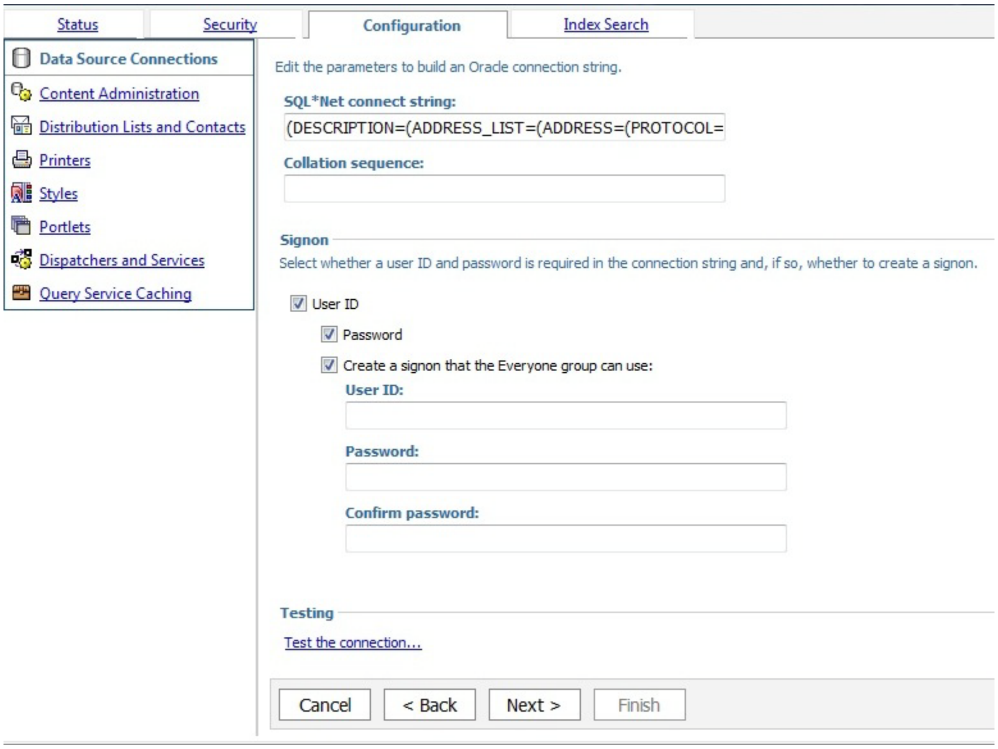
   a. In **SQL *Netconnect string:** field, enter the connection string.

      For example,

      (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<hostname>)(PORT=<Port>)))(CONNECT_DATA=(SERVICE_NAME=<Service Name>)))

b. In the **Signon** section, select **User ID** check box, and enter details in the **User ID**, **Password**, and **Confirm password** fields.

c. In the **Testing** section, click Test the connection...



Edit the parameters to build an Oracle connection string.

SQL*Net connect string: (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=

Collation sequence:

Signon

Select whether a user ID and password is required in the connection string and, if so, whether to create a signon.

☑ User ID

☑ Password

☑ Create a signon that the Everyone group can use:

User ID:

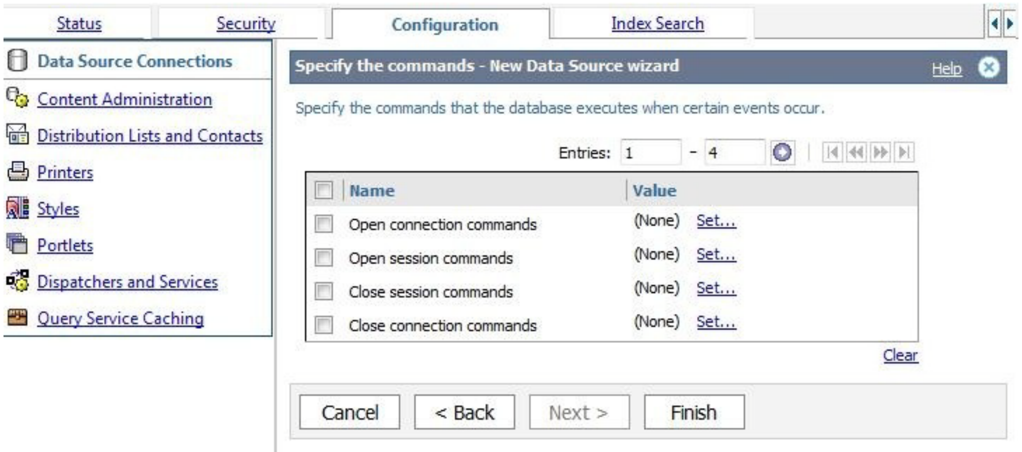
Password:

Confirm password:

Testing

Test the connection...

9. Click **Next**, and specify the commands for connection.



Specify the commands that the database executes when certain events occur.

Entries: 1 - 4

□	Name	Value
□	Open connection commands	(None) Set...
□	Open session commands	(None) Set...
□	Close session commands	(None) Set...
□	Close connection commands	(None) Set...

For more information on Cognos commands, refer to *Argus Insight Extensibility Guide > Section 5.3.2 Applying Argus Data Security* and *Section 5.3.3 Applying Enterprise Security*.

10. Click **Finish**.

The PRMART data source is created.

8.1.6 Configuring Cognos Security

This section includes the following topics:

- Activating the PowerReports Namespace

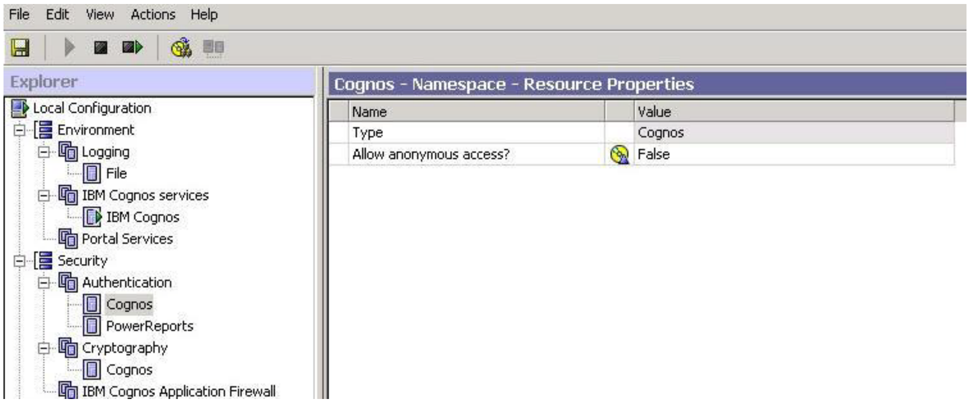
8.1.6.1 Activating the PowerReports Namespace

To activate the PowerReports namespace:

1. Open the Cognos 10 configuration.
2. Click **Start > All Programs > IBM Cognos 10,** and then select **IBM Cognos Configuration.**

   The IBM Cognos Configuration screen appears.
3. Navigate to **Security > Authentication,** and then select **Cognos.**

   The Cognos - Namespace - Resource properties screen appears.
4. Set the **Allow Anonymous access?** property to **False.**

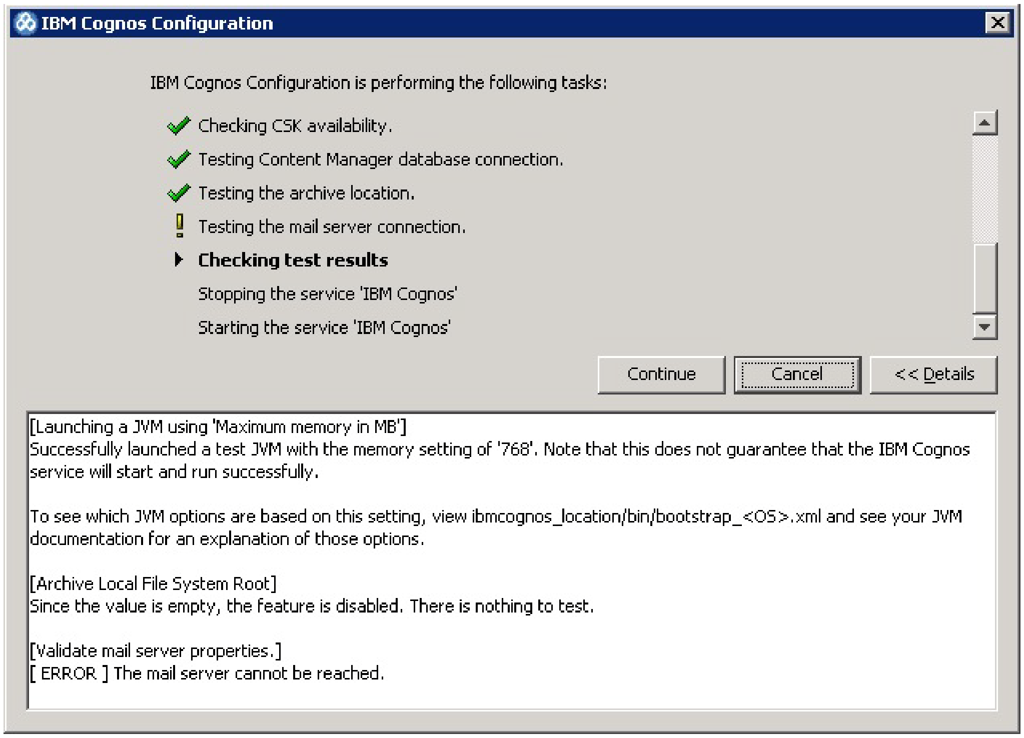


Cognos - Namespace - Resource Properties

Name	Value
Type	Cognos
Allow anonymous access?	False

5. From the File menu, select **Save.**
6. From the Actions menu, select **Restart** to restart the Cognos 10 service.

   The status information about each task being performed during the restart appears.



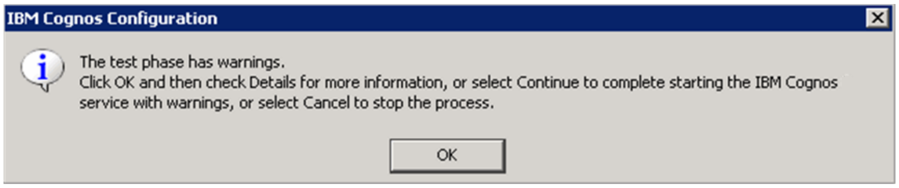
IBM Cognos Configuration

IBM Cognos Configuration is performing the following tasks:

- ✓ Checking CSK availability.
- ✓ Testing Content Manager database connection.
- ✓ Testing the archive location.
- ! Testing the mail server connection.
- **Checking test results**
- Stopping the service 'IBM Cognos'
- Starting the service 'IBM Cognos'

```
[Launching a JVM using 'Maximum memory in MB']
Successfully launched a test JVM with the memory setting of '768'. Note that this does not guarantee that the IBM Cognos
service will start and run successfully.

To see which JVM options are based on this setting, view ibmcognos_location/bin/bootstrap_<OS>.xml and see your JVM
documentation for an explanation of those options.

[Archive Local File System Root]
Since the value is empty, the feature is disabled. There is nothing to test.

[Validate mail server properties.]
[ ERROR ] The mail server cannot be reached.
```

During the Cognos service restart, a warning message may appear.



IBM Cognos Configuration

The test phase has warnings.
Click OK and then check Details for more information, or select Continue to complete starting the IBM Cognos service with warnings, or select Cancel to stop the process.

7. Process any warning message as follows:

   a. Click **OK.**

   b. To obtain more information about the warning, click **Details**.

      Depending on the type of warning:

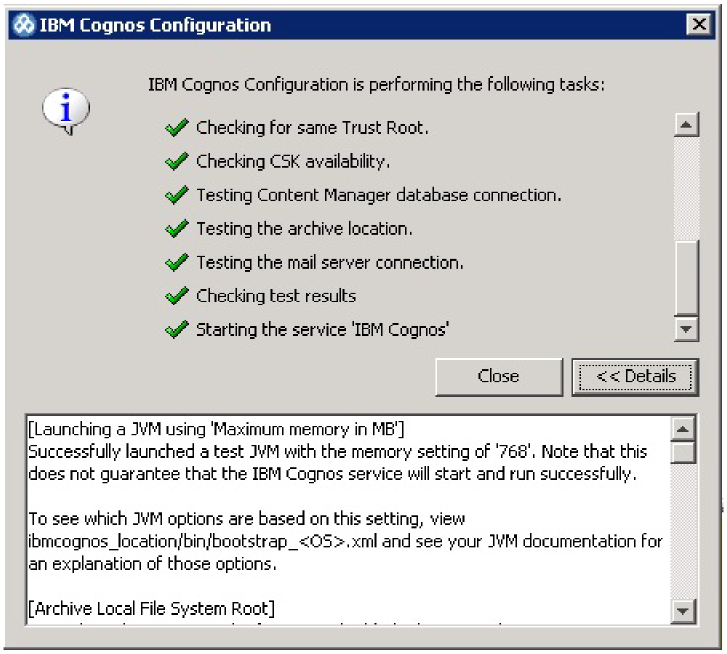
      — To ignore the warning and continue with the process of restarting the IBM Cognos 10 service, click **Continue**.

      For example, you may want to ignore a warning that the connection to the mail server failed.

      — To stop the restart process, click **Cancel**.

      If the warnings are due to reasons other than a mail server connection failure, you should stop the process, check your configuration, and then restart the IBM Cognos 10 service.

8. Wait until the all the configuration tasks are processed and the status for each task appears.



IBM Cognos Configuration

IBM Cognos Configuration is performing the following tasks:

- ✓ Checking for same Trust Root.
- ✓ Checking CSK availability.
- ✓ Testing Content Manager database connection.
- ✓ Testing the archive location.
- ✓ Testing the mail server connection.
- ✓ Checking test results
- ✓ Starting the service 'IBM Cognos'

```
[Launching a JVM using 'Maximum memory in MB']
Successfully launched a test JVM with the memory setting of '768'. Note that this
does not guarantee that the IBM Cognos service will start and run successfully.

To see which JVM options are based on this setting, view
ibmcognos_location/bin/bootstrap_<OS>.xml and see your JVM documentation for
an explanation of those options.

[Archive Local File System Root]
```

9. Click **Close** to exit the Cognos configuration.

Note: Make sure that you remove the **Everyone** user group from the **Directory Administrator** and **System Administrator** roles of Cognos. Before doing this, make sure that you have a valid user as part of the **System Administrator** role in Cognos.

If you have not added any user as part of the System Administrator role in Cognos, then you have to add Everyone user group in System Administrator roles of Cognos again.

To add the **Everyone** user group in the System Administrator role of Cognos:

1. Connect to the Content Store database as the content store user.
2. Navigate to the following folder:

   Cognos_10_Install_Path\C10\configuration\schemas\content
3. Run the **AddSysAdminMember.sql** script.
4. Commit the changes.

8.1.7 Configuring Roles and Permissions

To configure enterprise specific roles and permissions:

1. Log in to the Cognos 10 Server as an administrator user.
2. Create an Enterprise-specific role for each enterprise. For example:
   - ENT1_Role for Enterprise 1
   - ENT2_Role for Enterprise 2
3. Add all users belonging to the specific enterprises to their respective roles. For example:
   - Add ENT1_user to ENT1_Role

Note: If a user is a member of multiple enterprises, the user must be added to the roles for all the enterprises.

4. Create a folder in Public Folders for each enterprise. For example:
   - ENT1_Folder for Enterprise 1
   - ENT2_Folder for Enterprise 2
5. Select the required permissions of the Enterprise-specific role for the Enterprise-specific folder. For example,
   - Add ENT1_Role to the ENT1_Folder and provide the Read, Write, Execute, and Traverse permissions on this folder.

9 Configuring the OBIEE Environment

This chapter includes the following topics:

- Pre-installation Configuration
- Configuring the OBIEE Repository and Web Catalog using the BAR File
- Configuring OBIEE Repository and Web Catalog Manually
- Creating Users and Groups in OBIEE
- OBIEE Catalog Folder-level Permissions
- OBIEE Default Application Roles

9.1 Pre-installation Configuration

Before integrating OBIEE with Argus Insight, make sure to complete the following tasks:

1. Install JDK 1.8 on the machine where Argus Insight is installed.
2. Since the data for analysis is based on Argus Mart schema and not the Insight Mart schema, the TNS entry for the Argus Mart schema should be present in the OBIEE 12c home at the following path:

   <obiee_home>\user_projects\domains\bi\config\fmwconfig\bienv\core\

   > **Note:** In this chapter, **bi** is referred as the domain name. This domain name may differ based on your configuration.
   >
   > *<obiee_home>/user_projects/domains/bi*

3. Set up the TNS for Oracle Client Home in the PATH variable.
4. Run the Argus Mart Schema creation tool.

   When the tool is run, the new tables, indexes, packages and all the objects required for OBIEE are created in the Argus Mart schema.

   Additionally, a read only user AM_BI_USER with read-only privileges on BI Objects is created.

   For detailed information on installing and upgrading Argus Mart schema, refer to *Oracle Argus Mart Installation and Administration Guide*.

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

Oracle Business Intelligence Application Archive (BAR) file is a compressed archive file that contains a cohesive set of BI metadata artifacts (data model, content model, and authorization model). When deploying BI application from one server to another you can use these BAR files to transfer the metadata instead of transferring the RPD, Catalog, and the Security Model separately.

A BAR file contains the following BI application module artifacts:

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

This section comprises the following:

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

9.2.1 Importing the BAR file in an existing OBIEE instance

Before importing the BAR File, make sure:

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

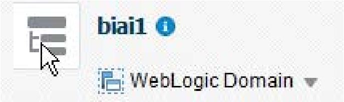
  (validate it from *http://<machinename>.<port>/console*)
- The Enterprise Manager (Fusion Middleware Control) is up and running

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

To import the BAR file:

1. Copy the BAR file from *<AI HOME>OBIEE\BAR File\ssi.bar* to a local folder on the machine where the OBIEE is installed.

   For example, copy the file at *C:\AIOBIEE\instance\import*.
2. Login to the Enterprise Manager with the WebLogic credentials.
3. Click **Target Navigation.**

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

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

   A confirmation dialog box appears.

6. Click **Yes**.

   All the running processes are stopped.

7. Go to the command prompt, and start the WebLogic Scripting Tool (using **wlst.cmd** on Windows, and **wlst.sh** on Unix/Linux) from the following path:

   <OracleBI Home>\Middleware\oracle_common\common\bin

8. To know the **BI Service Instance key**, type the following command, and press Enter.

   > listBIServiceInstances(domainHome)

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

   <obiee_home>/user_projects/domains/bi

   The Key appears at the end of the command.

   For example, **ssi** appears as the Key.

9. To import the BAR file, execute the following command:

   > importServiceInstance('Domain Home','BI ServiceInstance key', 'Bar file to import')

   For example, i*mportServiceInstance('C:/Oracle/Middleware/Oracle_Home/user_projects/domains/bi','ssi', 'C:/AIOBIEE/instance/import/ssi.bar')*

10. When the import of BAR file is complete, exit WLST using the **exit ()** command.

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

    A confirmation dialog box appears.

12. Click **Yes**.

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

> **Note:**
>
> All the WLST commands are case sensitive.
>
> To start the WebLogic Scripting Tool on Unix or Linux, use wlst.sh command, rest all of the commands mentioned in the procedure remains same.
>
> While executing the WLST commands on Windows server, you must use forward slash (/) to avoid any error messages. For example:
>
> ```
> C:/AIBOEE/instance/import/ssi.bar
> ```

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

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

   The following roles are imported as default application roles:

   - AI Admin Role
   - AI Author Role
   - AI Consumer Role

   For a list of privileges assigned to these roles, refer to Section 9.6, "OBIEE Default Application Roles."

2. To modify the Connection Pool Settings:

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

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

      The BI Admin Tool opens.

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

      Note:

      To open the RPD in online mode, you must set the Open Database Connectivity (ODBC). Refer to the Appendix A, "Creating ODBC Connection for OBIEE Administration Tool."

      If OBIEE is installed on the Unix or Linux machine, set up the Oracle Business Intelligence Developer Client Tool on any Windows machine to access the BI Administration Tool.

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

      Modify both the connection pools: AI80OBIEE_CP and AI80OBIEE_CP_InitBlocks.

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

   Ignore the warning messages that appear during the consistency check.

4. Create OBIEE Groups and Users. (See Section 9.4, "Creating Users and Groups in OBIEE")

5. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 9.5, "OBIEE Catalog Folder-level Permissions")

6. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics with WebLogic user credentials.

   Go to Administration > Security > Manage Privileges.

   For a list of privileges assigned to these roles, refer to Section 9.6, "OBIEE Default Application Roles."

7. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

8. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

9.2.2 Importing the BAR file when creating a new OBIEE Instance

1. Copy the BAR file from *<AI HOME>OBIEE\BAR File\ssi.bar* to a local folder on the machine where the OBIEE is installed.

2. When creating an instance in OBIEE 12c, enter the BAR file path in the **Path** field of the OBIEE Initial Application wizard screen.

3. When the installation is completed successfully, and all the processes are up, open the RPD in online mode, and change the **Connection Pool Settings**. (See To check if the BAR file has imported RPD, Catalog, and the Security Model: > Step 2)

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

   Ignore the warnings that appear during the consistency check

5. From the Enterprise Manager > Stop and Start the BI processes.

6. Create OBIEE Groups and Users. (See Section 9.4, "Creating Users and Groups in OBIEE")

7. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 9.5, "OBIEE Catalog Folder-level Permissions")

8. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics with WebLogic user credentials.

   Go to Administration > Security > Manage Privileges.

   For a list of privileges assigned to these roles, refer to Section 9.6, "OBIEE Default Application Roles."

9. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

10. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

9.3 Configuring OBIEE Repository and Web Catalog Manually

1. Copy the RPD, and Catalog files from *<AI HOME>OBIEE\RPD\ and <AI HOME>OBIEE\Catalog folders* to a machine where the OBIEE is installed.

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

   <obiee_home>\user_projects\domains\bi\bitools\bin\ admintool.cmd

   The default Repository Password is **insight123**.

3. Change the **Connection Pool Settings**. (See To check if the BAR file has imported RPD, Catalog, and the Security Model: > Step 2)

4. Save the changes, and close the RPD.

5. From the command prompt:

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

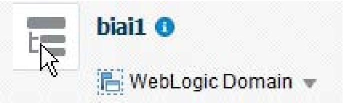
   b. Run the following command:

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

      For example, *data-model-cmd.cmd uploadrpd -I C:\AIOBIEE\RPD\ArgusInsight.rpd -W insight123 -U weblogic -P weblogic1 -SI ssi*

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

7. Click **Target Navigation**.

   The Target Navigation drop-down menu appears.

8. Go to Business Intelligence > biinstance.

The Business Intelligence Instance screen appears.

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

   A confirmation dialog box appears.

10. Click **Yes**.

    All the running processes are stopped.

11. Go to *Catalog\argusinsight\root\shared* folder:

    a. Copy **argus+insight** folder, and **argus+insight.atr** file.

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

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

    A confirmation dialog box appears.

13. Click **Yes**.

14. Create User Groups and Users manually in Admin Console. (See Section 9.4.1, "Creating Users and Groups in WebLogic Server.").

15. Create Roles and policies manually in Enterprise Manager. (See Section 9.4.2, "Creating Roles and Policies with Fusion Middleware Control.")

16. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics with WebLogic user credentials.

17. Go to Administration > Security > Manage Privileges.

    For a list of privileges assigned to these roles, refer to Section 9.6, "OBIEE Default Application Roles."

18. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 9.5, "OBIEE Catalog Folder-level Permissions")

19. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

20. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

> **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 commands on Windows server, you must use forward slash (/) to avoid any error messages. For example:
>
> ```
> C:/AIBOEE/instance/import/ssi.bar
> ```

9.4 Creating Users and Groups in OBIEE

This section provides the steps to create users and groups in OBIEE, and also comprises the following sub-sections:

- Creating Users and Groups in WebLogic Server

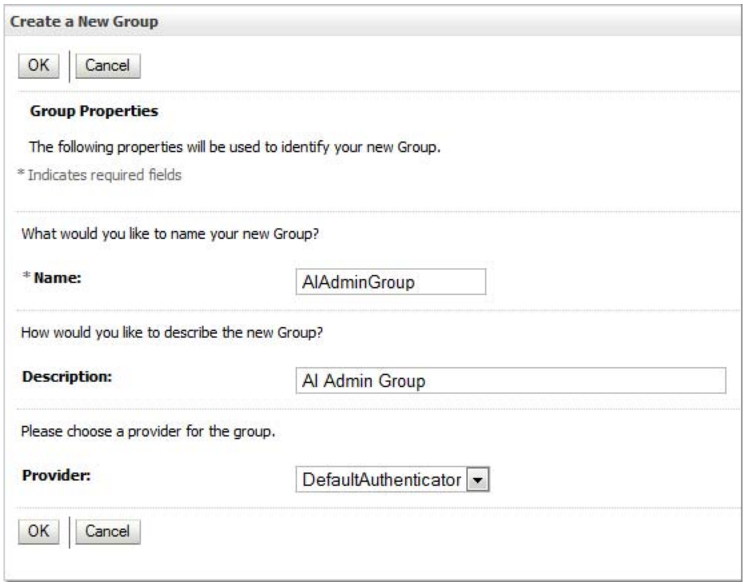
- Creating Roles and Policies with Fusion Middleware Control

9.4.1 Creating Users and Groups in WebLogic Server

To create users and groups in OBIEE:

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

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



Create a New Group

Group Properties

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

* Indicates required fields

What would you like to name your new Group?

*Name: AIAdminGroup

How would you like to describe the new Group?

Description: AI Admin Group

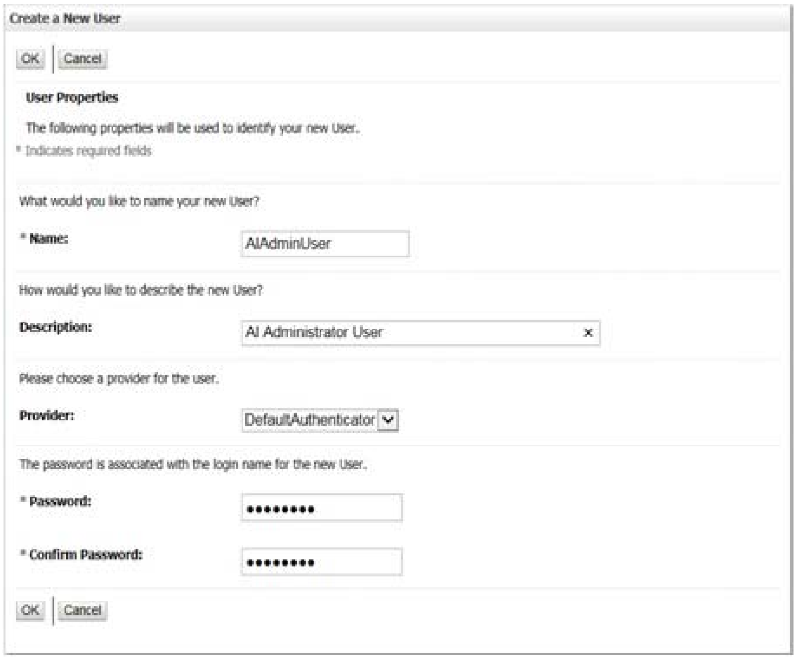
Please choose a provider for the group.

Provider: DefaultAuthenticator

To create users in the Fusion Middleware Control:

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

   The Create a New User dialog box appears.



Create a New User

User Properties

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

* Indicates required fields

What would you like to name your new User?

* Name: AIAdminUser

How would you like to describe the new User?

Description: AI Administrator User

Please choose a provider for the user.

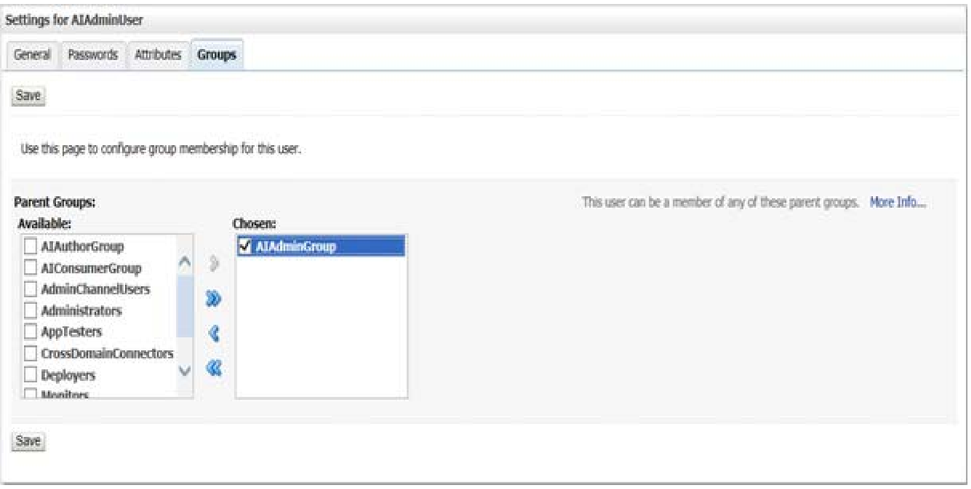
Provider: DefaultAuthenticator

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

* Password: ••••••••

* Confirm Password: ••••••••

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**.



Settings for AIAdminUser

Use this page to configure group membership for this user.

Parent Groups:

This user can be a member of any of these parent groups. More Info...

Available:

- □ AIAuthorGroup
- □ AIConsumerGroup
- □ AdminChannelUsers
- □ Administrators
- □ AppTesters
- □ CrossDomainConnectors
- □ Deployers
- □ Monitors

Chosen:

- ☑ AIAdminGroup

9.4.2 Creating Roles and Policies with Fusion Middleware Control

---

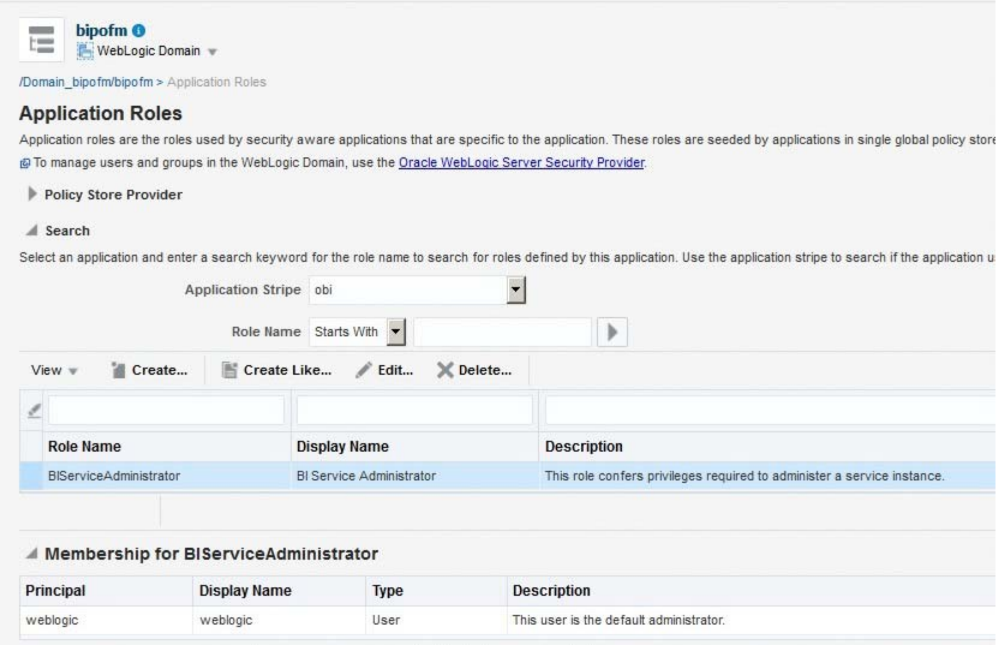
Note: This section is applicable only when you manually upload the RPD file and Catalog. For more details, refer to Section 9.3, "Configuring OBIEE Repository and Web Catalog Manually.".

To create new application roles:

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

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

   The default role available in clean slate installation appears.



/Domain_bipofm/bipofm > Application Roles

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store

To manage users and groups in the WebLogic Domain, use the Oracle WebLogic Server Security Provider.

Policy Store Provider

Search

Select an application and enter a search keyword for the role name to search for roles defined by this application. Use the application stripe to search if the application u

Application Stripe: obi

Role Name: Starts With

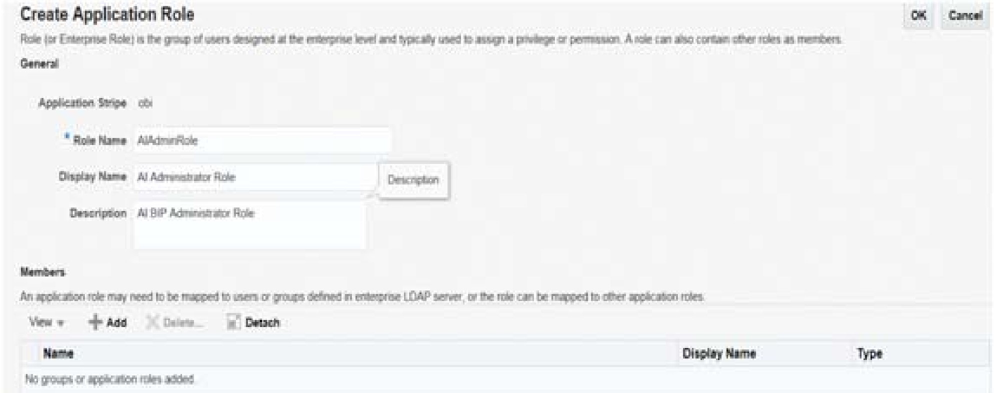
Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.

Membership for BIServiceAdministrator

Principal	Display Name	Type	Description
weblogic	weblogic	User	This user is the default administrator.

4. Click **Create**.

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



Create Application Role

Role (or Enterprise Role) is the group of users designed at the enterprise level and typically used to assign a privilege or permission. A role can also contain other roles as members.

General

Application Stripe: obi

* Role Name: AIAdminRole

Display Name: AI Administrator Role

Description: AI BIP Administrator Role

Members

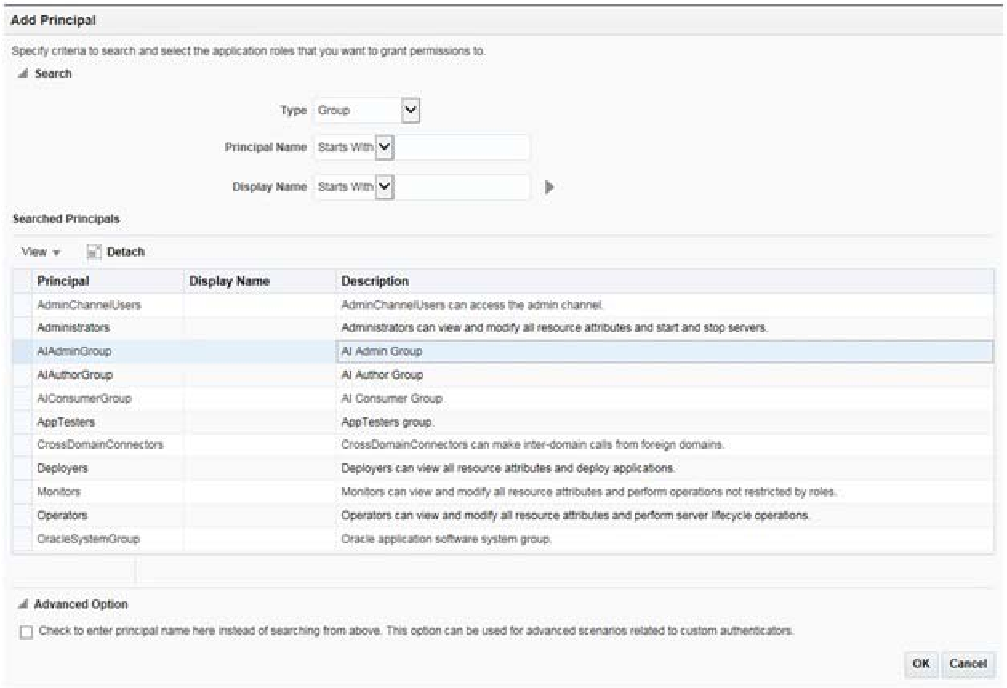
An application role may need to be mapped to users or groups defined in enterprise LDAP server, or the role can be mapped to other application roles.

Name	Display Name	Type
No groups or application roles added.		

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

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

   A list of principals appears.
8. From the list of Searched Principals, select **AIAdminGroup**, and click **OK**.



Add Principal

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

Search

Type: Group

Principal Name: Starts With

Display Name: Starts With

Searched Principals

Principal	Display Name	Description
AdminChannelUsers		AdminChannelUsers can access the admin channel.
Administrators		Administrators can view and modify all resource attributes and start and stop servers.
AIAdminGroup		AI Admin Group
AIAuthorGroup		AI Author Group
AIConsumerGroup		AI Consumer Group
AppTesters		AppTesters group.
CrossDomainConnectors		CrossDomainConnectors can make inter-domain calls from foreign domains.
Deployers		Deployers can view all resource attributes and deploy applications.
Monitors		Monitors can view and modify all resource attributes and perform operations not restricted by roles.
Operators		Operators can view and modify all resource attributes and perform server lifecycle operations.
OracleSystemGroup		Oracle application software system group.

Advanced Option

☐ Check to enter principal name here instead of searching from above. This option can be used for advanced scenarios related to custom authenticators.

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

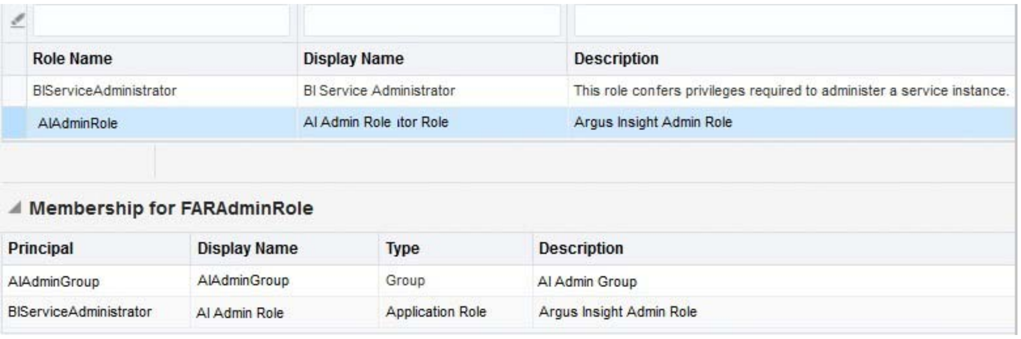
   The Add Principal dialog box appears.

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

    A list of principals appears.

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

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

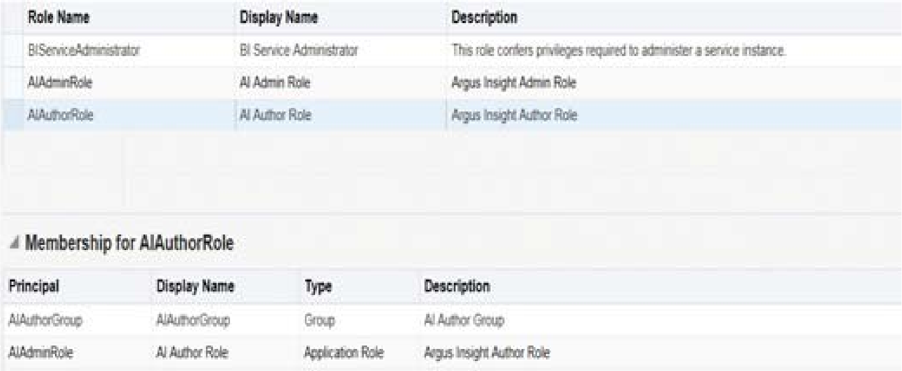


Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role ıtor Role	Argus Insight Admin Role

Membership for FARAdminRole

Principal	Display Name	Type	Description
AIAdminGroup	AIAdminGroup	Group	AI Admin Group
BIServiceAdministrator	AI Admin Role	Application Role	Argus Insight Admin Role

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

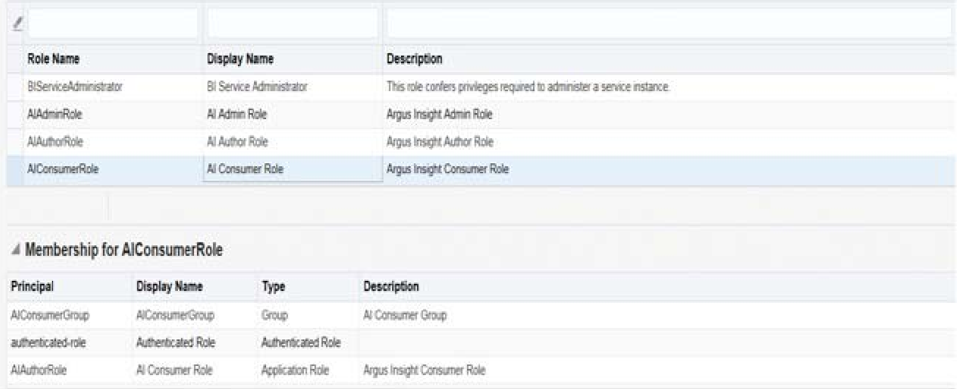


Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role	Argus Insight Admin Role
AIAuthorRole	AI Author Role	Argus Insight Author Role

Membership for AIAuthorRole

Principal	Display Name	Type	Description
AIAuthorGroup	AIAuthorGroup	Group	AI Author Group
AIAdminRole	AI Author Role	Application Role	Argus Insight Author Role

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



Role Name	Display Name	Description
BIServiceAdministrator	BI Service Administrator	This role confers privileges required to administer a service instance.
AIAdminRole	AI Admin Role	Argus Insight Admin Role
AIAuthorRole	AI Author Role	Argus Insight Author Role
AIConsumerRole	AI Consumer Role	Argus Insight Consumer Role

Membership for AIConsumerRole

Principal	Display Name	Type	Description
AIConsumerGroup	AIConsumerGroup	Group	AI Consumer Group
authenticated-role	Authenticated Role	Authenticated Role	
AIAuthorRole	AI Consumer Role	Application Role	Argus Insight Consumer Role

---

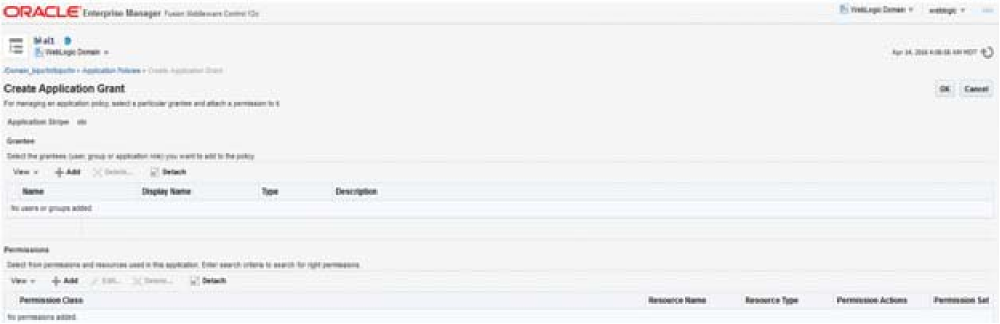
Note: For more details, refer *Section 2.8.3.1 Creating Application Roles Using Fusion Middleware Control* in *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*

To create new application policy:

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

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

   The Create Application Grant dialog box appears.



Create Application Grant

For managing an application policy, select a particular grantee and attach a permission to it

Application Stripe obi

Grantee

Select the grantees (user, group or application role) you want to add to the policy

Name	Display Name	Type	Description
No users or groups added			

Permissions

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

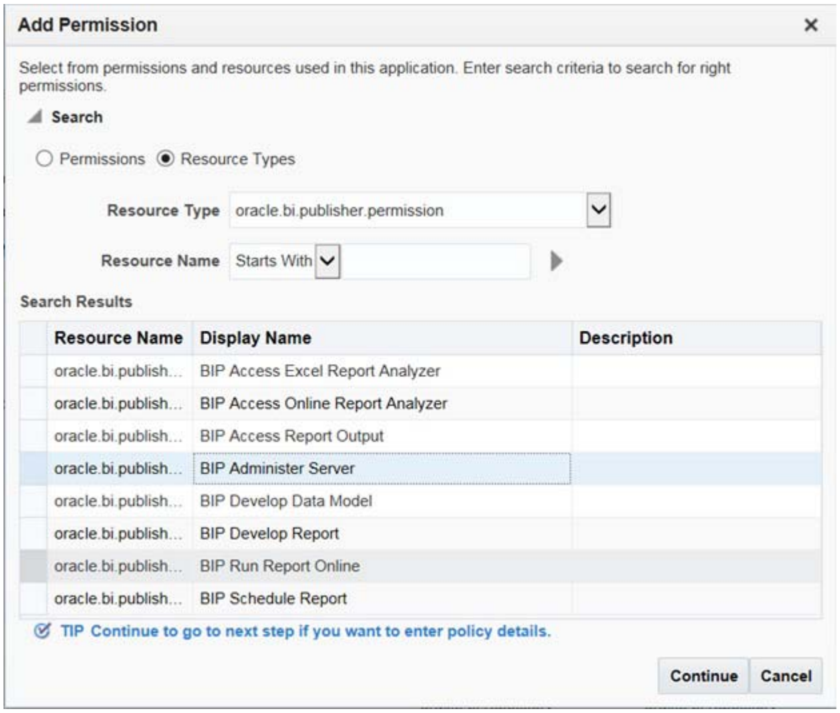
Permission Class	Resource Name	Resource Type	Permission Actions	Permission Set
No permissions added				

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 **AIAdminRole**, and click **OK**.
7. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.



Add Permission ✕

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

◢ **Search**

○ Permissions ● Resource Types

Resource Type oracle.bi.publisher.permission

Resource Name Starts With

Search Results

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

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

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
AI Admin Role	oracle.bi.catalog	*	manage
	oracle.bi.server.permission	oracle.bi.server.permission	_all_
	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanager.permission	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
	oracle.bi.repository	oracle.bi.repository	manage
	oracle.bi.scheduler.permission	oracle.bi.scheduler.permission	_all_
AI Author Role	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.develop DataModel	_all_
	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	*
	oracle.bi.delivers.job	*	schedule
AI Consumer Role	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	READ,EXECUTE
	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_

Note:

For more details, refer to *Section 2.8.3.2 Creating Application Policies Using Fusion Middleware Control* from *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*.

For a list of privileges for BIApplication Role specified above, refer to Section 9.6, "OBIEE Default Application Roles."

9.5 OBIEE Catalog Folder-level Permissions

1. Login to OBIEE Analytics with the WebLogic user credentials.
2. Go to Catalog > Shared Folders > Tasks > Permissions.

   The Permissions dialog box appears.
3. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
AI Admin Role	Open (Read, and Traverse)
AI Author Role	Open (Read, and Traverse)
AI Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

4. Go to Shared Folders > Argus Insight > Permissions.

   The Permissions dialog box appears.

5. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

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

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

   c. Click **OK**.

Setting Permission through the Catalog Manager

If you are unable to set the folder level permissions, refer to the OBIEE Catalog manager.

1. Open the catalog manager from the following path, right-click **runcat.cmd**, and click **Run as administrator**.

   <obiee_home >\user_projects\domains\<instance_name>\bitools\bin\runcat.cmd

2. Open the catalog in offline mode from the catalog path.

   For example:

   C:\Oracle\Middleware\Oracle_Home\user_projects\domains\bi1\bidata\service_instances\ssi\metadata\content\catalog\

3. Click the '/' folder.

   In the right pane, the Shared folder appears.

   a. Right-click the Shared folder, and select **Permissions**.

      The Permissions dialog box appears.

   b. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control

Accounts	Permissions
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

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

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

e. Click **OK**.

4. Right-click the Shared folder > **Properties**, set the owner as **BiServiceAdministrator**, and click **OK**.
5. From the tree structure (on the left side), click Shared folder.

   Argus Insight folder appears on the right side.

   a. Right-click Argus Insight folder, and click Permissions.

   The Permissions dialog box appears.

   b. Set the permissions as in Step 3 b to 3 d.

   c. Click **OK**.
6. Right-click Argus Insight folder > **Properties**, set the owner as **AIAdminRole**, and click **OK**.
7. Login to OBIEE Analytics, and check the folder level permissions.
8. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

9.6 OBIEE Default Application Roles

To view and administer privileges of Oracle Business Intelligence components:

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

Note:

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

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

Component	Privilege	Default Role Granted
Access	Access to Administration	AI Admin Role, BI Service Administrator
Access	Access to Answers	AI Author Role
Access	Access to BI Composer	AI Author Role
Access	Access to Briefing Books	AI Consumer Role
Access	Access to Dashboards	AI Consumer Role

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

Component	Privilege	Default Role Granted
Admin: Security	User Population - Can List Application Roles	AI Consumer Role, BI System
Admin: Security	User Population - Can List Catalog Groups	AI Consumer Role, BI System
Admin: Security	User Population - Can List Users	AI Consumer Role, BI System
Answers	Access Advanced Tab	AI Author Role
Answers	Add EVALUATE_PREDICATE Function	AI Author Role
Answers	Create Advanced Filters and Set Operations	AI Author Role
Answers	Create Analysis From Simple SQL	AI Admin Role, BI Service Administrator
Answers	Create Prompts	AI Author Role
Answers	Create Views	AI Author Role
Answers	Edit Column Formulas	AI Author Role
Answers	Edit Direct Database Analysis	AI Admin Role, BI Service Administrator
Answers	Enter XML and Logical SQL	AI Author Role
Answers	Execute Direct Database Analysis	AI Admin Role, BI Service Administrator
Answers	Save Column	AI Author Role
Answers	Save Content with HTML Markup	AI Admin Role, BI Service Administrator
Answers	Save Filters	AI Author Role
Answers	Upload Images	AI Author Role
Briefing Book	Add To or Edit a Briefing Book	AI Author Role
Briefing Book	Add to Snapshot Briefing Book	AI Consumer Role
Briefing Book	Download Briefing Book	AI Consumer Role
Catalog	Archive Catalog	AI Admin Role, BI Service Administrator
Catalog	Create Folders	AI Author Role
Catalog	Perform Extended Search	AI Author Role
Catalog	Perform Global Search	AI Author Role
Catalog	Personal Storage (My Folders and My Dashboard)	AI Consumer Role
Catalog	Reload Metadata	AI Admin Role, BI Service Administrator
Catalog	See Hidden Items	AI Author Role
Catalog	Unarchive Catalog	AI Admin Role, BI Service Administrator
Catalog	Upload Files	AI Admin Role, BI Service Administrator
Conditions	Create Conditions	AI Author Role
Dashboards	Assign Default Customizations	AI Author Role
Dashboards	Create Bookmark Links	AI Consumer Role
Dashboards	Create Prompted Links	AI Consumer Role
Dashboards	Export Entire Dashboard To Excel	AI Consumer Role
Dashboards	Export Single Dashboard Page To Excel	AI Consumer Role
Dashboards	Save Customizations	AI Consumer Role

Component	Privilege	Default Role Granted
Delivers	Chain Agents	AI Author Role
Delivers	Create Agents	AI Author Role
Delivers	Deliver Agents to Specific or Dynamically Determined Users	AI Admin Role, BI Service Administrator
Delivers	Modify Current Subscriptions for Agents	AI Admin Role, BI Service Administrator
Delivers	Publish Agents for Subscription	AI Author Role
Formatting	Save System-Wide Column Formats	AI Admin Role, BI Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access Catalog Search UI	AI Consumer Role
Home and Header	Access Catalog UI	AI Consumer Role
Home and Header	Access Data Loader	Denied: Authenticated User
Home and Header	Access Home Page	AI Consumer Role
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Rapid Search UI	AI Consumer Role
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Advanced Search Link	AI Consumer Role
Home and Header	Custom Links	AI Consumer Role
Home and Header	Dashboards Menu	AI Consumer Role
Home and Header	Favorites Menu	AI Consumer Role
Home and Header	Help Menu	AI Consumer Role
Home and Header	My Account Link	AI Consumer Role
Home and Header	New Menu	AI Consumer Role
Home and Header	Open Menu	AI Consumer Role
Home and Header	Simple Search Field	AI Consumer Role
List Formats	Access Options Tab	AI Author Role
List Formats	Add/Remove List Format Columns	AI Admin Role, BI Service Administrator
List Formats	Create Headers and Footers	AI Author Role
List Formats	Create List Formats	AI Author Role
Mobile	Enable Local Content	AI Consumer Role
Mobile	Enable Search	AI Consumer Role
My Account	Access to My Account	AI Consumer Role
My Account	Change Delivery Options	AI Consumer Role
My Account	Change Preferences	AI Consumer Role
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	AI Consumer Role
Scorecard	Add Annotations	AI Consumer Role
Scorecard	Add Scorecard Views To Dashboards	AI Consumer Role
Scorecard	Create Views	AI Author Role

Component	Privilege	Default Role Granted
Scorecard	Create/Edit Causes And Effects Linkages	AI Author Role
Scorecard	Create/Edit Initiatives	AI Author Role
Scorecard	Create/Edit KPIs	AI Author Role
Scorecard	Create/Edit Objectives	AI Author Role
Scorecard	Create/Edit Perspectives	AI Author Role
Scorecard	Create/Edit Scorecards	AI Author Role
Scorecard	Override Status	AI Consumer Role
Scorecard	View Scorecards	AI Consumer Role
Scorecard	Write Back to Database for KPI	AI Consumer Role
Segmentation	Access Segment Advanced Options Tab	AI Admin Role, BI Service Administrator
Segmentation	Access Segment Tree Advanced Options Tab	AI Admin Role, BI Service Administrator
Segmentation	Change Target Levels within Segment Designer	AI Author Role
Segmentation	Create Segment Trees	AI Author Role
Segmentation	Create Segments	AI Author Role
Segmentation	Create/Purge Saved Result Sets	AI Admin Role, BI Service Administrator
SOAP	Access AdministrationSOAPService Service	AI Consumer Role, BI System
SOAP	Access AnalysisExportViewsService Service	AI Consumer Role
SOAP	Access CatalogIndexingService Service	AI Consumer Role, BI System
SOAP	Access CatalogService Service	AI Consumer Role, BI System
SOAP	Access ConditionEvaluationService Service	AI Consumer Role, BI System
SOAP	Access DashboardService Service	AI Consumer Role, BI System
SOAP	Access HtmlViewService Service	AI Consumer Role, BI System
SOAP	Access IBotService Service	AI Consumer Role, BI System
SOAP	Access JobManagementService Service	AI Consumer Role, BI System
SOAP	Access KPIAssessmentService Service	AI Consumer Role, BI System
SOAP	Access MetadataService Service	AI Consumer Role, BI System
SOAP	Access MsgdbService Service	AI Consumer Role, BI System
SOAP	Access ReportEditingService Service	AI Consumer Role, BI System
SOAP	Access SchedulerService Service	AI Consumer Role
SOAP	Access ScorecardAssessmentService Service	AI Consumer Role, BI System
SOAP	Access ScorecardMetadataService Service	AI Consumer Role, BI System
SOAP	Access SecurityService Service	AI Consumer Role, BI System
SOAP	Access SOAP	AI Consumer Role, BI System
SOAP	Access Tenant Information	BI System
SOAP	Access UserPersonalizationService Service	AI Consumer Role

Component	Privilege	Default Role Granted
SOAP	Access XmlGenerationService Service	AI Consumer Role, BI System
SOAP	Impersonate as system user	BI System
Subject Area: "AI-Aggregate Analysis"	Access within Oracle BI Answers	AI Admin Role, AI Author Role, AI Consumer Role, BI Service Administrator
View Canvas	Add/Edit Canvas View	AI Author Role
View Column Selector	Add/Edit Column Selector View	AI Author Role
View Compound Layout	Add/Edit Compound Layout View	AI Author Role
View Contribution Wheel	Add/Edit Contribution Wheel View	AI Author Role
View Create Segment	Add/Edit Create Segment View	AI Author Role
View Create Target List	Add/Edit Create Target List View	AI Author Role
View Dashboard Prompt	Add/Edit Dashboard Prompt View	AI Author Role
View Filters	Add/Edit Filters View	AI Author Role
View Funnel	Add/Edit Funnel View	AI Author Role
View Gauge	Add/Edit Gauge View	AI Author Role
View Generic Plugin View	Add/Edit Generic Plugin View View	AI Author Role
View Graph	Add/Edit Graph View	AI Author Role
View Heat Matrix	Add/Edit Heat Matrix View	AI Author Role
View Javascript view	Edit Javascript View	AI Author Role
View Legend	Add/Edit Legend View	AI Author Role
View Logical SQL	Add/Edit Logical SQL View	AI Author Role
View Map	Add/Edit Map View	AI Author Role
View Micro Chart	Add/Edit Micro Chart View	AI Author Role
View Narrative	Add/Edit Narrative View	AI Author Role
View No Results	Add/Edit No Results View	AI Author Role
View Performance Tile	Add/Edit Performance Tile View	AI Author Role
View Pivot Table	Add/Edit Pivot Table View	AI Author Role
View Report Prompt	Add/Edit Report Prompt View	AI Author Role
View Selection Steps	Add/Edit Selection Steps View	AI Author Role
View Static Text	Add/Edit Static Text View	AI Author Role
View Table	Add/Edit Table View	AI Author Role
View Ticker	Add/Edit Ticker View	AI Author Role
View Title	Add/Edit Title View	AI Author Role
View Treemap	Add/Edit Treemap View	AI Author Role

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

10

Managing the Argus Insight Cryptography Key

This chapter describes how to update the cryptography key in Argus Insight *after* the key has been updated in Argus Safety.

10.1 Updating the Cryptography Key

After the cryptography key has been updated in Argus Safety, you must update the cryptography key in Argus Insight. This process will update all the required passwords in Argus Insight using the new key.

To update the cryptography key and regenerate passwords:

1. Log in to the Argus Insight client.
2. Click **Start.**
3. Navigate to **Programs > Oracle > Argus Insight,** and then select **Cryptography Key Management.**

   The Argus Insight Key Management - Login dialog box appears.
4. Enter the following to log in to the Key Management tool:

   a. APR_USER password.

   b. Argus Insight database name.

   c. Click **OK.**

      After successful authentication, the Argus Insight Key Management - Regenerate passwords dialog box appears.
5. Enter the new key from the Argus Safety Server.

   You may copy **UserCryptoKey** from the ArgusSecureKey.ini file, which is present on all Argus Safety Servers in C:\Windows folder. Make sure you use the exact key used by the corresponding Argus Safety Server.
6. Click **Regenerate passwords** to start the password regeneration process.

   When the password regeneration process completes, the following information appears:

   - Status of the regeneration process (success or fail)
   - Lists of the passwords that changed

10.1.1 Copying Initialization Files to Other Servers

After you change the cryptography key using the Key Management tool, you must manually copy the **AI.ini** and **Argus SecureKey.ini** initialization files from the C:\Windows folder of the Argus Insight Web Server to the following folders:

- C:\Windows of all Cognos Servers
- C:\Windows of all Argus Insight Web Servers

You must copy the AI.ini and Argus SecureKey.ini files to keep the cryptography key and the APR_USER password in sync on all the servers. In case these files are not copied, the Cognos Server or any other Argus Insight Web Server will not function.

10.1.2 Restarting IIS and Running ETL

After you change the cryptography key, you must complete the following steps on the Argus Insight Web Server to reflect the changes:

1. Restart the Internet Information Services (IIS).
2. Run the incremental ETL.

11

Uninstalling the Argus Insight Application

This chapter describes how to uninstall the Argus Insight application.

11.1 Uninstalling Argus Insight from the Web Server

To uninstall the Argus Insight application from the Web Server:

1. Log in to the Argus Insight Web Server as a user with administrator privileges.
2. Navigate to **Control Panel, Programs,** and then select **Program and Features.**
3. Select **Uninstall or change a program.**
4. Right-click on Argus Insight, and click **Uninstall**.

   The Argus Insight wizard is initiated and the Welcome screen appears with options to modify, verify, and remove programs.
5. Select **Remove**, and click **Next.**

   A dialog box appears to confirm that you want to completely remove the selected application and all of its features.
6. Click **Yes** to continue.

   The Argus Insight application is uninstalled completely and a message appears when the process is completed.
7. Click **Finish.**

   A warning message appears stating that you must restart your computer to complete uninstall process of Argus Insight.

   Be sure to save your work and close other open applications before continuing.
8. Click **OK** to restart the Argus Insight Web Server.

11.1.1 Deleting the Argus Insight Folder from the Web Server

After you uninstall the Argus Insight application, you must restart the server. In addition, you must manually remove the Argus Insight folder from the installation directory. The install wizard does not automatically remove this folder.

To remove the Argus Insight folder after an uninstall:

1. Log in to the Argus Insight Web Server as a user with administrator privileges.
2. Go to the Argus Insight installation directory (that is, the directory where Argus Insight was installed before you uninstalled the application).
3. Delete the Argus Insight folder and its contents from this location.

11.1.2 Resetting the IIS

If you uninstall Argus Insight, be sure to reset the Internet Information Services (IIS) before you install the Argus Insight application again.

A

Creating ODBC Connection for OBIEE Administration Tool

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

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

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

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

   The Oracle BI Server DSN Configuration dialog box appears.
5. Enter the following fields:

   a. **Name—**AIOBIEE (or any name)

   b. **Description**—Argus Insight OBIEE (or any description)

   c. **Server—**OBIEE Server Name
6. Click **Next**.

   a. **Login ID**—weblogic

   b. **Password—**<password for weblogic>

   c. **Port—**The port must be same as mentioned in the Managed Server port list for OBIEE BI Server.

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

   The Oracle BI Server DSN Configuration dialog box appears.
8. From the list of database, select **AI80_SRC**.
9. Click **Finish**.