# Oracle® Argus Insight

Installation Guide

Release 7.0.2

**E38586-01**

February 2013

Oracle Argus Insight Installation Guide, Release 7.0.2

E38586-01

# Contents

## 1 Introduction

## 2 Installing Argus Insight

## 3 Creating the Argus Insight Data Mart Structure

## 4 Configuring the Argus Insight Application

## 5 Extracting, Transforming, and Loading Data

## 6 Configuring the Cognos 8 Environment

## 7 Configuring the BusinessObjects XI Environment

## 8 Configuring the BIP Environment

## 9 Managing the Argus Insight Cryptography Key

## 10 Uninstalling the Argus Insight Application

# Preface

This *Oracle Argus Insight Installation Guide* describes installing — or upgrading to — Argus Insight 7.0.2. 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
- Related Documents
- 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 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.

## Related Documents

This section lists the documents in the Argus Insight documentation set, followed by their part number. The most recent version of each guide is posted on the Oracle website; see "Finding Oracle Health Sciences Documentation" on page xi.

- *Oracle Argus Insight Administrator's Guide*
- *Oracle Argus Insight User's Guide*
- *Oracle Argus Insight Minimum Security Configuration Guide*
- *Oracle Argus Insight Extensibility Guide*
- *Oracle Argus Insight Report Mapping Guide*

The release notes are also posted in the Oracle Health Sciences documentation library.

In addition, Argus Insight customers can request copies of the following Argus Insight technical reference manuals from Customer Support:

- *Oracle Argus Insight CMN Profile Enterprise Table Guide* (Part E28489)
- *Oracle Argus Insight CMN Profile Global Table Guide* (Part E28488)
- *Oracle Argus Insight Database Administrator's Guide* (Part E28486)
- *Oracle Argus Insight Entity Relationship Diagram Reference* (Part E28485)
- *Oracle Argus Insight Report Mapping Reference* (Part E28487)

# 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 that compliments Argus Safety.

The Argus Insight Extract Transform and Load (ETL) engine extracts data from the Argus Safety database and populates a data warehouse in a format to enable efficient querying. The various query, drill-down, and output features of Argus Insight let you analyze your safety, workflow, or product data from all angles and produce reports that provide immediate business impact and maximum efficiency in decision-making.

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** and the two terms have been used interchangeably in this document.

## 1.1 Argus Insight Product Overview

In Argus Insight, you can generate a report in either of the following ways:

- Through a query, retrieve a set of specific type of cases (*Case Series*) from the data mart and then run 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 one of these reports on the Case Series: the built-in *Standard Reports* or the custom reports you create and store in the *Report Writer library*.

- Run the report on all the cases in the data mart.

You can use the Report Writer to query the data mart directly and run reports.

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

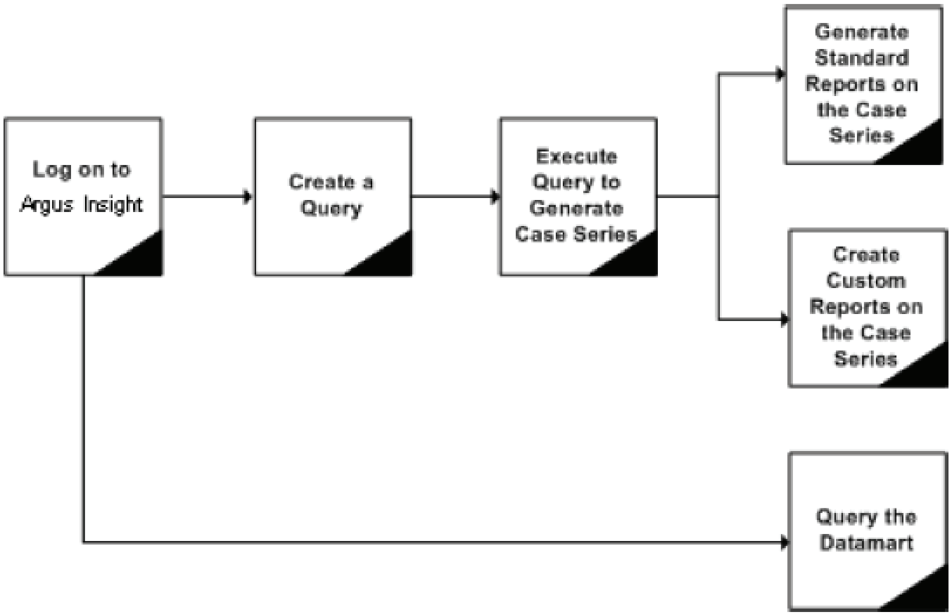

Log on to Argus Insight
Create a Query
Execute Query to Generate Case Series
Generate Standard Reports on the Case Series
Create Custom Reports on the Case Series
Query the Datamart

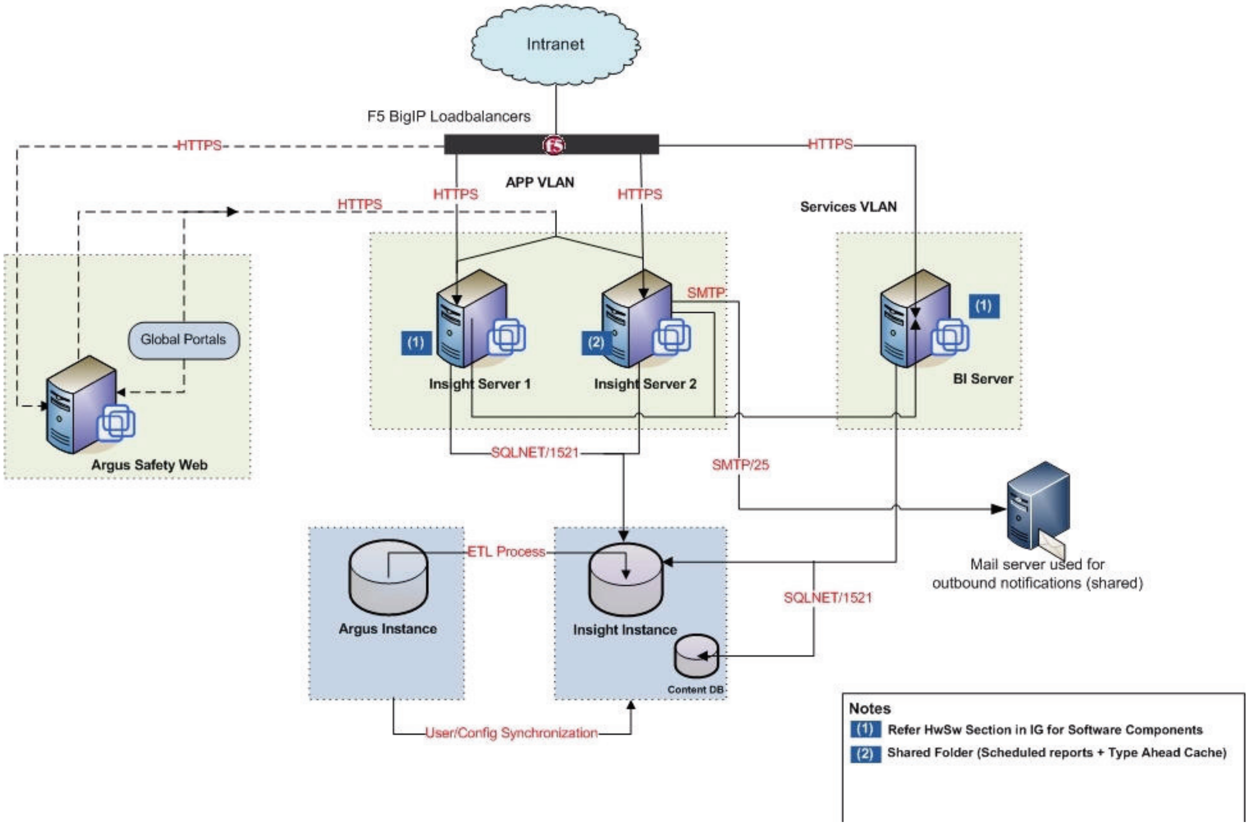
Table 1–1 describes the various features of Argus Insight:

***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 and applying Boolean and Set operations on them. |
| Case Series | A list of cases that match the query criteria. |
| Standard Reports | Predefined reports built into Argus Insight. These reports are grouped into these categories:<br>■ Case Processing (for use with BusinessObjects only)<br>■ Compliance<br>■ Configuration<br>■ General<br>■ Management<br>■ Pharmacovigilance<br>Typically, these reports are run on the Case Series. |
| Report Writer | Lets you query the data mart and create custom reports by selecting any data mart fields as report columns. In the report output, you can apply filters, create nested groupings, and perform operations such as sort, total, count, and drill.<br>The custom reports you create can be stored in the Report Writer Library or added to the Argus Insight application; you can run the stored reports on a Case Series. |

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

---

**Note:** You can use the following combinations of the Business Intelligence tools with Argus Insight:

- BusinessObjects/BIP
- Cognos/BIP
- BIP

---

- Database Server
- Argus Insight Client

***Table 1–2 Argus Insight Software and Hardware Requirements***

| Component | Requirements |
|---|---|
| **Argus Insight Web Server** | **Supported Operating Systems:**<br>■ Windows 2008 R2 Enterprise (64 bit) (English version)<br>**Oracle Database Software:**<br>■ Oracle Client 11.2.0.1 or 11.2.0.3 (32 bit) (with SQL Plus, SQL Loader, Oracle and OLEDB Objects)<br>■ Oracle Data Provider for .Net 11.2.0.1 or 11.2.0.3<br>**Hardware Requirements:**<br>■ Up to 5000 cases in the system: 2x2.6 GHz processors, 4 GB memory<br>■ More than 5000 cases in the system: 4x2 GHz processors, 8 GB memory<br>**Additional Software Requirements:**<br>■ Dotnet Framework 3.5 Service Pack 1<br>■ IIS 7.5 (IIS 6.0 compatibility pack should also be installed)<br>■ SOAP Toolkit 3.0<br>■ Microsoft Internet Explorer 7.0, 8.0, or 9.0<br>■ Adobe Reader 9.3.4<br>■ Microsoft Visual C++ 2008 Redistributable<br>■ MSXML 6.0<br>**Note:** The Argus Insight Web Server should be configured for Simple Mail Transfer Protocol (SMTP) for email support.<br>**BusinessObjects XI Requirements:**<br>If you are using BusinessObjects XI (BOXI) with Argus Insight, you need a BusinessObjects XI, Release 3.1, Service Pack 4 client on the Argus Insight Web Server. |
| **Cognos or BusinessObjects Server** | **Supported Operating Systems:** Same as the Argus Insight Web Server<br>**Oracle Database Software:** Same as the Argus Insight Web Server<br>**Hardware Requirements:** Same as the Argus Insight Web Server<br>**Additional Software Requirements:**<br>■ Dotnet Framework 3.5 Service Pack 1<br>■ IIS 7.5 (IIS 6.0 compatibility pack should also be installed)<br>■ Microsoft Internet Explorer 7.0, 8.0, or 9.0<br>**Reporting Tool (if you are using Cognos):**<br>■ Cognos 8.4.1 BI Server (default installation with all components except Cognos Content Database)<br>■ Cognos 8.4.1 BI Modeling (default installation with all components)<br>■ Cognos 8.4.1 SDK (default installation with all components)<br>■ SOAP Toolkit 3.0<br>**Reporting Tool (if you are using BusinessObjects):**<br>■ BusinessObjects XI, Release 3.1, Service Pack 4 (for single tenant installations only). The server should be installed with both IIS and JSP enabled.<br>■ Apache Tomcat 5.0.27 (default installation on BOXI) / WebSphere 6.0 |

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

| Component | Requirements |
|---|---|
| **BI Publisher (BIP)** | **Supported Operating Systems:**<br>▪ Windows 2008 R2 Enterprise (64 bit), (English version)<br>▪ Oracle Enterprise Linux X86 (Version: 5.5.0.0.0 and 5.7.0.0), (English version)<br>▪ Oracle Enterprise Linux X86-64 (Version: 5.5.0.0.0 and 5.7.0.0), (English version)<br>▪ Solaris 10, (English version)<br>▪ Oracle Enterprise Linux 6.3 UEK, (English version)<br>**Oracle Database Software:**<br>▪ 11.2.0.1 Client<br>▪ 11.2.0.3 Client<br>**Tool Version:**<br>▪ BIP 11.1.1.6 |

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

| Component | Requirements |
|---|---|
| **Database Server** | **Supported Operating Systems:**<br>■ Oracle Enterprise Linux X86 (Version: 5.5.0.0.0 and 5.7.0.0), (English version)<br>■ Oracle Enterprise Linux X86-64 (Version: 5.5.0.0.0 and 5.7.0.0), (English version)<br>■ Solaris 10, (English version)<br>■ Oracle Enterprise Linux 6.3 UEK (English version)<br>**Oracle Database Software:**<br>■ Oracle Database Server (Standard/Enterprise - AL32UTF8 character set) - Version 11.2.0.1/11.2.0.3 (32/64-bit)<br>❏ Oracle Advanced Security Transparent Data Encryption* (Optional)<br>❏ Oracle Advanced Security Network Encryption (Optional)<br>***Note:** Oracle Database TDE feature is part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition 11g (http://www.oracle.com/technetwork/database/options/advanced-security/index.html).<br>TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications.<br>While Argus Insight product has not undergone a full certification with the Oracle Database TDE feature, a set of basic sanity tests show that Argus Insight will functionally work with TDE using tablespace level encryption. This result is in-line with the expected result given the transparent nature of TDE to applications.<br>Hence, when Argus Insight is used in conjunction with TDE using tablespace encryption, it is a supported configuration.<br>However, customers who wish to use TDE on the Argus Insight Database should perform their own functional testing and performance testing to verify the performance impacts. The factors of TDE should be taken into account in the performance requirements and hardware sizing necessary to support the solution in the customer's environment.<br>■ Oracle RAC 11g R2<br>■ Exadata 11g R2<br>**Note:** Oracle database standard edition is supported for single tenant deployment only.<br>**Note:** Cognos Content Store for Argus Insight is not supported by Cognos on Oracle Database 11.2.0.3 database when installed on the Oracle Enterprise Linux operating system.<br>Content Store for Cognos is supported on Oracle 11.2.0.2 database when installed on the Oracle Enterprise Linux operating system. In this case, Oracle Client on Cognos Web Server must be 11.2.0.2. You must note that Oracle 11.2.0.2 for OEL is supported only for Cognos Content Database and not for Argus Insight data mart.<br>**Hardware Requirements:**<br>■ Up to 5000 cases in the system: 2x2 GHz processors, 4 GB memory<br>■ 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 |
|---|---|
| **Argus Insight Client** | **Supported Operating Systems:**<br>- Windows XP Professional, Service Pack 3 (32 bit), (English version)<br>- Windows 7 (32 bit), (English version)<br>**Hardware Requirements:**<br>- 2.0 GHz Minimum, 1 GB Memory<br>**Additional Software Requirements:**<br>- Adobe Acrobat Reader 9.3.4<br>- Microsoft Excel 2007 or 2010<br>- Microsoft Internet Explorer 7.0, 8.0, or 9.0 |

## 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, Cognos Server, or BusinessObjects 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. Type **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, type **United States.**
     b. Click **OK** to save your changes and close the dialog box.
  4. Exit from the Registry Editor.
  5. Restart the server. Your changes will not take effect until you restart the server.

#### 1.3.1.1 Additional Notes for the 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.

#### 1.3.1.2 Additional Notes for the 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.
- During installation verification, the system reports that files from the Cognos 8 folder are missing. You can ignore this error.

#### 1.3.1.3 Additional Notes for the 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.
- If you are not being authenticated in BusinessObjects through the Argus Insight application, run the following command on the BusinessObjects Server before you open a web intelligence document through Argus Insight:

  ```
  C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis-ga "NT AUTHORITY\NETWORK SERVICE"
  ```

  Alternatively, you can assign the required rights to IIS users.

### 1.3.2 Installation Requirements for the Argus Insight Client

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

- The Argus Insight URL must be added to the trusted sites.
- Cookies must be enabled to the lowest possible security level.
- Javascript must be enabled.
- The **Allow script-initiated windows without size or position constraints** setting in Internet Explorer must be enabled.

  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 your changes.

#### 1.3.2.1 Troubleshooting Problems with the Cognos Report Writer

> **Note:** The information in this section applies *only if* the following two conditions are true:
>
> - You are using Cognos as your Business Intelligence tool.
> - You are using either Internet Explorer 8 or 9.

If you are unable to open the Cognos Report Writer from Argus Insight using Internet Explorer 8 or 9, execute the following steps on each Argus Insight client machine where this issue is encountered:

1. Start Internet Explorer.
2. Open the **Tools** menu and select **Internet Options.**
3. Select the **Security** tab.
4. Select **Trusted Sites** and then click **Sites.**
5. Enter the URL for Argus Insight and then click **Add.**
6. Click **Close** to return to the Security tab.
7. Select **Trusted Sites** and then click **Custom level.**
8. Scroll to the Scripting settings.
9. Disable the **Enable XSS Filter** setting.
10. Click **OK** to save your changes.

### 1.3.3 General Installation Notes and Information

- Single Sign On (through Oracle Access Manager) in Argus Safety does not work if Cognos is LDAP enabled. In this scenario, you will be presented with the Argus Insight Login screen.
- 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. Enter either the Argus Safety URL or the Argus Safety Load Balancer URL in the Argus Safety Load Balancer Server text box.

# 2

# Installing Argus Insight

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

This chapter includes the following topics:

## 2.1 About a Cognos 8 versus BusinessObjects XI Installation

With Argus Insight 7.0.2, you can use Cognos 8 or BusinessObjects XI as your Business Intelligence (BI) tool. Installing Argus Insight is different depending on which BI tool you are using:

- If you are using Cognos 8, installing Argus Insight is a two-step process. First, you run the installation wizard to install Argus Insight components onto the Web Server. You then run the installation wizard again to install Argus Insight components onto the Cognos Server.
- If you are using BusinessObjects XI, installing Argus Insight is a one-step process. You run the installation wizard to install Argus Insight components onto the Web Server only.

## 2.2 Before You Install the Argus Insight Application

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

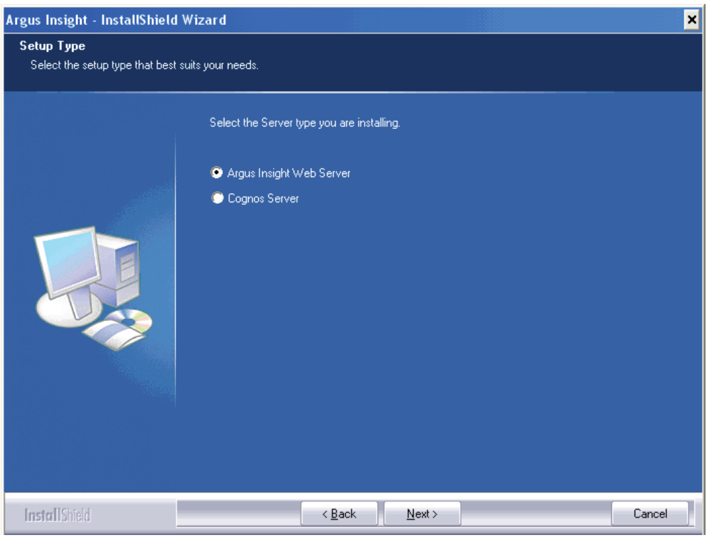
1. **Requirements —** Read Section 1.2, "Software and Hardware Requirements" and verify that your system meets the minimum requirements.
2. **Database Instance —** Verify that the Argus Insight database instance has been created and that it is running. In addition, verify that the database has been created using the character set of your Argus Safety database.
3. **Cryptographic Key —** Log in to the Argus Safety Web Server. Copy the cryptographic key from the ArgusSecureKey.ini file. You need to specify this key during the installation of Argus Insight.

4. **Security —** Log in to the Argus Insight Web Server.
    a. Make sure 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.
5. **Cognos Requirement —** If you are using Cognos 8 with Argus Insight, log in to the Cognos Server and ensure that ASP and ASP.Net extensions are enabled in IIS.

## 2.3 Installing Argus Insight Components onto the Web Server

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 system opens the Welcome screen for the installation wizard, which will guide you through the installation of Argus Insight.
4. Click **Next** to continue.
5. Select the Business Intelligence (BI) tool that you are using. Argus Insight supports the following BI tools:
    - **BusinessObjects**
    - **Cognos 8**
6. Click **Next** to continue.
    - If you selected **Cognos 8,** you need to specify whether you are installing Argus Insight components onto the Argus Insight Web Server or the Cognos Server. Select **Argus Insight Web Server** and then click **Next.**



Argus Insight - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

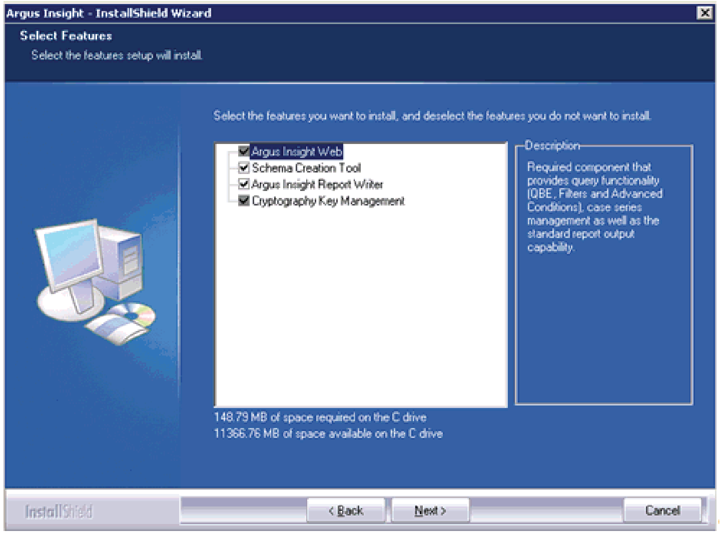
Select the Server type you are installing.

● Argus Insight Web Server

○ Cognos Server

    - If you selected **BusinessObjects,** you only install Argus Insight components onto the Argus Insight Web Server. Therefore, the system immediately prompts for your user name and company name.

7. Enter your user name and company name into the appropriate fields.
8. Click **Next** to continue. The Select Features dialog box opens.



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
- ☑ Argus Insight Report Writer
- ☑ Cryptography Key Management

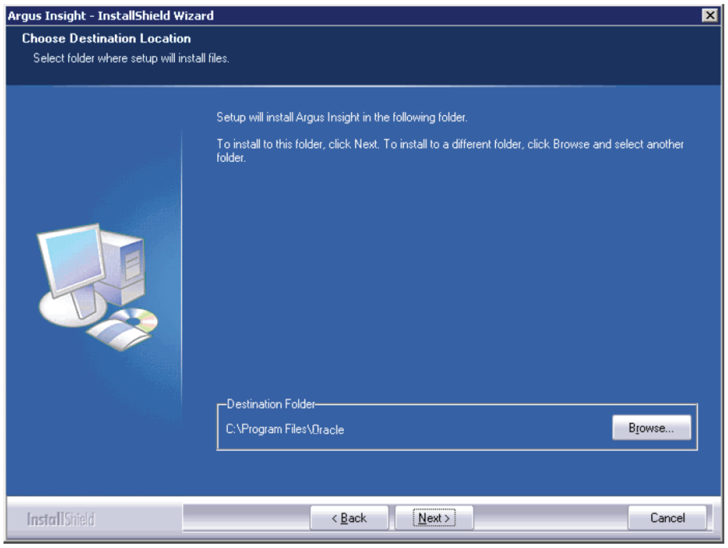
Description

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

148.79 MB of space required on the C drive

11366.76 MB of space available on the C drive

9. Clear any feature that you do not want to install. By default, the wizard installs all features.
10. Click **Next** to continue. The Choose Destination Location dialog box opens.



Argus Insight - InstallShield Wizard

**Choose Destination Location**

Select folder where setup will install files.

Setup will install Argus Insight in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

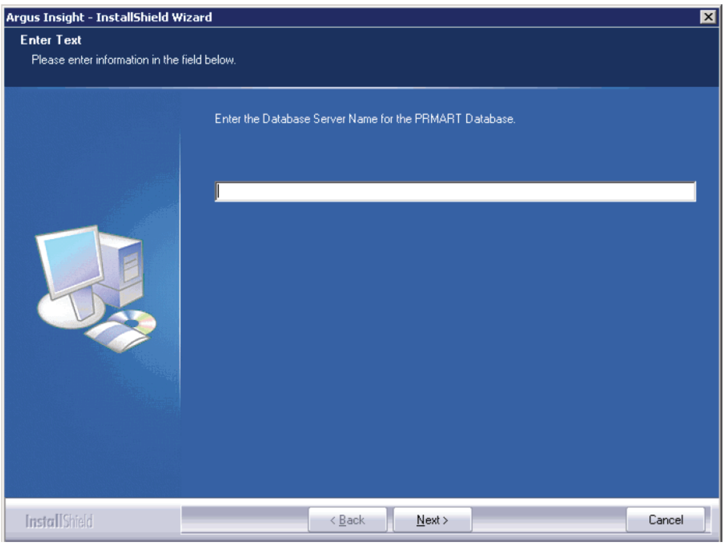
Destination Folder

C:\Program Files\Oracle

11. Specify the folder into which 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.**

    The system reports that the wizard is ready to install the Argus Insight files.
12. Click **Install** to start the installation. The system reports that Argus Insight is configuring your new software and displays a progress bar the reports the status of the installation.

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



Please enter information in the field below.

Enter the Database Server Name for the PRMART Database.

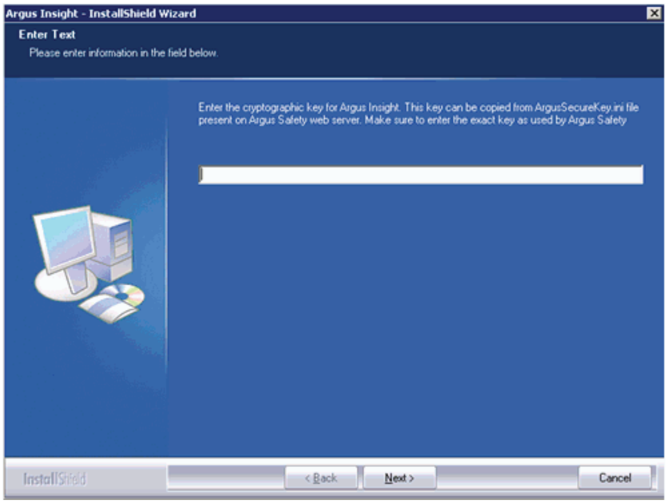
13. Enter the name of the host database server where the Argus Insight data mart is located. Click **Next.**

14. Enter the instance name for the Argus Insight data mart. Click **Next.**

15. Enter the database port number you want to assign to the Argus Insight database. Click **Next.**

    The system updates the TNSNAME.ORA file with the information you specified about the Argus Insight database.

    When the update is done, the Cryptographic Key dialog box opens.



Please enter information in the field below.

Enter the cryptographic key for Argus Insight. This key can be copied from ArgusSecureKey.ini file present on Argus Safety web server. Make sure to enter the exact key as used by Argus Safety

16. Enter the cryptographic key for Argus Insight, and then click **Next** to continue.

> **Note:** The cryptographic key is in the ArgusSecureKey.ini file located on the Argus Safety Web Server. You should have obtained this key during the pre-installation tasks.

17. Enter the password for APR_USER.

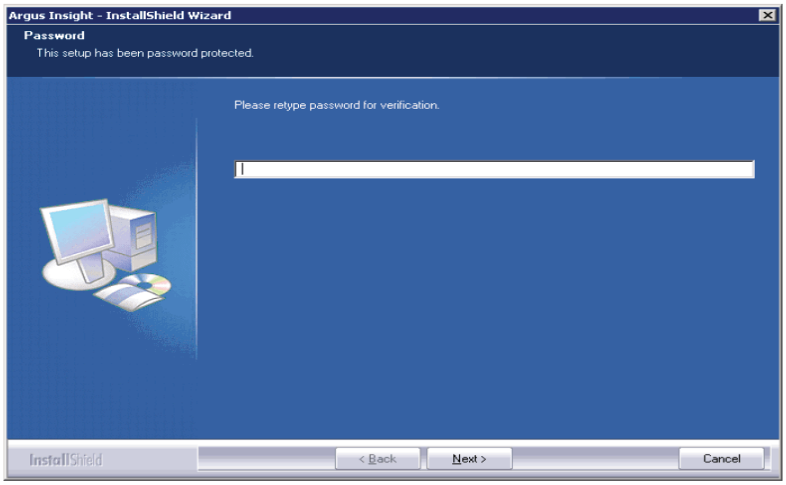
---

**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/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 2.3.1, "Changing the APR_USER Password."

---

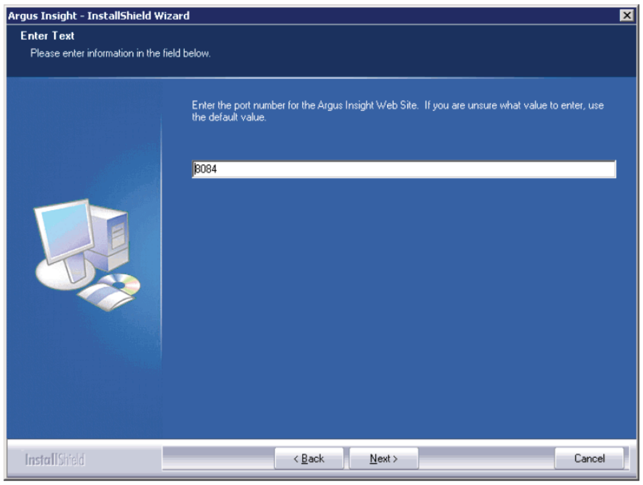
18. Click **Next** to continue. The Confirm Password dialog box opens.



Argus Insight - InstallShield Wizard
Password
This setup has been password protected.
InstallShield
< Back
Next >
Cancel

Please retype password for verification.

19. Re-enter the APR_USER password for verification.
20. Click **Next.** The Port Number dialog box opens.



Argus Insight - InstallShield Wizard
Enter Text
Please enter information in the field below.
InstallShield
< Back
Next >
Cancel

Enter the port number for the Argus Insight Web Site. If you are unsure what value to enter, use the default value.

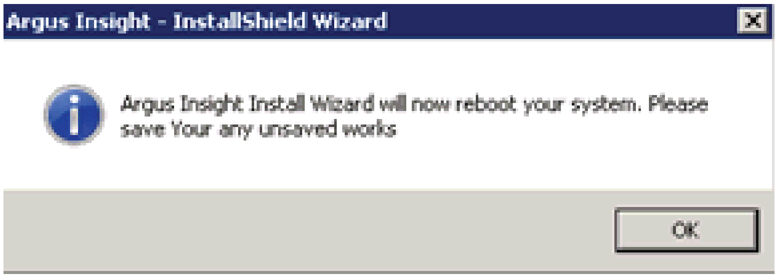
8084

21. 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.

22. Click **Next.** The system reports that the Argus Insight application has been installed successfully.

23. Click **Finish** to exit from the installation wizard. The system displays the following message:



Argus Insight Install Wizard will now reboot your system. Please save Your any unsaved works

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

## 2.3.1 Changing the APR_USER Password

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

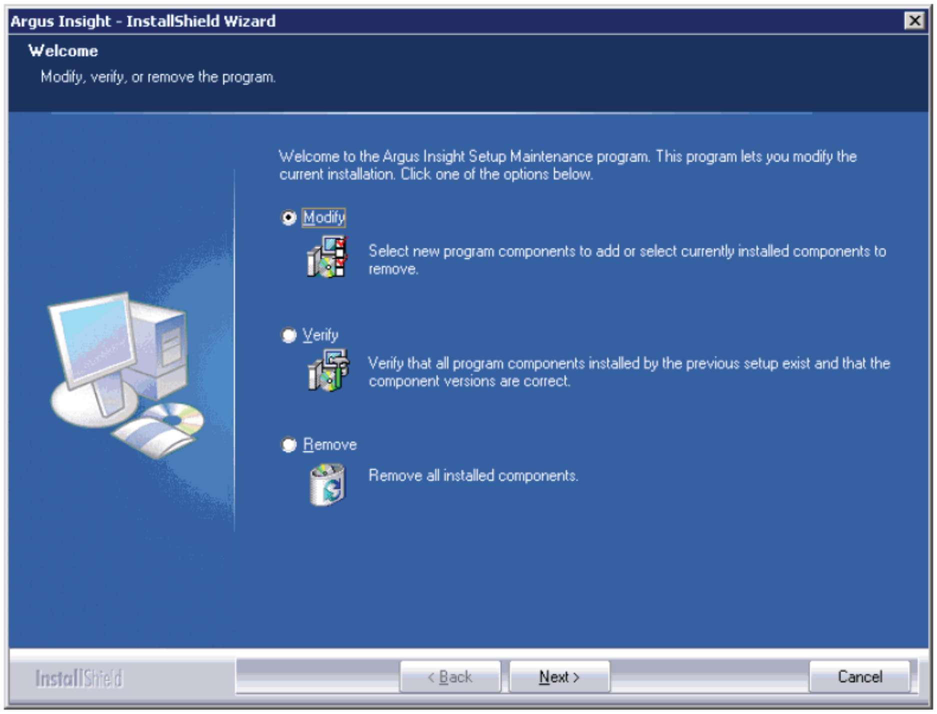
Before changing the password for the APR_USER on any Argus Insight Web Server/Cognos Server:

- Stop the Argus Insight service.
- Stop IIS on the Argus Insight Web Server.
- Stop the IIS and the Cognos service on the Cognos Server. You only need to complete this task if you are using Cognos 8 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/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 opens.



**Argus Insight - InstallShield Wizard**

**Welcome**

Modify, verify, or remove the program.

Welcome to the Argus Insight Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

● Modify

Select new program components to add or select currently installed components to remove.

○ Verify

Verify that all program components installed by the previous setup exist and that the component versions are correct.

○ Remove

Remove all installed components.

2. Select **Modify** and then click **Next.**
3. Select **Change the password for APR_USER.** 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.** The system prompts for confirmation of the new password.
6. Enter the new **APR_USER** password a second time for verification.
7. Click **Next.**

   The system updates the password for APR_USER.

### 2.3.2 Copying the ADODB.DLL for Report Scheduling

Argus Insight needs the ADODB.DLL file, which is a Microsoft ActiveX Data Object, so report scheduling works properly.

To copy the ADODB.DLL to the correct location:

1. Locate the adobe.dll file in the following folder:

   *Argus_Insight_Installation_Directory*\Oracle\ArgusInsight\Bin
2. Drag and drop the adodb.dll from that location into the following folder:

   *drive:*\WINDOWS\assembly

## 2.4 Installing Argus Insight Components onto the Cognos Server

> **Note:** This installation is required ***only if*** you are using Cognos 8 as your Business Intelligence tool with Argus Insight.

In the previous section, you installed the Argus Insight components onto the Argus Insight Web Server. If you use Cognos 8 for your Business Intelligence tool and you use different servers for Argus Insight and Cognos 8, you also need to install the Argus Insight components onto the Cognos Server.

### 2.4.1 Running the Wizard to Install Components for Cognos 8

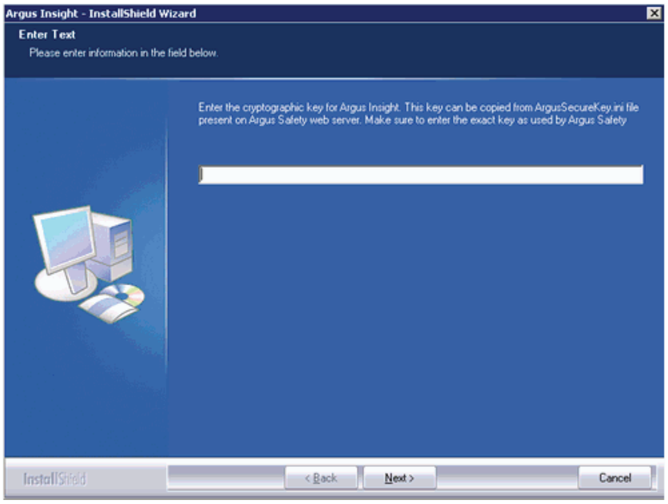
To install the Argus Insight components onto the Cognos Server:

1. Download the Argus Insight software from Oracle E-delivery and copy the software to the Cognos Server.
2. Log in to the Cognos Server as a user with administrator privileges.
3. Click **setup.exe.** The system opens the Welcome screen for the installation wizard, which will guide you through the installation of Argus Insight.
4. Click **Next** to continue.
5. Select **Cognos 8** and then click **Next.**
6. Select **Cognos Server** and then click **Next.**
7. Enter your user name and company name into the appropriate fields.
8. Click **Next** to continue. The Select Features dialog box opens.
9. Clear any feature that you do not want to install. By default, the wizard installs all features.
10. Click **Next** to continue. The Choose Destination Location dialog box opens.
11. Specify the folder into which 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.**

    The system reports that the wizard is ready to install the Argus Insight files.
12. Click **Install** to start the installation. The system reports that Argus Insight is configuring your new software and displays a progress bar the reports the status of the installation. Wait until the Database Server dialog box opens.
13. Enter the name of the host database server where the Argus Insight data mart is located. Click **Next.**
14. Enter the instance name for the Argus Insight data mart. Click **Next.**
15. Enter the database port number you want to assign to the Argus Insight database. Click **Next.**

    The system updates the TNSNAME.ORA file with the information you specified about the Argus Insight database.

    When the update is done, the Cryptographic Key dialog box opens.



Enter Text

Please enter information in the field below.

Enter the cryptographic key for Argus Insight. This key can be copied from ArgusSecureKey.ini file present on Argus Safety web server. Make sure to enter the exact key as used by Argus Safety

16. Enter the cryptographic key for Argus Insight, and then click **Next** to continue.

---

**Note:** The cryptographic key is in the ArgusSecureKey.ini file located on the Argus Safety Web Server. You should have obtained this key during the pre-installation tasks.

---

17. Enter the password for APR_USER.

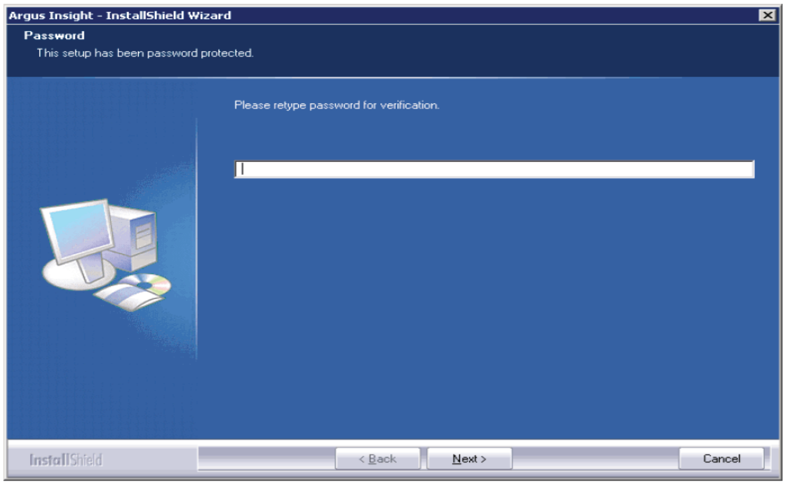
---

**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/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 2.3.1, "Changing the APR_USER Password."

---

18. Click **Next** to continue. The Confirm Password dialog box opens.

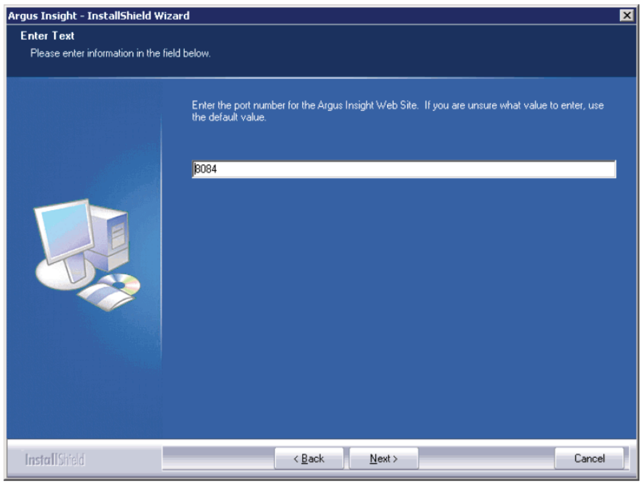


Password

This setup has been password protected.

Please retype password for verification.

19. Re-enter the APR_USER password for verification.
20. Click **Next.** The Port Number dialog box opens.



Argus Insight - InstallShield Wizard
Enter Text
Please enter information in the field below.

Enter the port number for the Argus Insight Web Site. If you are unsure what value to enter, use the default value.

8084

InstallShield
< Back
Next >
Cancel

21. Click **Next.** The system reports that the Argus Insight application has been installed successfully.
22. Click **Finish** to exit from the installation wizard. A message dialog box informs you that the Argus Insight installation wizard will now restart your system.
23. Click **OK** to restart the Cognos 8 Server.

### 2.4.2 Configuring the Cognos 8 Software Development Kit

If you are using Cognos 8 for your Business Intelligence tool, you need to configure the Cognos 8 Software Development Kit (SDK) so that Argus Insight can communicate with Cognos.

To configure the Cognos 8 Software Development Kit (SDK):

1. Change to the following directory on the Cognos Server:

   `C:\Program Files\Cognos\c8\sdk`

2. Copy the following files from the Cognos Server:
   - CDK.dll
   - cognosdotnet_2_0.dll
   - cognosdotnetassembly_2_0.dll
3. Paste the three DLL files into the following directory on the Argus Insight Web Server:

   `Argus_Insight_Installation_Directory\Oracle\ArgusInsight\Bin`

4. Register the CDK.dll file:
   1. Open the command prompt.
   2. Enter the **regsvr32** command followed by the complete path to the location of the CDK.dll. For example:

      ```
      regsvr32 "C:\Program Files\Oracle\ArgusInsight\bin\cdk.dll"
      ```

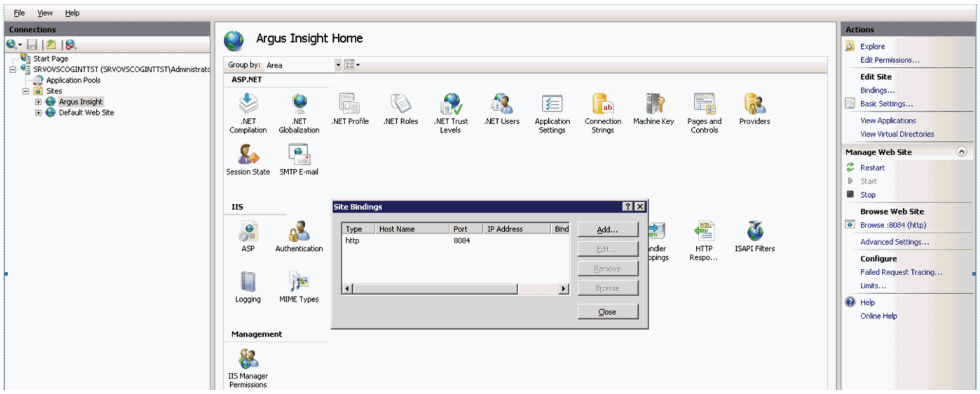
5. Click **Start,** select **Run,** and then type **assembly.**

Drag and drop the cognosdotnet_2_0.dll and cognosdotnetassembly_2_0.dll files from the `Insight_Installation_Directory\Oracle\ArgusInsight\Bin` directory into the `C:\WINDOWS\assembly` directory.

## 2.5 Enabling SSL Support for the Argus Insight Website

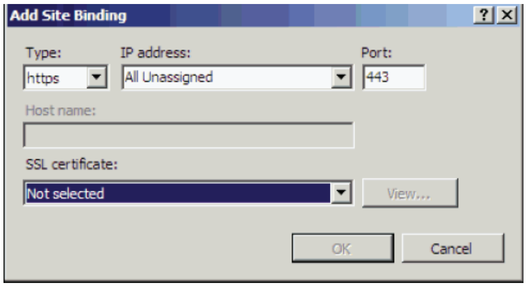
To enable SSL support for the Argus Insight website:

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 then select **Bindings.** The Site Bindings dialog box opens.



| Type | Host Name | Port | IP Address | Bind |
|---|---|---|---|---|
| http | | 8084 | | |

5. Click **Add.** The Add Site Binding dialog box opens.



Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: Not selected

6. Complete the Add Site Binding dialog box as follows:
   - 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 your source Argus database and your new Argus Insight data mart. The Extract Transform and Load (ETL) process uses this link to transfer data from your Argus database to the Argus Insight data mart for reporting purposes.

During the schema creation process, you are required to create four database users: one user for logging in to the Argus Insight application, two other users who are schema owners, and one user for supporting 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 7.0.1 to Argus Insight 7.0.2

> **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 for your changes to take effect.

## 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 11*g*R2) | 11.2.0.0.0 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:<br>■ Small (< 30,000 cases): 16<br>■ Medium (30,000 to 200,000 cases): 32<br>■ Large (200,000 to 1,000,000 cases): Default<br>■ Extra Large (> 1,000,000 cases): Default |
| PGA_AGGREGATE_TARGET | Minimum value recommended based on the total number of cases:<br>■ Small (< 30,000 cases): 0.5 GB<br>■ Medium (30,000 to 200,000 cases): 2 GB<br>■ Large (200,000 to 1,000,000 cases): 3 GB<br>■ Extra Large (> 1,000,000 cases): 4 GB |
| QUERY_REWRITE_ENABLED | TRUE (if computing statistics regularly)<br>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:<br>■ Small (< 30,000 cases): 1 GB<br>■ Medium (30,000 to 200,000 cases): 2.5 GB<br>■ Large (200,000 to 1,000,000 cases): 3.5 GB<br>■ Extra Large (> 1,000,000 cases): 4.5 GB<br>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:<br>RETENTION=NOGUARANTEE<br>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 |

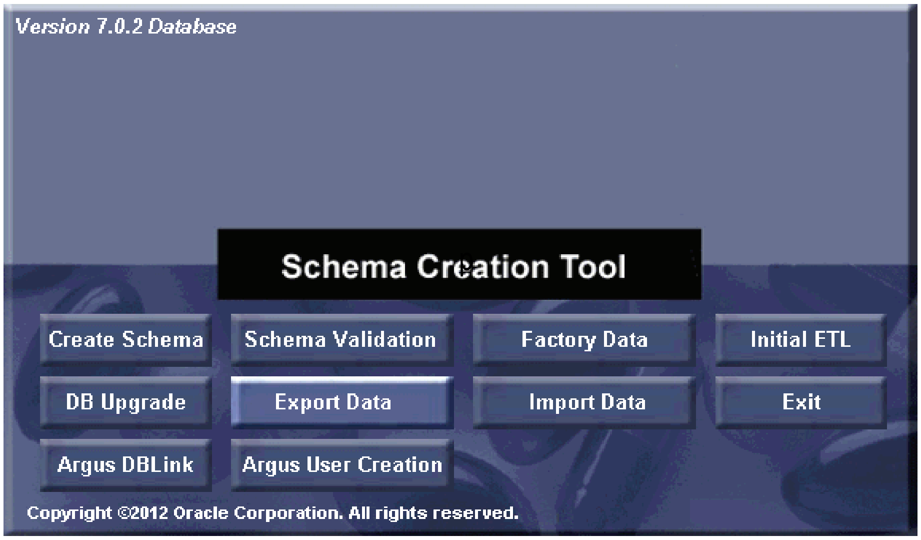
*Table 3–4 (Cont.) Tablespaces Created for the Argus Insight Data Mart*

| | | |
|---|---|---|
| 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 main window for the Schema Creation Tool opens.



Summary of the Schema Creation Tool options:

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

- **Initial ETL** — Runs the initial process of extracting, transforming, and loading data. See Chapter 5, "Extracting, Transforming, and Loading Data" for more information.
- **DB Upgrade** — Upgrades an existing Argus Insight 7.0.1 database to an Argus Insight 7.0.2 database. See Section 3.8, "Upgrading Database from Argus Insight 7.0.1 to Argus Insight 7.0.2" for more information.
- **Export Data** — Exports data. For details, see Section 4.10.1, "Exporting Data" for more information.
- **Import Data** — Imports data. For details, see Section 4.10.2, "Importing Data" for more information.
- **Argus DBLink** — Creates a link between Argus Insight and Argus Safety. See Section 3.7, "Creating a Database Link from Argus Safety to Insight Database" for more information.
- **Argus User Creation** — Lets you create Argus Insight users and roles. See Section 3.5.1, "Creating Users and Roles in the Argus Safety Database" for more information.
- **Exit** — Exits from the Schema Creation Tool.

## 3.5 Creating the Database Schema

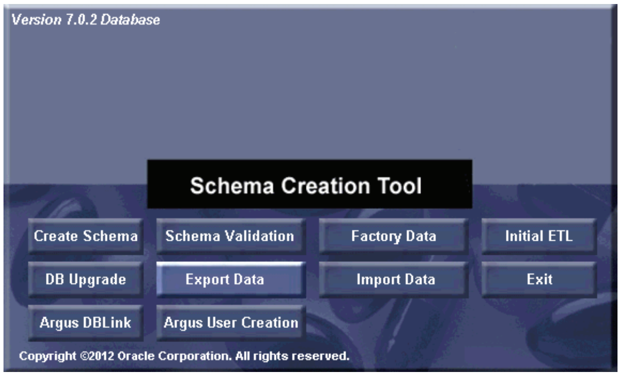
This section describes the tasks associated with creating the database schema:

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

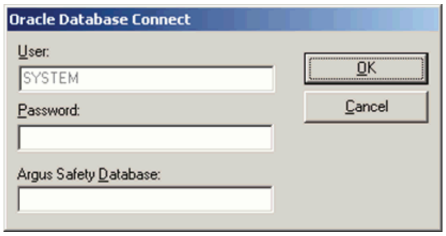
### 3.5.1 Creating Users and Roles in the Argus Safety Database

To create users and roles:

1. Start the Argus Insight Schema Creation Tool.

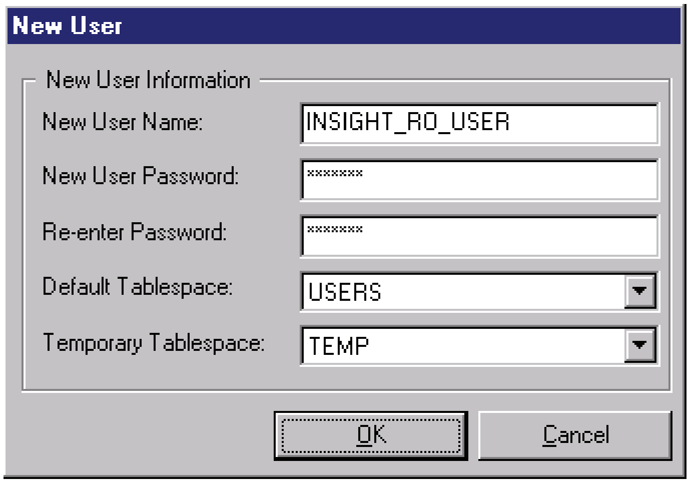


2. Click **Argus User Creation.** The Oracle Database Connect dialog box opens.



User: SYSTEM

3. Connect to the Oracle Database:
    a. In the **Password** field, type the password for the SYSTEM user.
    b. In the **Argus Safety Database** field, type the name of your Argus Safety Database instance.
    c. Click **OK.** The Argus Safety Read Only User Creation dialog box opens.
4. Click **New User.** The New User dialog box opens.



New User Name: INSIGHT_RO_USER

New User Password: *******

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

Default Tablespace: USERS

Temporary Tablespace: TEMP

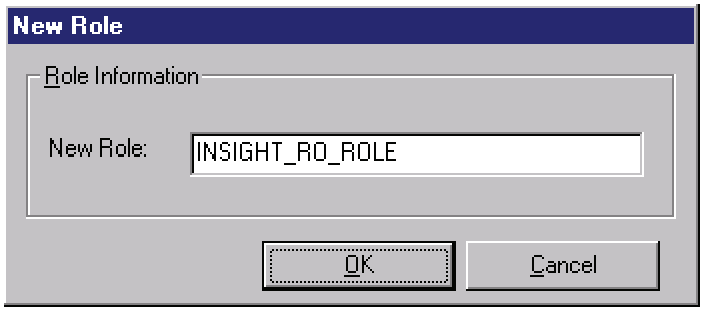
5. Complete the New User dialog box as follows:
    a. Enter a name for the new user.
    b. Specify and confirm the password for the user.
    c. Select the default and temporary tablespaces required by your corporate standards, or leave the default values.
    d. Click **OK.** The system returns to the Argus Safety Read Only User Creation dialog box.

---

**Note:** You must create the INSIGHT_RO_USER and INSIGHT_RO_ROLE even if they already 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.

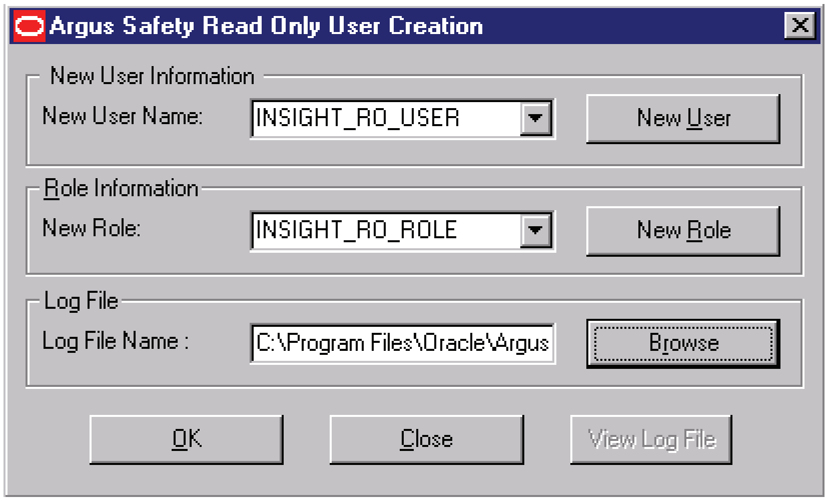
---

6. Click **New Role.** The New Role dialog box opens:



New Role: INSIGHT_RO_ROLE

7. Enter the name of the new role to create and then click **OK.** The system returns to the Argus Safety Read Only User Creation dialog box.



New User Name: INSIGHT_RO_USER

New Role: INSIGHT_RO_ROLE

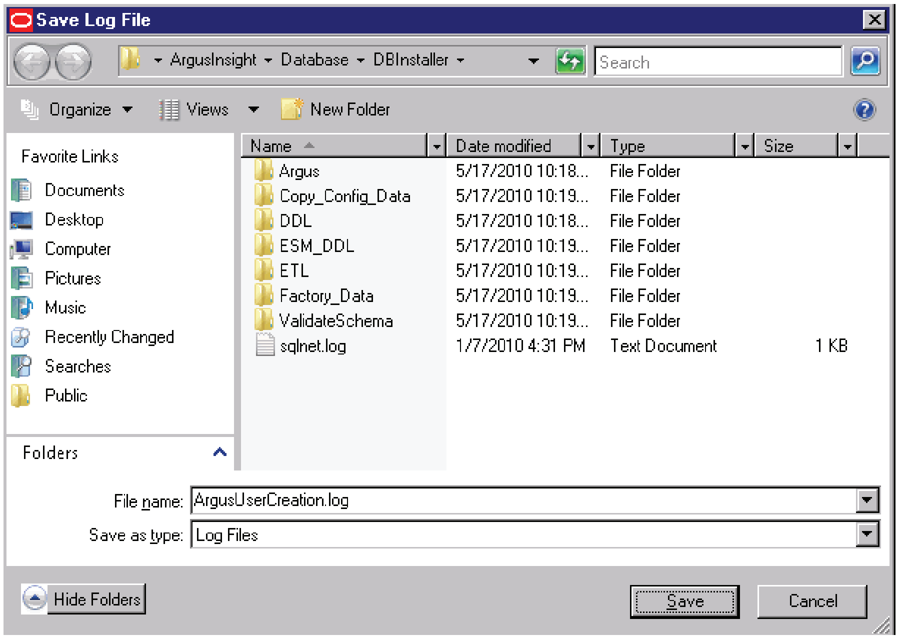
Log File Name : C:\Program Files\Oracle\Argus

---

**Note:** In case you have upgraded the database from Argus Insight 7.0.1 to 7.0.2, 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.**

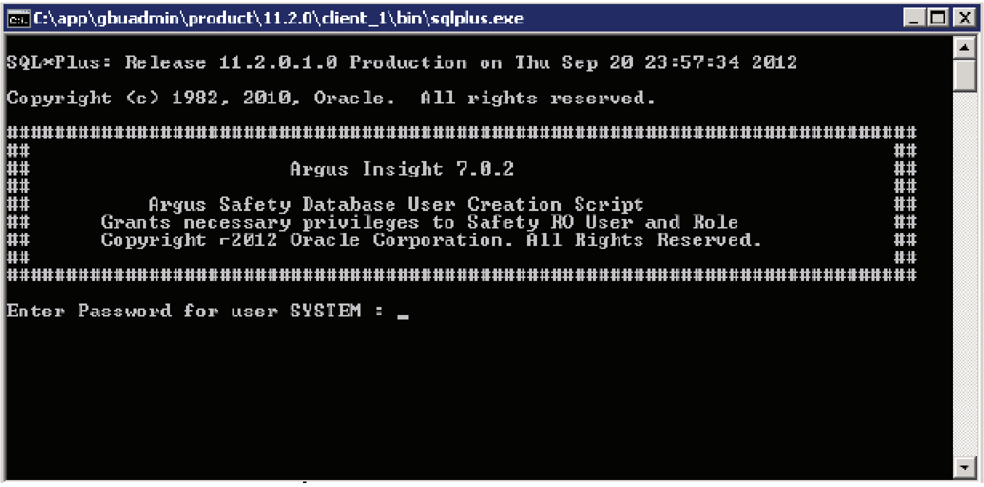


File name: ArgusUserCreation.log

Save as type: Log Files

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

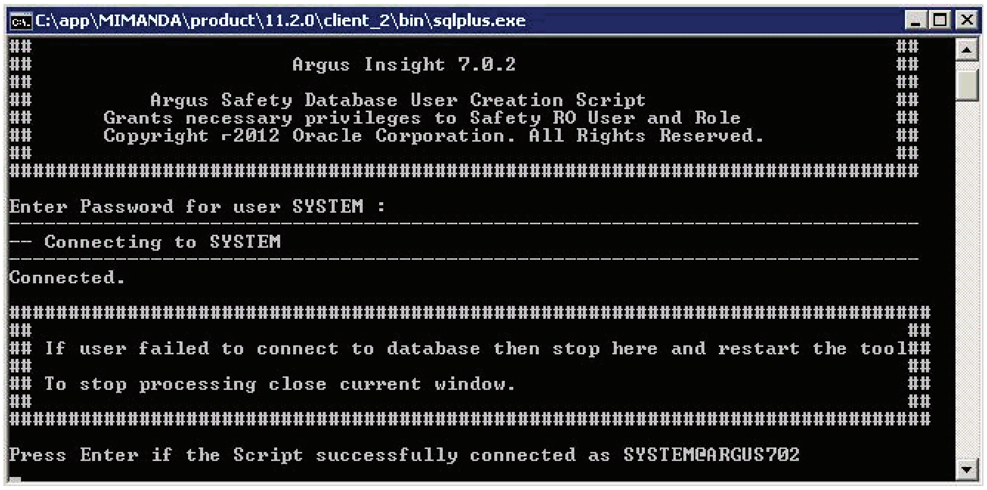
   The system displays the command prompt as shown in the following figure:



```
SQL*Plus: Release 11.2.0.1.0 Production on Thu Sep 20 23:57:34 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

#############################################################################
##                                                                         ##
##                      Argus Insight 7.0.2                                ##
##                                                                         ##
##          Argus Safety Database User Creation Script                     ##
##      Grants necessary privileges to Safety RO User and Role             ##
##      Copyright ⌐2012 Oracle Corporation. All Rights Reserved.           ##
##                                                                         ##
#############################################################################

Enter Password for user SYSTEM : _
```

10. Enter the password for the SYSTEM user and press **Enter**.

11. Verify that the script is successfully connected as <SYSTEM User Name>@<Argus Safety Database Name> as shown in the following figure:

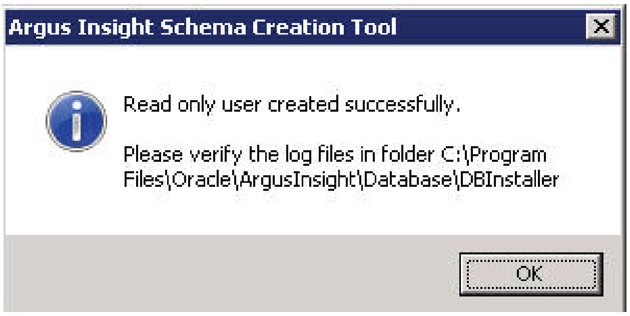


```
##                                                                         ##
##                      Argus Insight 7.0.2                                ##
##                                                                         ##
##          Argus Safety Database User Creation Script                     ##
##      Grants necessary privileges to Safety RO User and Role             ##
##      Copyright ⌐2012 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@ARGUS702
```

12. Press **Enter**. The system displays 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.

13. Verify that the information is correct, and then press **Enter** to continue. The system displays additional information about creating the user and granting privileges.

14. Press **Enter** to complete the installation. The system displays a message that the user account has been created successfully and lists the folder location of the log files as shown in the following figure:



Read only user created successfully.

Please verify the log files in folder C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller

15. Click **OK** to close the message box. The system returns 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. Close the log file when you are done reviewing.

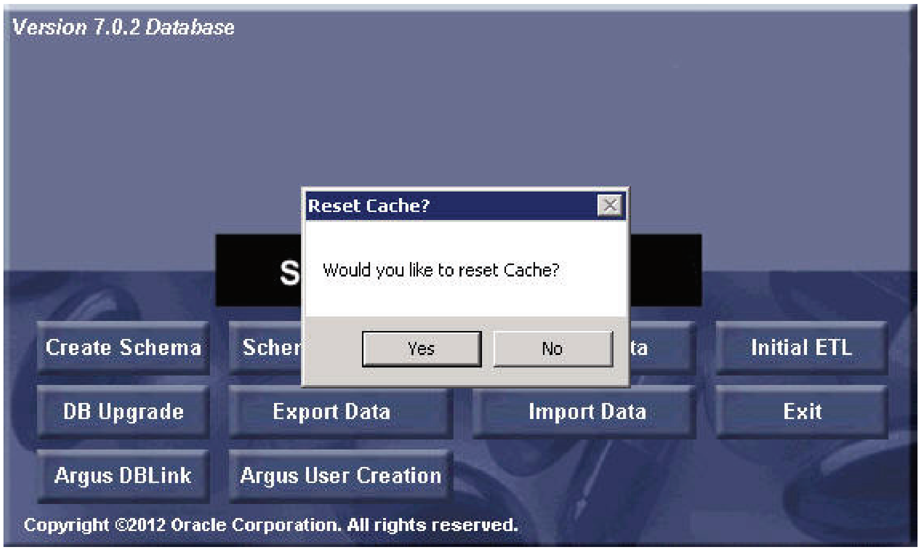
17. Click **Close** to close the **Argus Safety Read Only User Creation** dialog box.

## 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. Argus Insight prompts for confirmation that you want to reset the Cache.



2. Click **Yes.**

   Argus Insight clears the cache and logs the action 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.

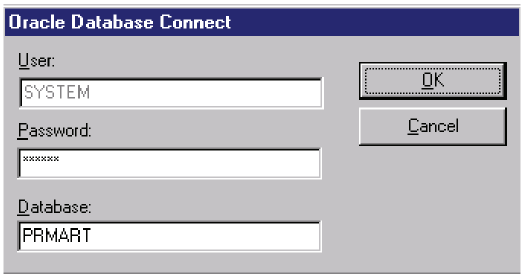
If you **do not** have remote access to SYS user, execute the **ai_sys{grant}.sql** script through SYS user. This SQL script is located in the following folder:

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 opens.



User: SYSTEM

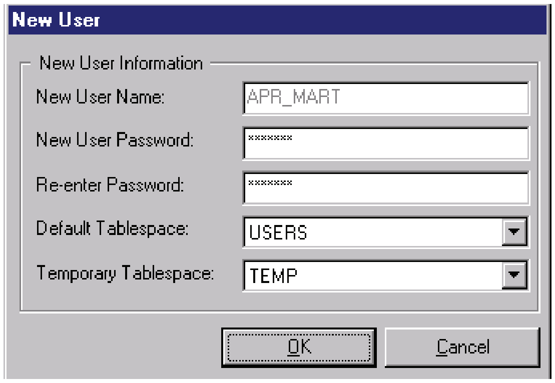
Password: ******

Database: PRMART

3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the SYSTEM user.
   b. In the **Database** field, type the TNS entry for the Argus Insight Database.
   c. Click **OK.**

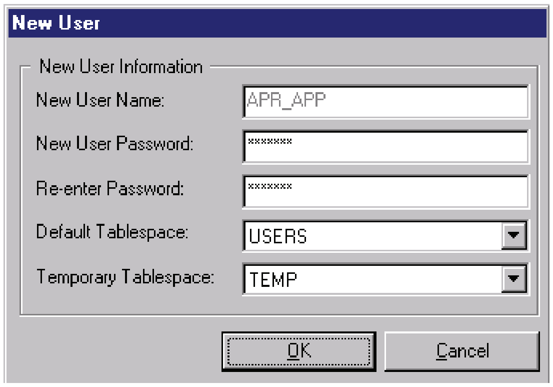
Note that:

- **If the NLS_LENGTH_SEMANTICS database parameter is not set to CHAR,** the system displays an error message. 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 system opens the New User dialog box for the **APR_MART** user.



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 system opens the New User dialog box for the **APR_APP** user.



New User Name: APR_APP
New User Password: *******
Re-enter Password: *******
Default Tablespace: USERS
Temporary Tablespace: TEMP

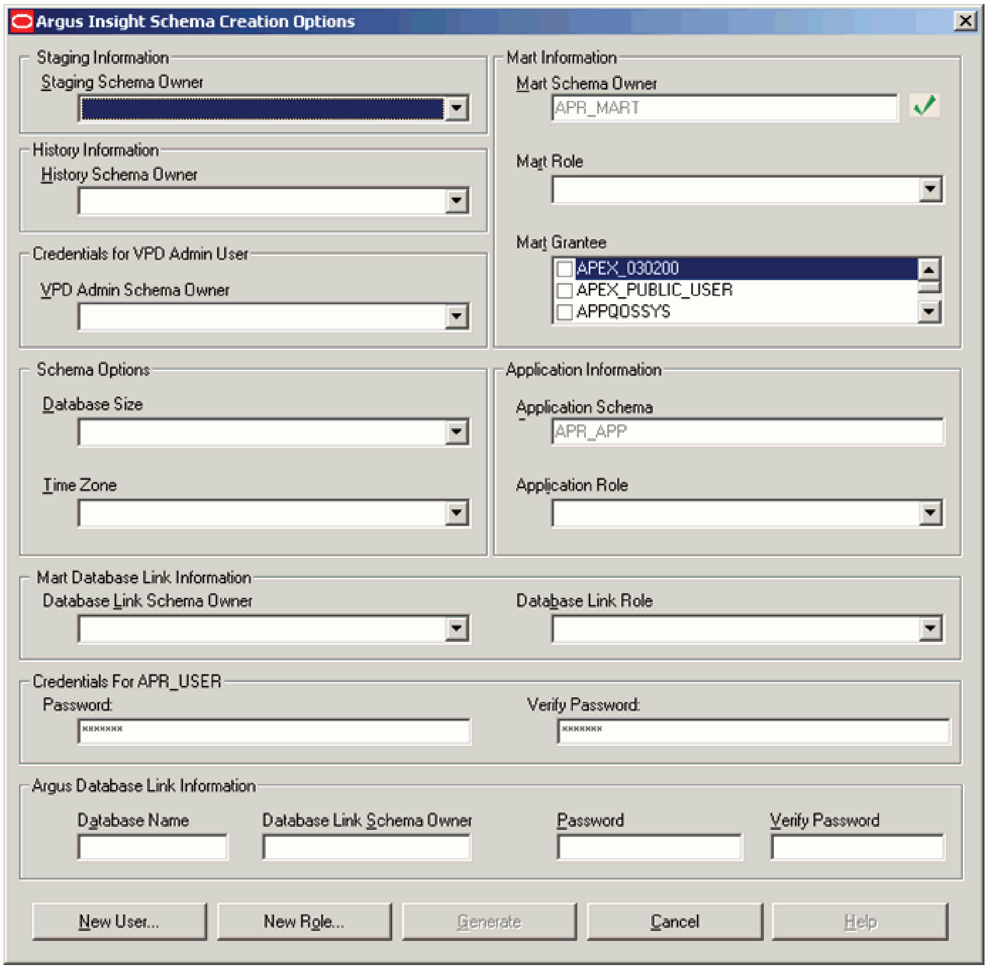
6. Enter a password for the **APR_APP** user, and then re-enter to confirm the password.

---

**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 synch 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 opens.



Mart Schema Owner: APR_MART ✓

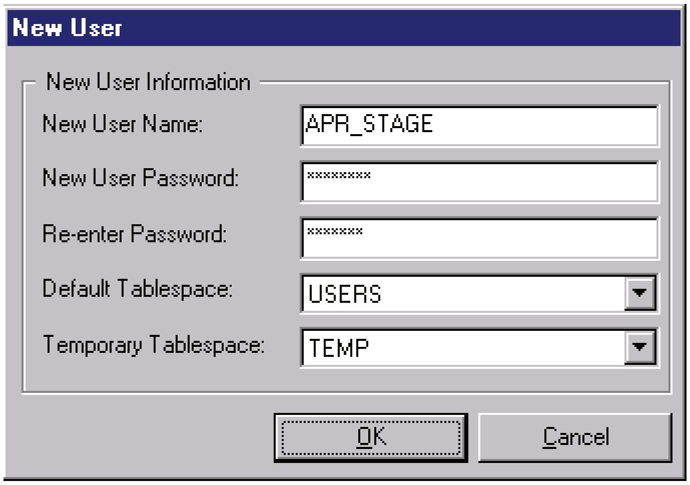
Mart Grantee:
- ☐ APEX_030200
- ☐ APEX_PUBLIC_USER
- ☐ APPQOSSYS

Application Schema: APR_APP

Password: *******

Verify Password: *******

8. Click **New User.** The **New User** dialog box opens.



New User Name: APR_STAGE

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

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

Default Tablespace: USERS

Temporary Tablespace: TEMP

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

   – APR_STAGE

   – APR_LOGIN

    - APR_LINK_USER
    - APR_HIST
    - RLS_USER

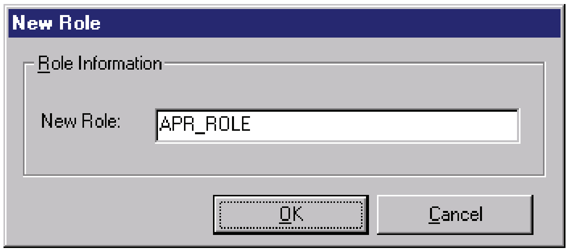
   b. In the **New User Password** field, type the password for the specified user.

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

   d. Click **OK.** The system returns to the Argus Insight Schema Creation Options screen.

   Repeat this step until you have created all five (5) users.

9. Click **New Role.** The New Role dialog box opens.



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.** The system returns to the Argus Insight Schema Creation Options screen.

   Repeat this step until you have created all three (3) roles.

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

   a. Select **APR_STAGE** from the **Staging Schema Owner** drop-down list.

   b. Select **APR_HIST** from the **History Schema Owner** drop-down list.

   c. In the **VPD Admin Schema Owner** field of the Credentials for VPD Admin Users section, select **RLS_USER.**

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

   e. Select **APR_ROLE** from the **Mart Role** drop-down list.

   f. Check the **APR_LOGIN** checkbox from the **Mart Grantee** section.

   g. Select **APR_APP_ROLE** from the **Application Role** drop-down list.

   h. In the **Database Link Schema Owner** drop-down list of the **MART Database Link Information** section, select **APR_LINK_USER.**

   i. In the **Database Link Role** drop-down list of the **MART Database Link Information** section, select **APR_LINK_ROLE.**

   j. 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.

---

**k.** Enter the name of the Argus Safety database in the **Database Name** field.

**l.** Enter **INSIGHT_RO_USER** in the **Database Link Schema Owner** field.

**m.** Enter the password for the **INSIGHT_RO_USER** in the **Password** field.

**n.** Re-enter the password in the **Verify Password** field.

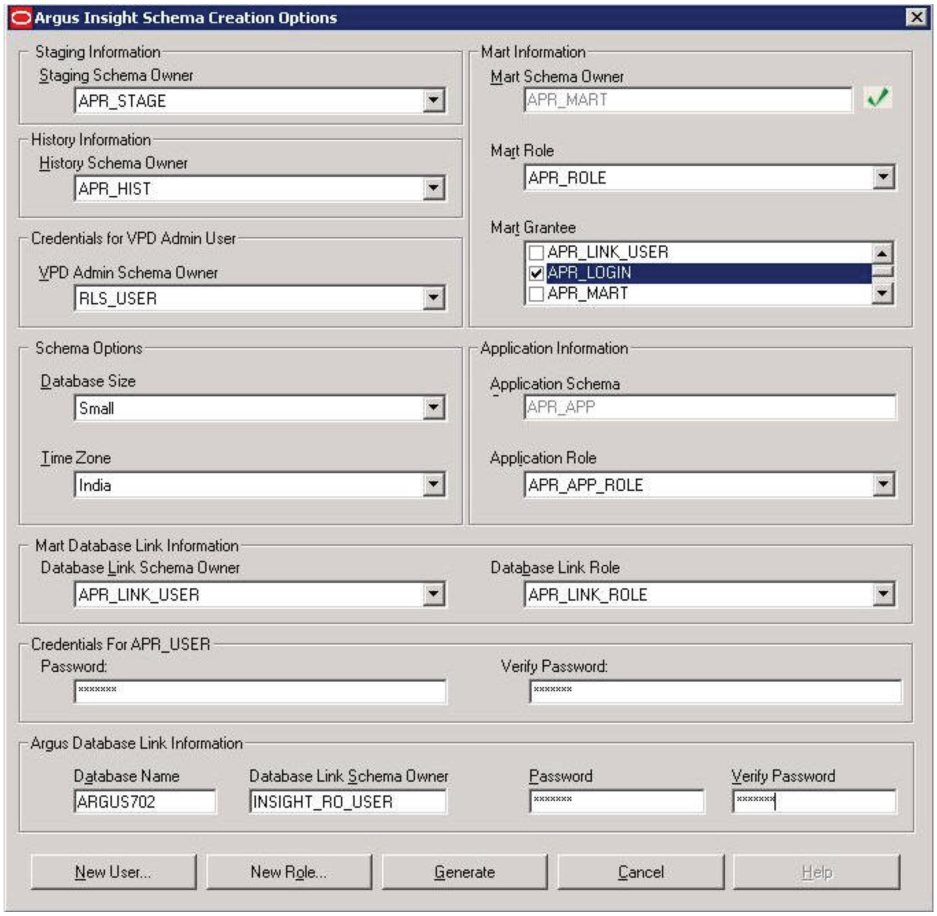
**o.** Optionally, in the Credentials for **APR_USER** section, enter and verify a new password only if you want to change the password for **APR_USER**.

All these inputs have been depicted in the following figure:

---

**Note:** You must update the **APR_USER** password using the instructions in the 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.

---



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_LINK_USER
☑ APR_LOGIN
☐ APR_MART

Schema Options
Database Size: Small
Time Zone: India

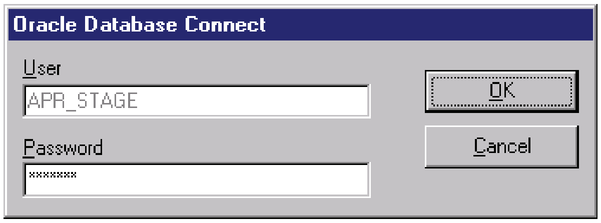
Application Information
Application Schema: APR_APP
Application Role: APR_APP_ROLE

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: ARGUS702
Database Link Schema Owner: INSIGHT_RO_USER
Password: *******
Verify Password: *******

11. Click **Generate.** The system prompts for the password of the staging user (APR_STAGE user).



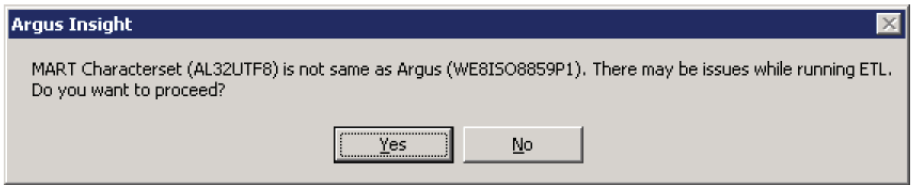
**Oracle Database Connect**

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.



**Argus Insight**

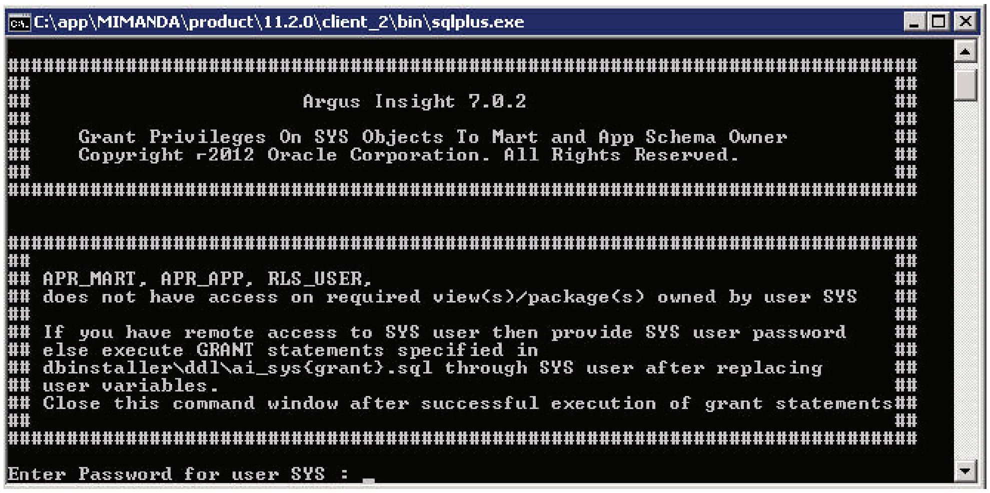
MART Characterset (AL32UTF8) is not same as Argus (WE8ISO8859P1). There may be issues while running ETL.
Do you want to proceed?

      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 screen is displayed:

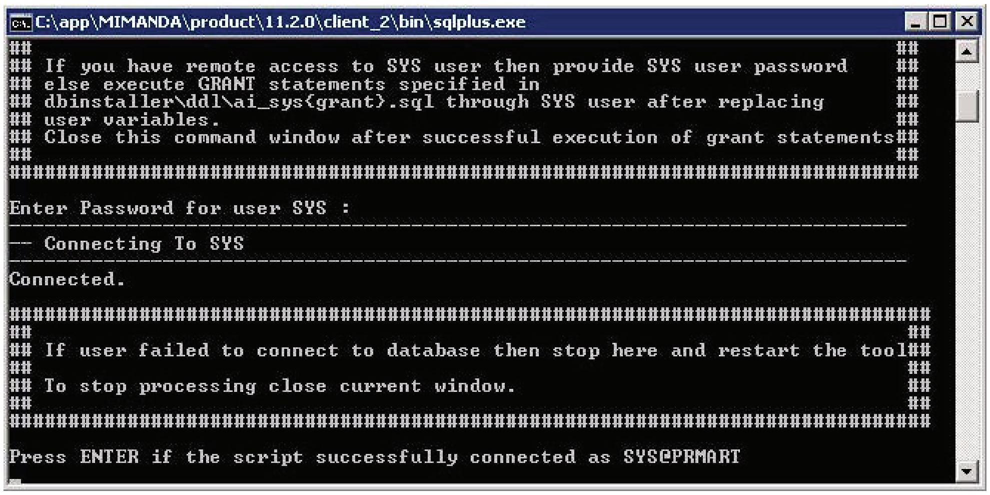


C:\app\MIMANDA\product\11.2.0\client_2\bin\sqlplus.exe

```
#############################################################################
##                                                                         ##
##                       Argus Insight 7.0.2                               ##
##                                                                         ##
##    Grant Privileges On SYS Objects To Mart and App Schema Owner         ##
##    Copyright r2012 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**.

    This displays the following command screen:



C:\app\MIMANDA\product\11.2.0\client_2\bin\sqlplus.exe

```
##                                                                         ##
## 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

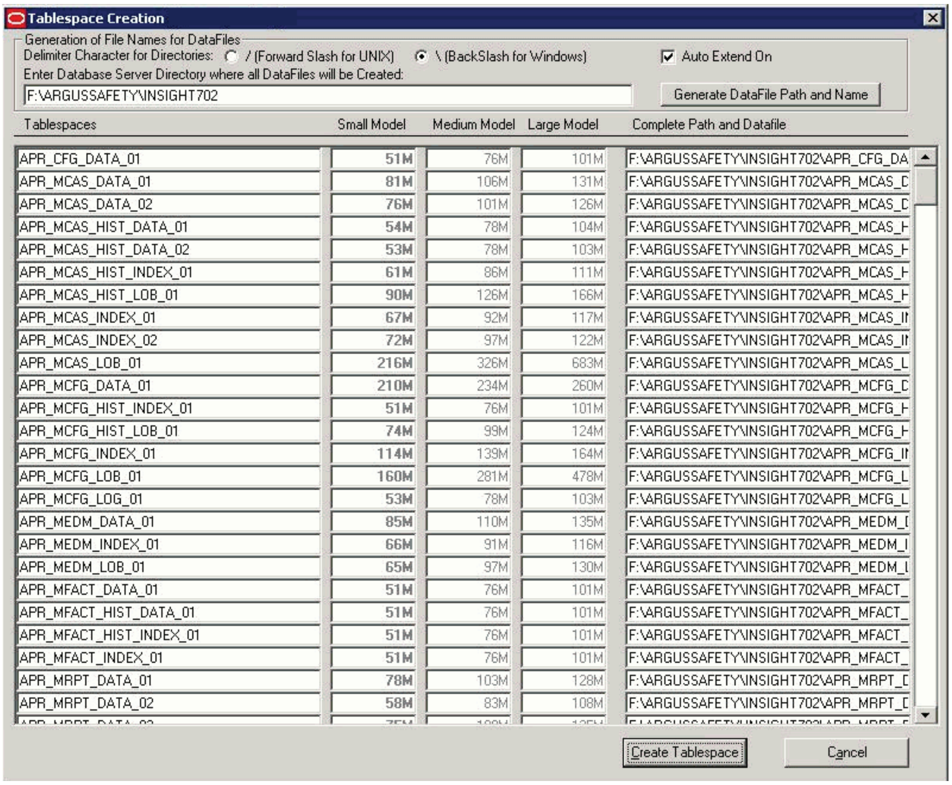
    If you **do not** have remote access to SYS user,  and you have already executed the **ai_sys{grant}.sql** script through SYS user, you would execute Step17 of this procedure. This SQL script is located in the following folder:

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

14. Verify that the script is successfully connected as <SYS User Name >@<Argus Insight Database Name> and press **Enter**. This again displays the command screen with the Grant succeeded message displayed 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 opens.



Tablespace Creation

Generation of File Names for DataFiles

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

Enter Database Server Directory where all DataFiles will be Created:

F:\ARGUSSAFETY\INSIGHT702

| Tablespaces | Small Model | Medium Model | Large Model | Complete Path and Datafile |
|---|---|---|---|---|
| APR_CFG_DATA_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_CFG_DA |
| APR_MCAS_DATA_01 | 81M | 106M | 131M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_DATA_02 | 76M | 101M | 126M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_HIST_DATA_01 | 54M | 78M | 104M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_HIST_DATA_02 | 53M | 78M | 103M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_HIST_INDEX_01 | 61M | 86M | 111M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_HIST_LOB_01 | 90M | 126M | 166M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_INDEX_01 | 67M | 92M | 117M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_INDEX_02 | 72M | 97M | 122M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_ |
| APR_MCAS_LOB_01 | 216M | 326M | 683M | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS_L |
| APR_MCFG_DATA_01 | 210M | 234M | 260M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_ |
| APR_MCFG_HIST_INDEX_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_ |
| APR_MCFG_HIST_LOB_01 | 74M | 99M | 124M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_ |
| APR_MCFG_INDEX_01 | 114M | 139M | 164M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_ |
| APR_MCFG_LOB_01 | 160M | 281M | 478M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_L |
| APR_MCFG_LOG_01 | 53M | 78M | 103M | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG_L |
| APR_MEDM_DATA_01 | 85M | 110M | 135M | F:\ARGUSSAFETY\INSIGHT702\APR_MEDM_ |
| APR_MEDM_INDEX_01 | 66M | 91M | 116M | F:\ARGUSSAFETY\INSIGHT702\APR_MEDM_ |
| APR_MEDM_LOB_01 | 65M | 97M | 130M | F:\ARGUSSAFETY\INSIGHT702\APR_MEDM_ |
| APR_MFACT_DATA_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_MFACT_ |
| APR_MFACT_HIST_DATA_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_MFACT_ |
| APR_MFACT_HIST_INDEX_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_MFACT_ |
| APR_MFACT_INDEX_01 | 51M | 76M | 101M | F:\ARGUSSAFETY\INSIGHT702\APR_MFACT_ |
| APR_MRPT_DATA_01 | 78M | 103M | 128M | F:\ARGUSSAFETY\INSIGHT702\APR_MRPT_ |
| APR_MRPT_DATA_02 | 58M | 83M | 108M | F:\ARGUSSAFETY\INSIGHT702\APR_MRPT_ |

17. Complete the Tablespace Creation screen as follows:

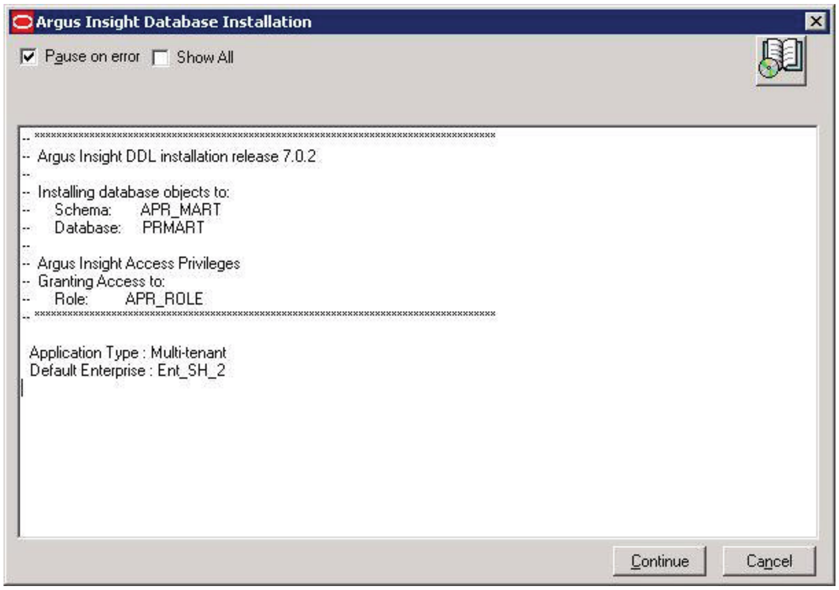
    a. In the **Enter Database Server Directory where all Data Files will be Created** field, enter the complete path to the directory for the tablespace data files that will be used by Argus Insight. For example, /u01/app/oracle/SMTEST. Note that the directory you specify must already exist.

    b. Click **Generate DataFile Path and Name.** The system automatically fills in the Complete Path and Datafile column for all tablespaces.

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

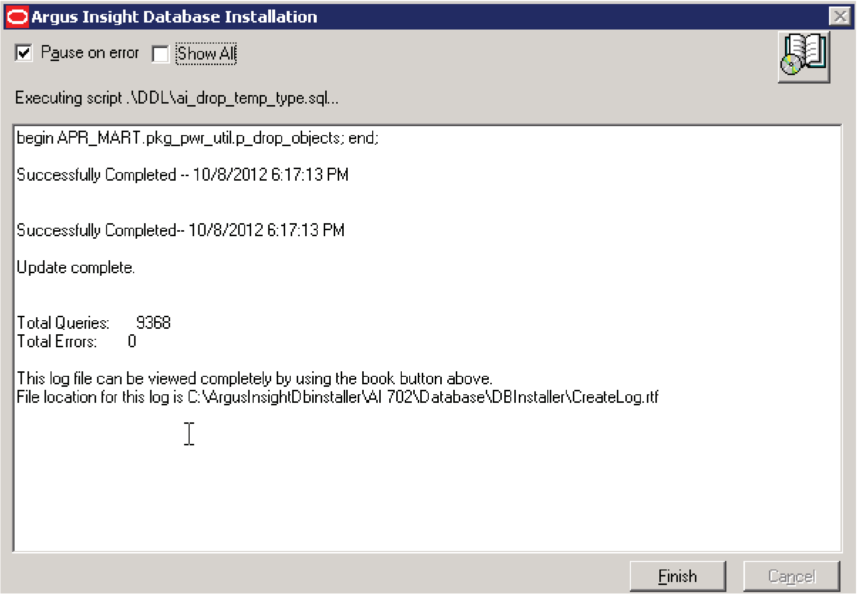
18. Click **Create Tablespace** to create all tablespaces.

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 7.0.2
--
-- 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 : Ent_SH_2
```

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.



```
Executing script .\DDL\ai_drop_temp_type.sql...
```

```
begin APR_MART.pkg_pwr_util.p_drop_objects; end;

Successfully Completed -- 10/8/2012 6:17:13 PM


Successfully Completed-- 10/8/2012 6:17:13 PM

Update complete.


Total Queries:     9368
Total Errors:      0

This log file can be viewed completely by using the book button above.
File location for this log is C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\CreateLog.rtf
```

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:

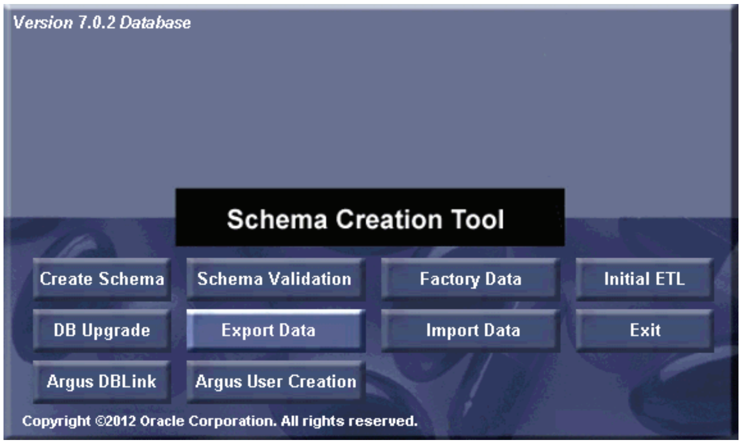
    *drive:*\Argus_Insight_Working\AI702\Database\DBInstaller\CreateLog.rtf

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

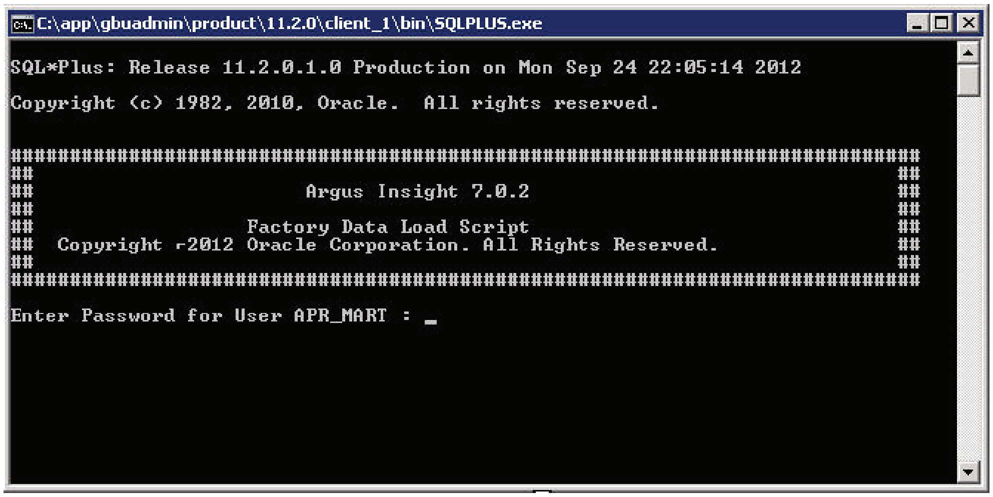
### 3.5.4 Loading Factory Data

To load the factory data:

1. Start the Argus Insight Schema Creation Tool.

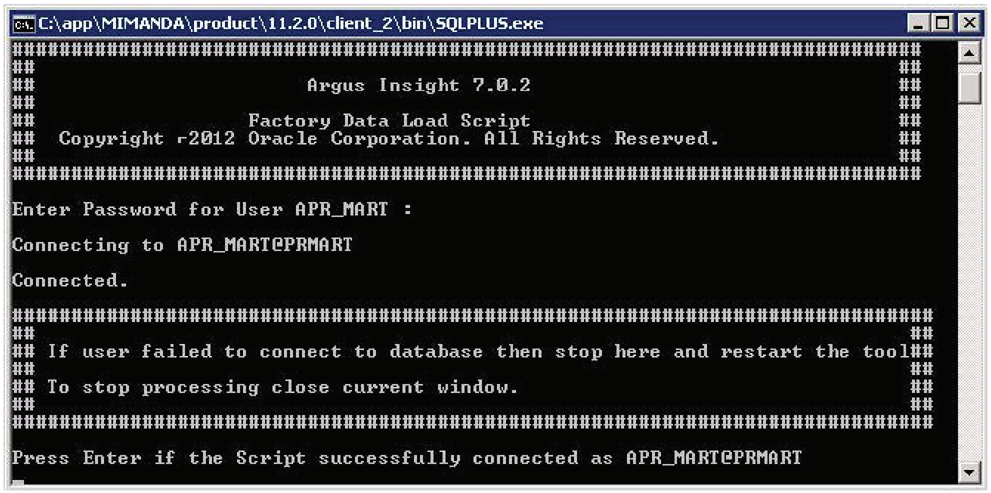


2. Click **Factory Data** to load the factory data. This displays the command screen, as shown in the following figure:



```
SQL*Plus: Release 11.2.0.1.0 Production on Mon Sep 24 22:05:14 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                       Argus Insight 7.0.2                                ##
##                                                                          ##
##                  Factory Data Load Script                                ##
##  Copyright r2012 Oracle Corporation. All Rights Reserved.                ##
##                                                                          ##
##############################################################################

Enter Password for User APR_MART : _
```

3. Enter the password for the **APR_MART** User and press **Enter**. This displays the following command screen:

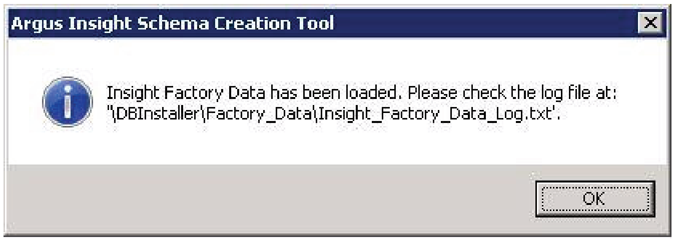


```
##############################################################################
##                                                                          ##
##                       Argus Insight 7.0.2                                ##
##                                                                          ##
##                  Factory Data Load Script                                ##
##  Copyright r2012 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**. This again displays the command screen with the row creation messages displayed multiple times along

with the  name and location of the log file. The name of the log file that is displayed is **insight_factory_data_log.txt**.

5. Press **Enter** again. Argus Insight displays the following message when it finishes loading the factory data:



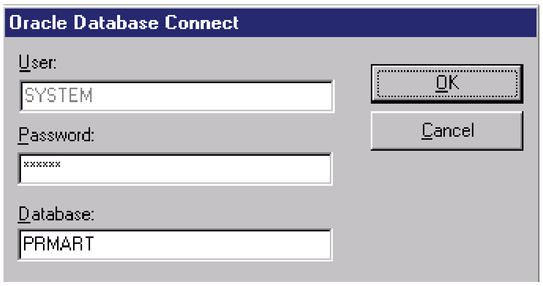
Insight Factory Data has been loaded. Please check the log file at: '\DBInstaller\Factory_Data\Insight_Factory_Data_Log.txt'.

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 opens.

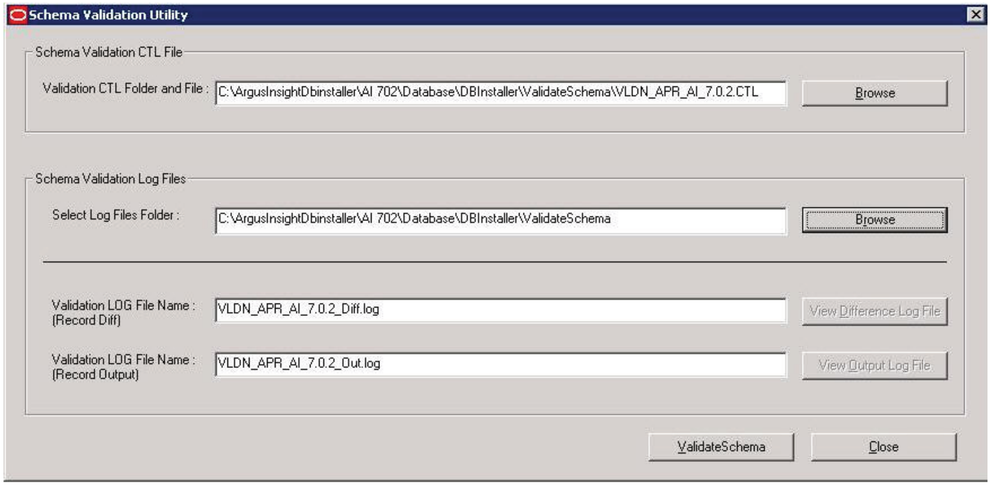


User: SYSTEM

Password: ******

Database: PRMART

3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the SYSTEM user.
   b. In the **Database** field, type the name of the Argus Insight Data Mart instance.
   c. Click **OK.** The **Schema Validation Utility** dialog box opens.


Schema Validation Utility
Schema Validation CTL File
Browse
Schema Validation Log Files
Browse
View Difference Log File
View Output Log File
ValidateSchema
Close

Validation CTL Folder and File : C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\ValidateSchema\VLDN_APR_AI_7.0.2.CTL

Select Log Files Folder : C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\ValidateSchema

Validation LOG File Name : (Record Diff) VLDN_APR_AI_7.0.2_Diff.log

Validation LOG File Name : (Record Output) VLDN_APR_AI_7.0.2_Out.log

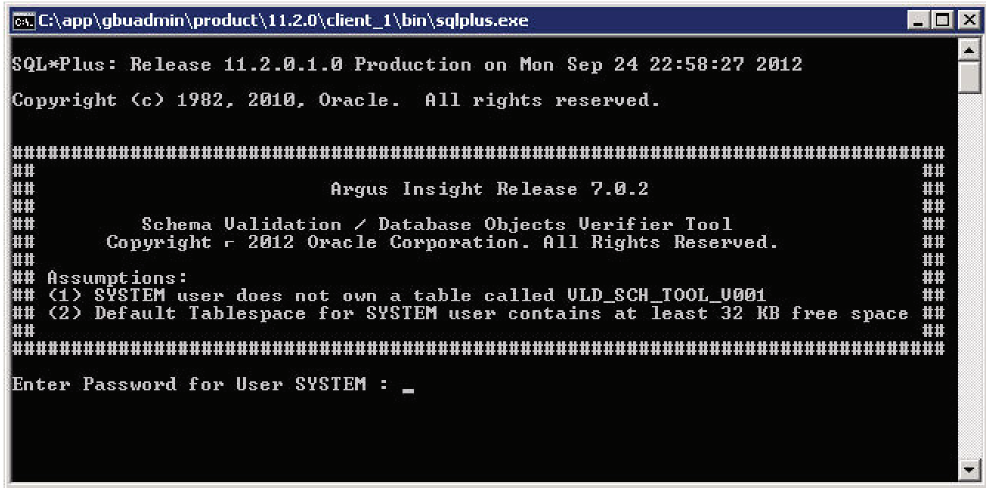
4. Complete the Schema Validation Utility dialog box as follows:

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.** The system returns 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.

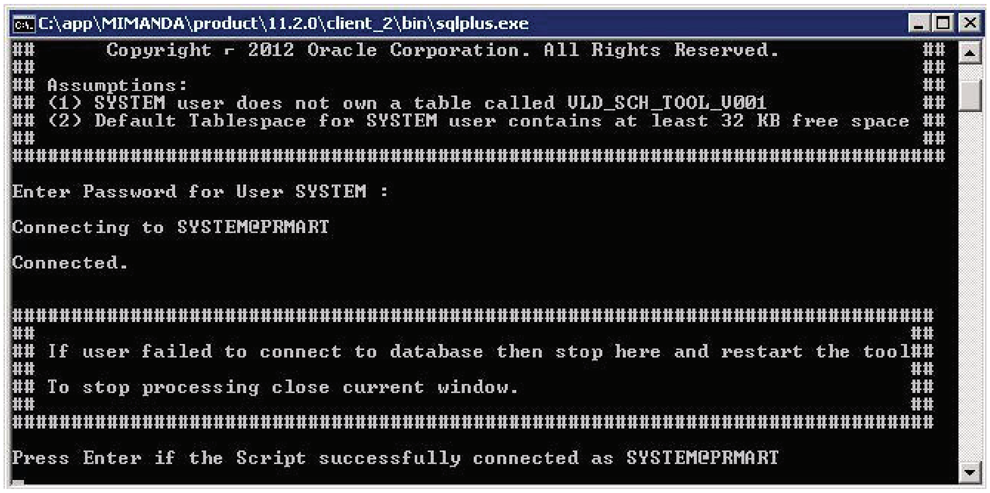
Note that the system automatically inserts the default file names into the Validation LOG File Name (Record Diff) and Validation LOG File Name (Record Output) fields. You can change the log file names if you want.

5. Click **Validate Schema.** This displays the following command screen:



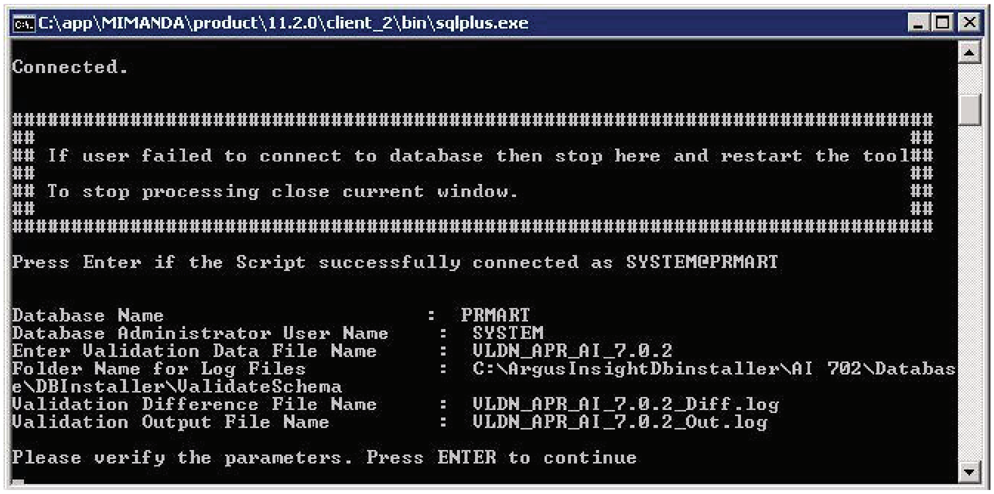
```
SQL*Plus: Release 11.2.0.1.0 Production on Mon Sep 24 22:58:27 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


###############################################################################
##                                                                           ##
##                         Argus Insight Release 7.0.2                       ##
##                                                                           ##
##         Schema Validation / Database Objects Verifier Tool                ##
##      Copyright r 2012 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 **SYSTEM** user and press **Enter**. This displays the following command screen:



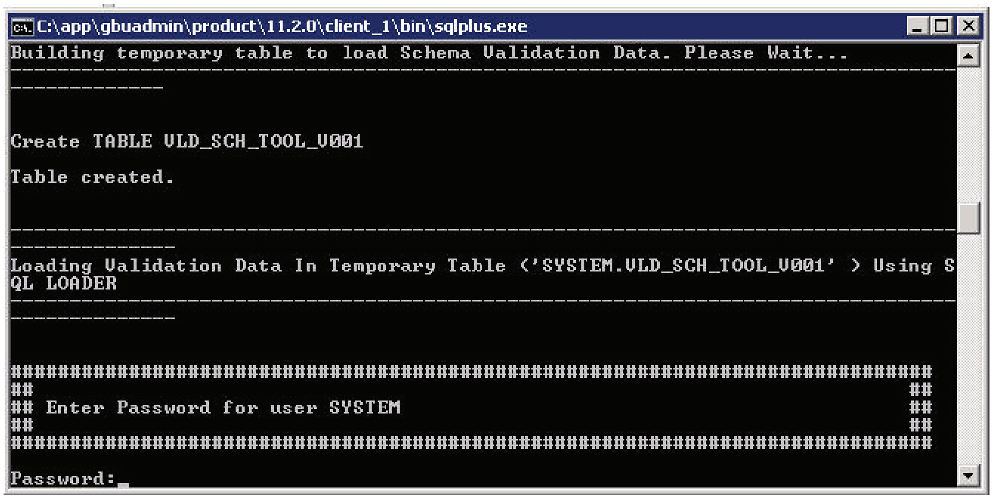
```
##      Copyright r 2012 Oracle Corporation. All Rights Reserved.            ##
##                                                                           ##
## Assumptions:                                                              ##
## (1) SYSTEM user does not own a table called VLD_SCH_TOOL_V001             ##
## (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 User Name>@<Argus Insight Database Name> and press **Enter**. This displays the screen that confirms the Database Name, Database Administrator User Name, Validation File Name, and the Folder Name for Log Files as shown in the following figure:



```
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_7.0.2
Folder Name for Log Files                :  C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller\ValidateSchema
Validation Difference File Name          :  VLDN_APR_AI_7.0.2_Diff.log
Validation Output File Name              :  VLDN_APR_AI_7.0.2_Out.log

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

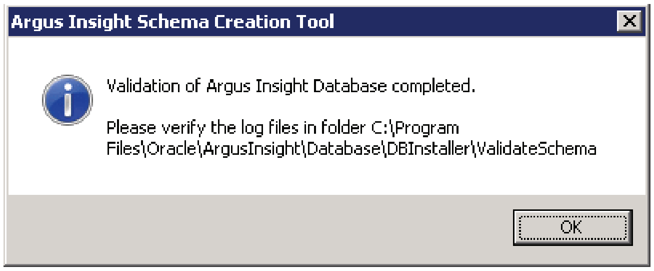
8. Review the information on the command screen and press **Enter.** This displays the following command screen:



```
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 SYSTEM user and press **Enter**.

10. Press **Enter** again on the next displayed screen. This displays a message that the validation of the Argus Insight Database is completed:



Validation of Argus Insight Database completed.

Please verify the log files in folder C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\ValidateSchema

11. Click **OK.**

When the system returns to the Schema Validation Utility dialog box, you can:

- Click **View Difference Log File** to check for any schema discrepancies, such as missing objects.

- Click **View Output Log File** to see the list of errors, if any, that occurred during schema validation.
- Click **Close** to close the dialog box.

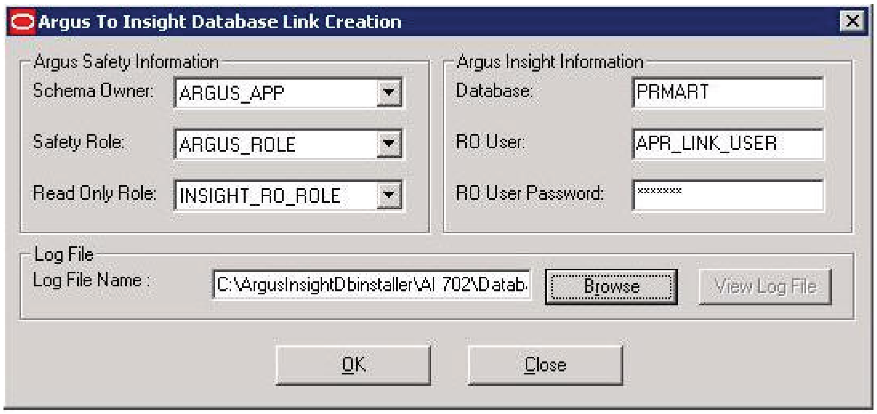
## 3.7 Creating a Database Link from Argus Safety to Insight Database

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, type the password for the SYSTEM user.
   b. In the **Argus Safety Database** field, type the name of your Argus Safety database.
   c. Click **OK.**

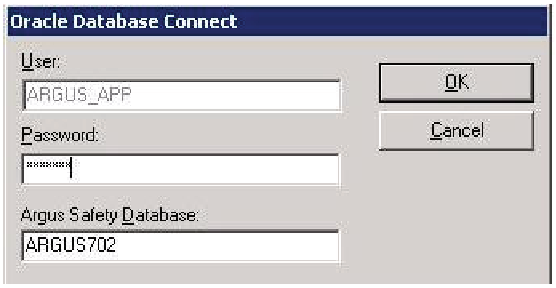
   The Argus To Insight Database Link Creation dialog box opens.


Argus To Insight Database Link Creation
Argus Safety Information
Argus Insight Information
Log File
Browse
View Log File
OK
Close

Schema Owner: ARGUS_APP
Safety Role: ARGUS_ROLE
Read Only Role: INSIGHT_RO_ROLE
Database: PRMART
RO User: APR_LINK_USER
RO User Password: *******
Log File Name : C:\ArgusInsightDbinstaller\AI 702\Datab

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

7. Click **OK** to create the database link. The system first prompts for the information required to connect to the database as the **ARGUS_APP** user.



User: ARGUS_APP

Password: *******

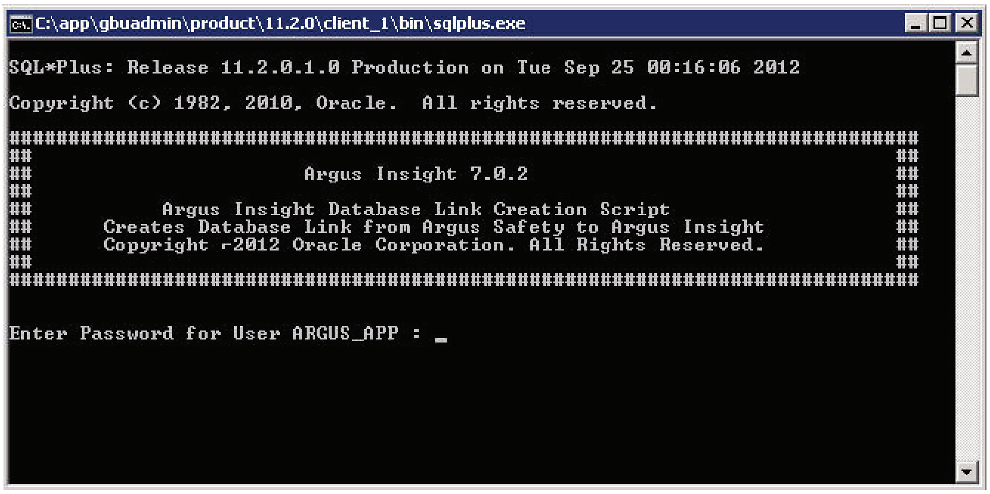
Argus Safety Database: ARGUS702

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

   The system then prompts for the information to connect to the database as the SYSTEM user.

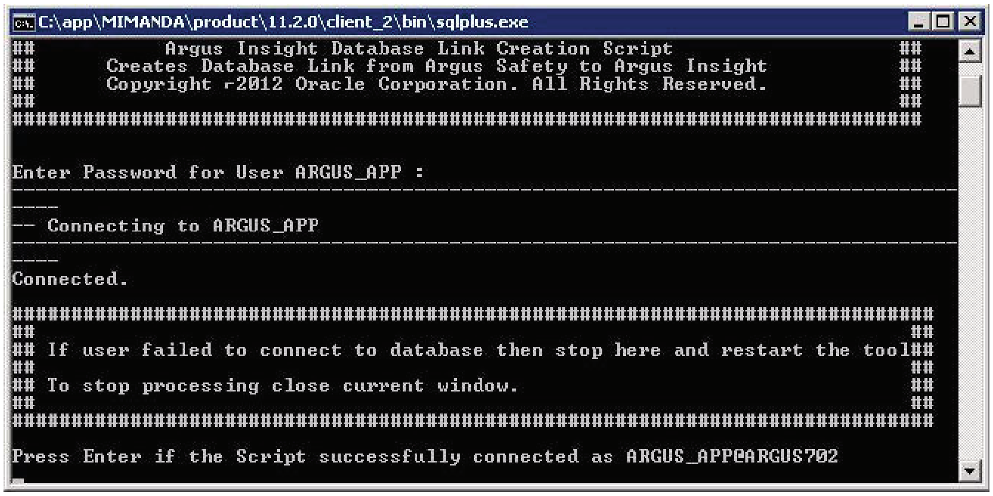
9. Enter the password for the SYSTEM user and click **OK.**

   The system displays the following screen:



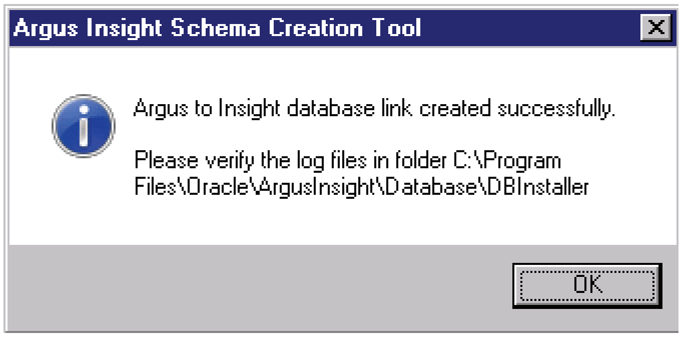
```
SQL*Plus: Release 11.2.0.1.0 Production on Tue Sep 25 00:16:06 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

#############################################################################
##                                                                         ##
##                         Argus Insight 7.0.2                             ##
##                                                                         ##
##               Argus Insight Database Link Creation Script               ##
##        Creates Database Link from Argus Safety to Argus Insight         ##
##        Copyright r2012 Oracle Corporation. All Rights Reserved.         ##
##                                                                         ##
#############################################################################


Enter Password for User ARGUS_APP : _
```

10. Enter the password for the **ARGUS_APP** user and press **Enter**. This displays the following command screen:



```
##               Argus Insight Database Link Creation Script               ##
##        Creates Database Link from Argus Safety to Argus Insight         ##
##        Copyright r2012 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@ARGUS702
_
```

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 the system reports that the Argus to Insight database link was created successfully:



Argus to Insight database link created successfully.

Please verify the log files in folder C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller

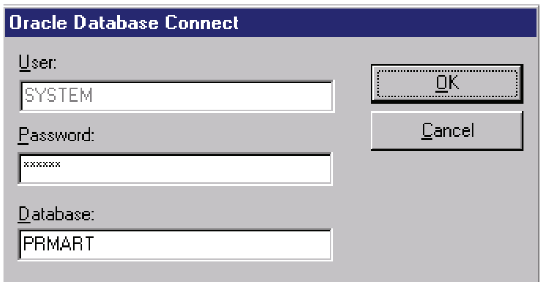
13. Click **OK.**
14. Check the log files located in the following folder for status information:

    *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 7.0.1 to Argus Insight 7.0.2

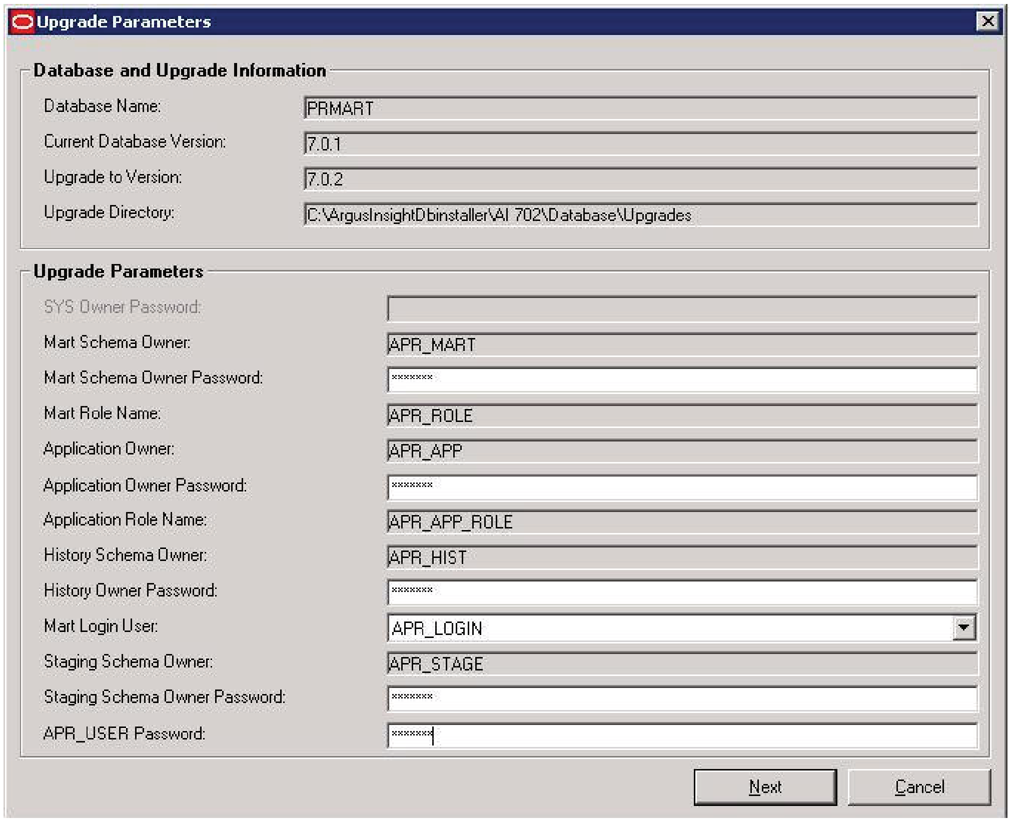
To upgrade the database from Argus Insight 7.0.1 to Argus Insight 7.0.2:

1. Start the Argus Insight Schema Creation Tool.
2. Click **DB Upgrade.** The Oracle Database Connect dialog box opens.



User: SYSTEM
Password: ******
Database: PRMART

3. Connect to the Oracle Database:
    a. In the **Password** field, type the password for the SYSTEM user.
    b. In the **Database** field, type the name of your Argus Insight database.
    c. Click **OK.** The Upgrade Parameters dialog box opens.



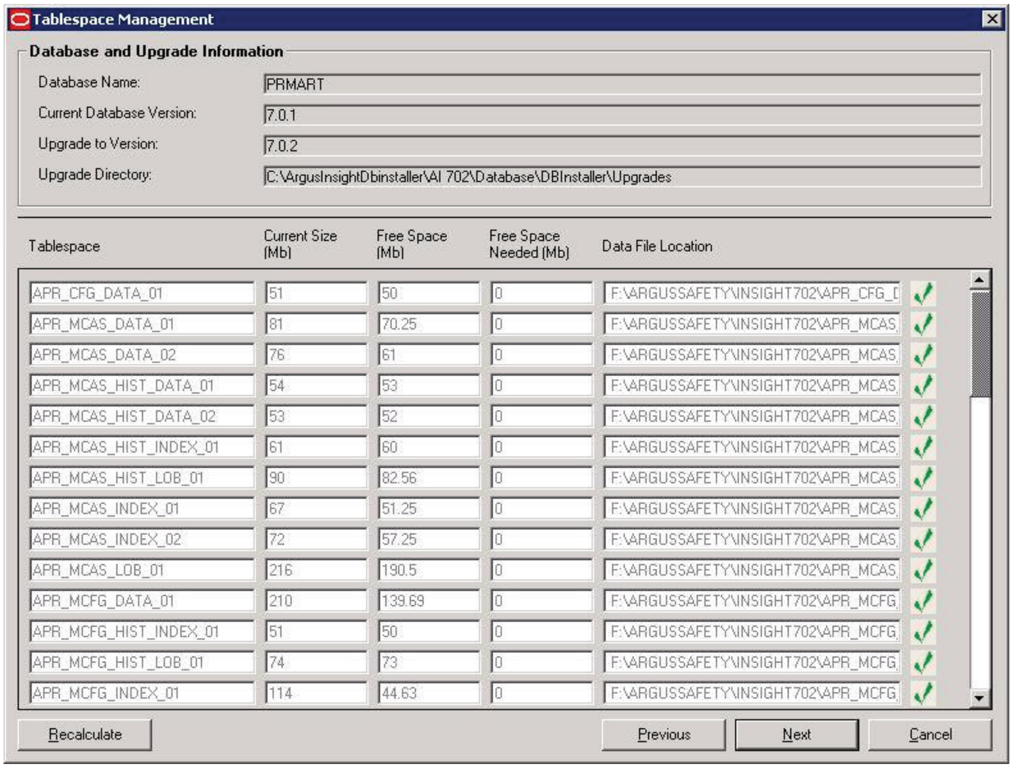
Database and Upgrade Information

Database Name: PRMART
Current Database Version: 7.0.1
Upgrade to Version: 7.0.2
Upgrade Directory: C:\ArgusInsightDbinstaller\AI 702\Database\Upgrades

Upgrade Parameters

SYS Owner 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_LOGIN
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 opens.



Database Name: PRMART
Current Database Version: 7.0.1
Upgrade to Version: 7.0.2
Upgrade Directory: C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\Upgrades

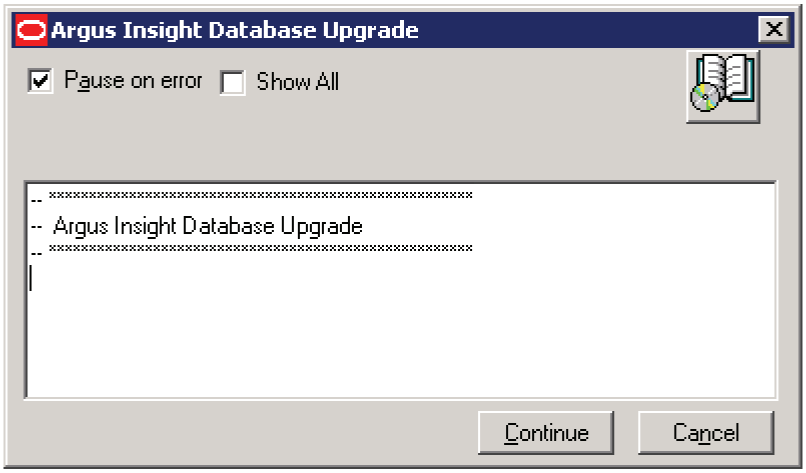
| Tablespace | Current Size (Mb) | Free Space (Mb) | Free Space Needed (Mb) | Data File Location | |
|---|---|---|---|---|---|
| APR_CFG_DATA_01 | 51 | 50 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_CFG_ | ✓ |
| APR_MCAS_DATA_01 | 81 | 70.25 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_DATA_02 | 76 | 61 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_HIST_DATA_01 | 54 | 53 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_HIST_DATA_02 | 53 | 52 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_HIST_INDEX_01 | 61 | 60 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_HIST_LOB_01 | 90 | 82.56 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_INDEX_01 | 67 | 51.25 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_INDEX_02 | 72 | 57.25 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCAS_LOB_01 | 216 | 190.5 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCAS | ✓ |
| APR_MCFG_DATA_01 | 210 | 139.69 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG | ✓ |
| APR_MCFG_HIST_INDEX_01 | 51 | 50 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG | ✓ |
| APR_MCFG_HIST_LOB_01 | 74 | 73 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG | ✓ |
| APR_MCFG_INDEX_01 | 114 | 44.63 | 0 | F:\ARGUSSAFETY\INSIGHT702\APR_MCFG | ✓ |

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, click the **Add** button corresponding to the tablespace name to increase the size.

7. Click **Next.**

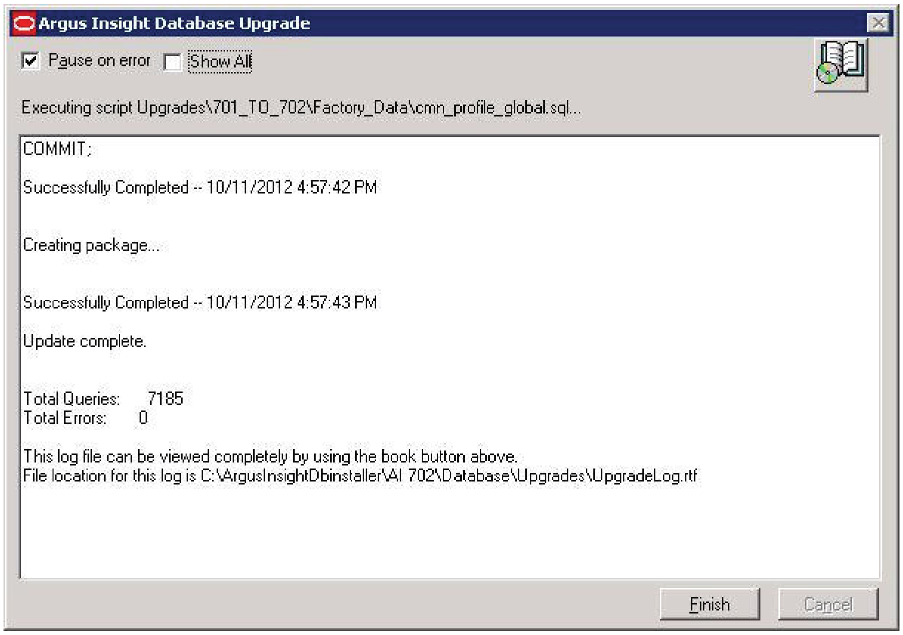


☑ Pause on error ☐ Show All

```
-- ************************************************************
-- Argus Insight Database Upgrade
-- ************************************************************
```

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.



Executing script Upgrades\701_TO_702\Factory_Data\cmn_profile_global.sql...

```
COMMIT;

Successfully Completed -- 10/11/2012 4:57:42 PM


Creating package...


Successfully Completed -- 10/11/2012 4:57:43 PM

Update complete.


Total Queries:    7185
Total Errors:     0

This log file can be viewed completely by using the book button above.
File location for this log is C:\ArgusInsightDbinstaller\AI 702\Database\Upgrades\UpgradeLog.rtf
```

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** to close the dialog box.

12. Once you have upgraded the database from Argus Insight 7.0.1 to Argus Insight 7.0.2, you must 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.

# 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:

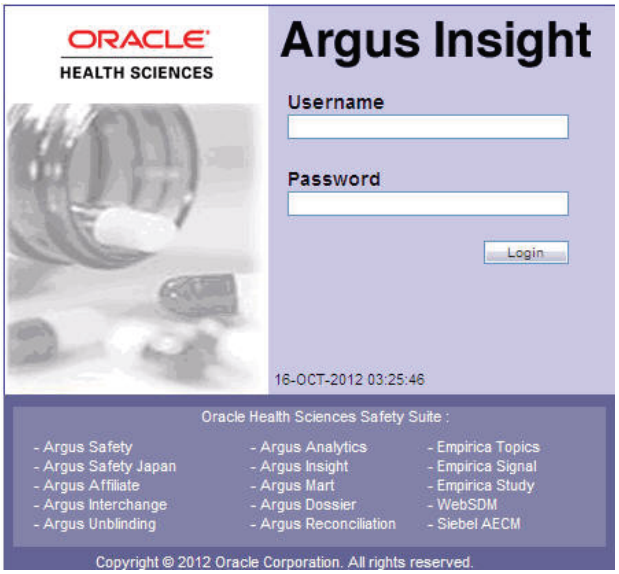
## 4.1 Logging In to Argus Insight for Configuration and Setup

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. Start the Argus Insight application by typing the following URL in the Address bar:

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

4. Press **Enter.** The Argus Insight Login screen opens.



5. Log in to the Argus Insight application:
   a. In the **User Name** field, type **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 all the 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 be able to run the initial ETL.

For detailed information about all the profile switches, see the following documents:

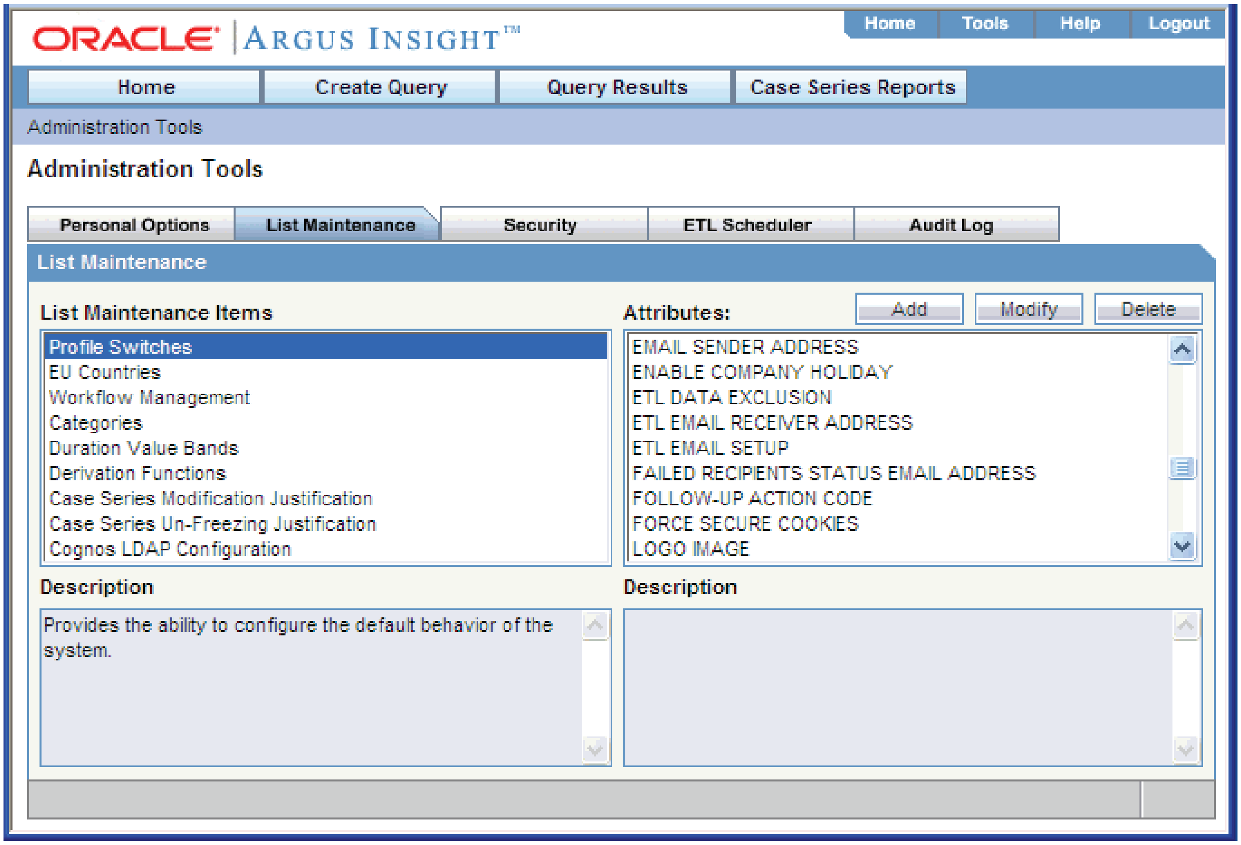
- *Oracle Argus Insight CMN Profile Enterprise Table Guide* (CMN_PROFILE_ENTERPRISE.pdf)
- *Oracle Argus Insight CMN Profile Global Table Guide* (CMN_PROFILE_GLOBAL.pdf)

### 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. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
3. Click the **List Maintenance** tab.
4. Select **Profile Switches** from the List Maintenance Items group. The system updates the Attributes group with the profile switches that you can 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
- Cognos LDAP Configuration

Attributes:

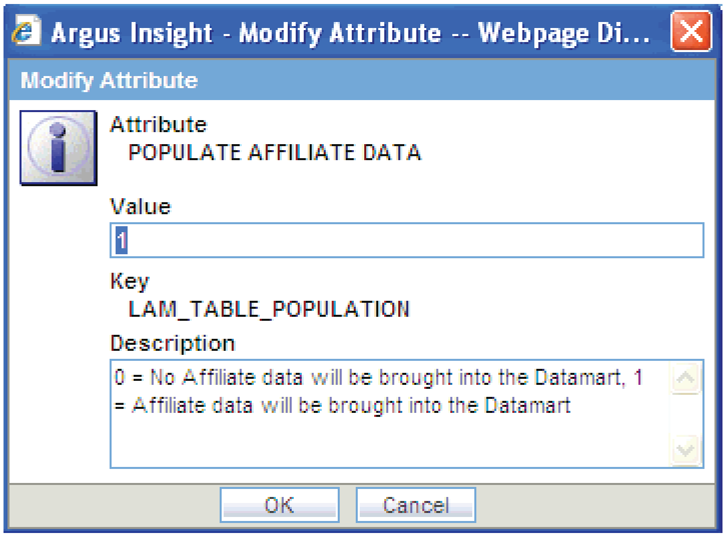
- EMAIL SENDER ADDRESS
- ENABLE COMPANY HOLIDAY
- ETL DATA EXCLUSION
- ETL EMAIL RECEIVER ADDRESS
- ETL EMAIL SETUP
- FAILED RECIPIENTS STATUS EMAIL ADDRESS
- FOLLOW-UP ACTION CODE
- FORCE SECURE COOKIES
- LOGO IMAGE

Description: Provides the ability to configure the default behavior of the system.

### 4.2.2 Setting the Populate Data Attributes

To set the data attributes:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **POPULATE AFFILIATE DATA** from the Attributes group.
    a. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
POPULATE AFFILIATE DATA

Value
1

Key
LAM_TABLE_POPULATION

Description
0 = No Affiliate data will be brought into the Datamart, 1 = Affiliate data will be brought into the Datamart

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

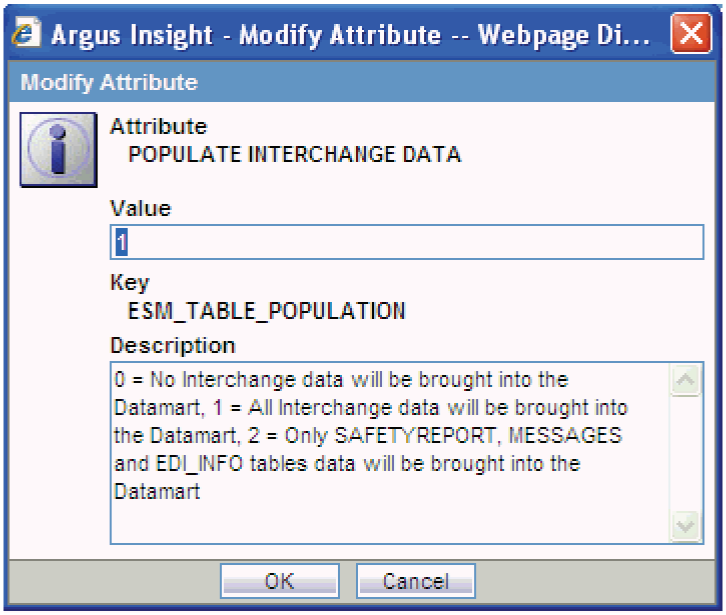
0 = Do not bring any affiliate data into the data mart.

1 = Bring all affiliate data into the data mart.

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

4. Select **POPULATE INTERCHANGE DATA** from the Attributes group.

a. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
POPULATE INTERCHANGE DATA

Value
1

Key
ESM_TABLE_POPULATION

Description
0 = No Interchange data will be brought into the Datamart, 1 = All Interchange data will be brought into the Datamart, 2 = Only SAFETYREPORT, MESSAGES and EDI_INFO tables data will be brought into the Datamart

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

0 = Do not bring any interchange data into the data mart.

1 = Bring all interchange data into the data mart.

2 = Bring only the SAFETYREPORT, MESSAGES, and EDI_INFO tables data into the data mart.

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

5. Select **POPULATE NARRATIVE LANGUAGES TABLE** from the Attributes group.

   a. Click **Modify.**

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

      0 = Do not populate the RPT_CNL_MLINGUAL and RPT_CNL_ENGLISH tables.

      1 = Populate the RPT_CNL_MLINGUAL and RPT_CNL_ENGLISH tables. Argus Insight uses the information in these tables in the following reports:

      - Case Narrative Listing - English
      - Serious Adverse Events Report (for BusinessObjects only)

      Set this value to 1 only if you these reports.

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

### 4.2.3 Setting the Email Attributes

The following attributes relate to sending and receiving email after an extract, transform, and load (ETL) operation has completed, as well as sending email for scheduled reports.

- ETL EMAIL SETUP
- ETL EMAIL RECEIVER ADDRESS
- EMAIL SENDER ADDRESS
- FAILED RECIPIENTS STATUS EMAIL ADDRESS
- MAX EMAIL SIZE

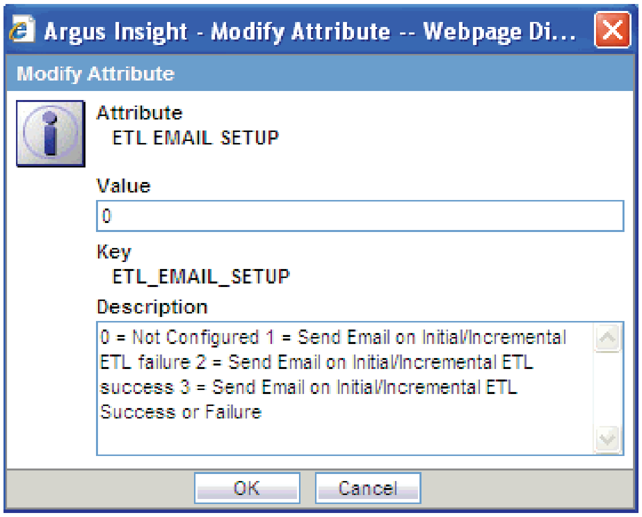
**Note:** In previous releases, the three attributes for report scheduling (that is, EMAIL SENDER ADDRESS, FAILED RECIPIENTS STATUS EMAIL ADDRESS, and MAX EMAIL SIZE) were part of the Mailconfig.xml file. Beginning with Argus Insight 7.0, these attributes were moved to the List Maintenance section.

To configure the attributes related to email messages and delivery:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Define whether to send email following the failure or success of an extract, transform, and load (ETL) operation.

   a. Select **ETL EMAIL SETUP** from the Attributes group.

   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
ETL EMAIL SETUP

Value
0

Key
ETL_EMAIL_SETUP

Description
0 = Not Configured 1 = Send Email on Initial/Incremental ETL failure 2 = Send Email on Initial/Incremental ETL success 3 = Send Email on Initial/Incremental ETL Success or Failure

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

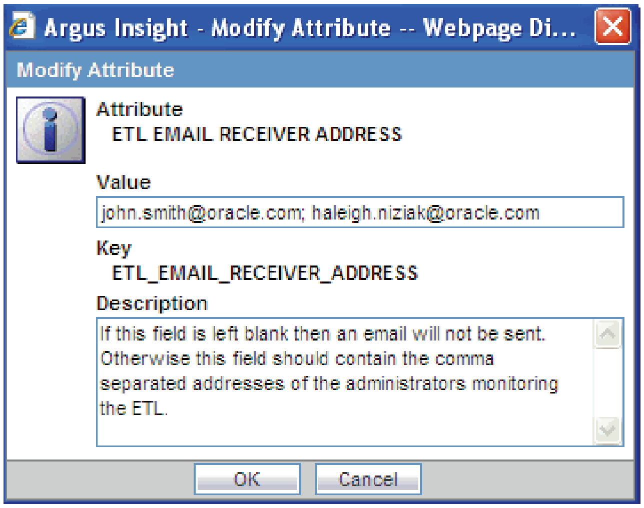
0 = Send no email message after an ETL operation.
1 = Send an email message only if an initial or incremental ETL fails.
2 = Send an email message only if an initial or incremental ETL succeeds.
3 = Send an email message after any initial or incremental ETL (failure or success).

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

4. Specify the email address of each administrator who should receive email status messages of the ETL process.

   a. Select **ETL EMAIL RECEIVER ADDRESS** from the Attributes group.

   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
ETL EMAIL RECEIVER ADDRESS

Value
john.smith@oracle.com; haleigh.niziak@oracle.com

Key
ETL_EMAIL_RECEIVER_ADDRESS

Description
If this field is left blank then an email will not be sent. Otherwise this field should contain the comma separated addresses of the administrators monitoring the ETL.

   c. Click the **Value** field, and enter the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry.

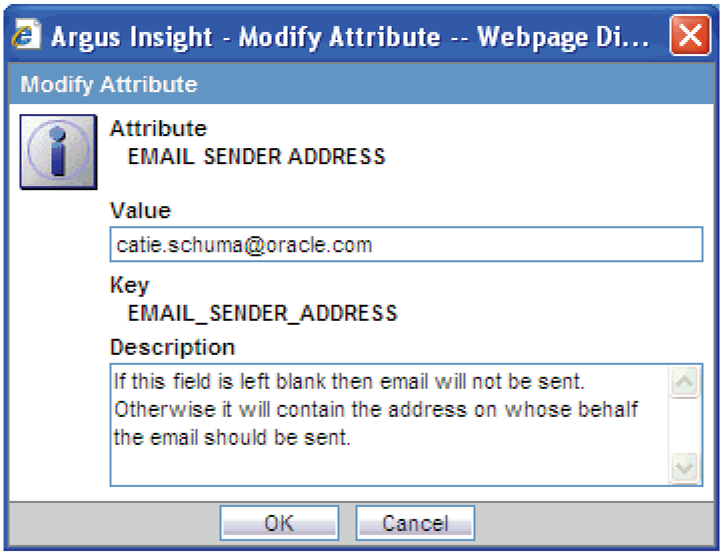
   If you leave the Value field blank, then Argus Insight sends no email messages.

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

5. Specify the email address of the person who will send all the Argus Insight email messages.

   a. Select **EMAIL SENDER ADDRESS** from the Attributes group.

   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
EMAIL SENDER ADDRESS

Value
catie.schuma@oracle.com

Key
EMAIL_SENDER_ADDRESS

Description
If this field is left blank then email will not be sent. Otherwise it will contain the address on whose behalf the email should be sent.

   c. Click the **Value** field, and enter the email address of the person on whose behalf Argus Insight sends all email messages.

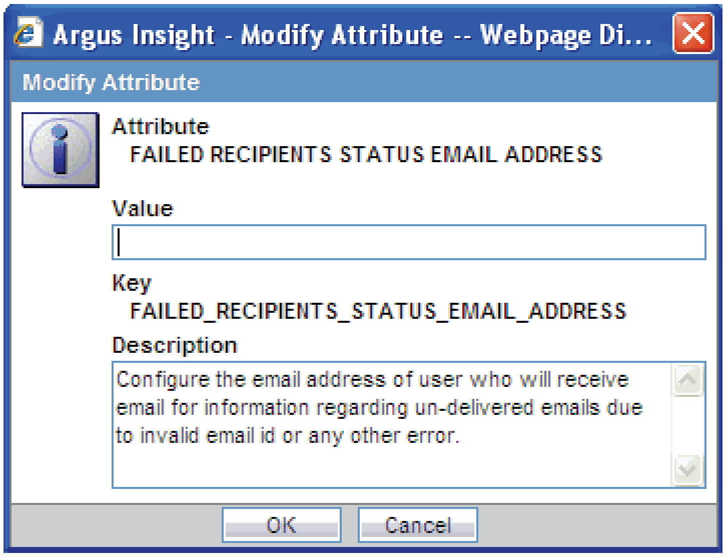
   If you leave the Value field blank, then Argus Insight sends no email messages.

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

6. Specify the email address of the user who will receive information about undeliverable emails:

   a. Select **FAILED RECIPIENTS STATUS EMAIL ADDRESS** from the Attributes group.

   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
FAILED RECIPIENTS STATUS EMAIL ADDRESS

Value

Key
FAILED_RECIPIENTS_STATUS_EMAIL_ADDRESS

Description
Configure the email address of user who will receive email for information regarding un-delivered emails due to invalid email id or any other error.

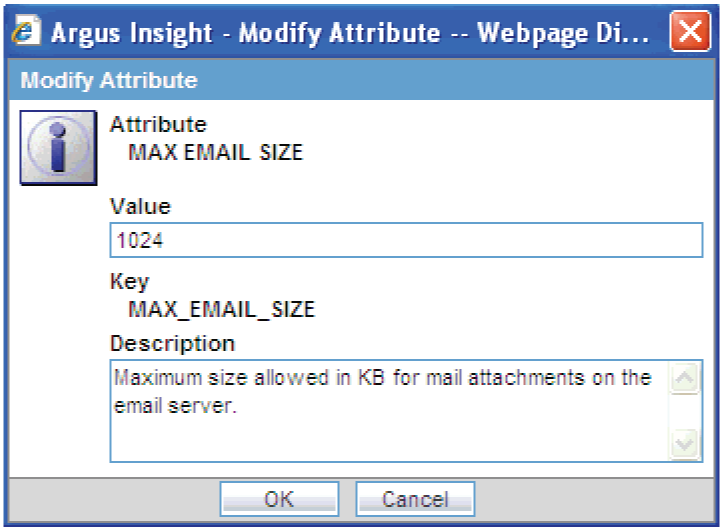
c. Click the **Value** field, and enter the email address of the user who will receive information about undeliverable emails.

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

7. Specify the maximum size of an email message sent from the Argus Insight Web Server:

   a. Select **MAX EMAIL SIZE** from the Attributes group.

   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
MAX EMAIL SIZE

Value
1024

Key
MAX_EMAIL_SIZE

Description
Maximum size allowed in KB for mail attachments on the email server.

   c. Click the **Value** field, and enter a numeric value that defines the maximum attachment size limit (in KB) of the mail server in the organization.

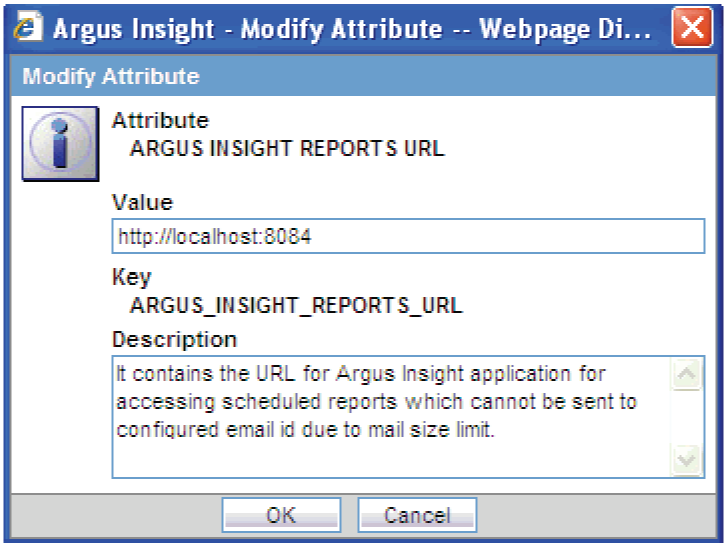
   d. Click **OK** to save your changes and return to the List Maintenance tab.

### 4.2.4 Specifying the URL for Reports Exceeding Mail Size

Depending on the value set in the MAX EMAIL SIZE attribute, some reports may be too large to send by email. For such reports, users can view the reports at a specified URL.

To define the URL where users can access reports that cannot be sent by email:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **ARGUS INSIGHT REPORTS URL** from the Attributes group.
4. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
ARGUS INSIGHT REPORTS URL

Value
http://localhost:8084

Key
ARGUS_INSIGHT_REPORTS_URL

Description
It contains the URL for Argus Insight application for accessing scheduled reports which cannot be sent to configured email id due to mail size limit.

5. Click the **Value** field, and enter the URL for the Argus Insight application for accessing scheduled reports that cannot be sent to the configured email ID, due to mail size limit. For more information on mail size limit, see Section 4.2.3, "Setting the Email Attributes."
6. Click **OK** to save your changes and return to the List Maintenance tab.

## 4.2.5 Specifying the Images for Company Logos

You can specify the image to use for the following logos:

- **LOGO IMAGE.** This image is used in the following reports:

  — CIOMS report

  — CIOMS II Line Listing report

  — US FDA MedWatch 3500A report

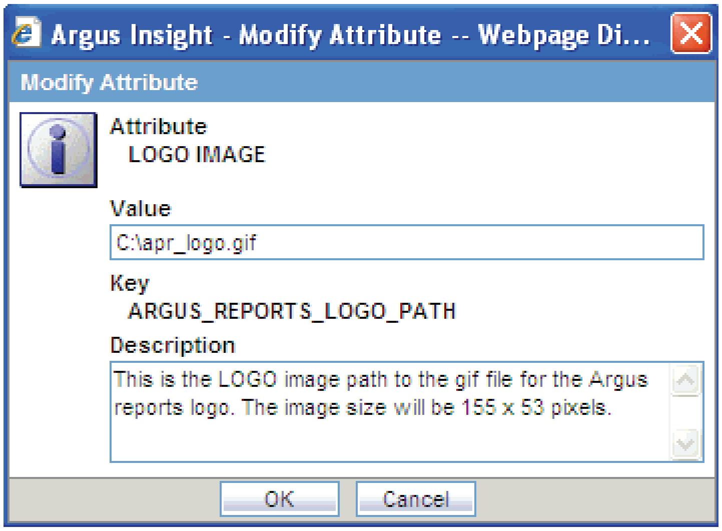
  These reports are called the *Argus Reports*. By default, a logo does not print on these reports.

- **COMPANY LOGO PATH.** This image is used in the header of reports generated using your Business Intelligence tool.

### 4.2.5.1 Specifying the Logo Image for the *Argus Reports*

To specify the image for the logo used in the *Argus Reports:*

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **LOGO IMAGE** from the Attributes group.
4. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
LOGO IMAGE

Value
C:\apr_logo.gif

Key
ARGUS_REPORTS_LOGO_PATH

Description
This is the LOGO image path to the gif file for the Argus reports logo. The image size will be 155 x 53 pixels.

5. Click the **Value** field, and enter the complete path to the GIF image on the Argus Insight Web Server that you want to use as the logo for the Argus Reports. For example:

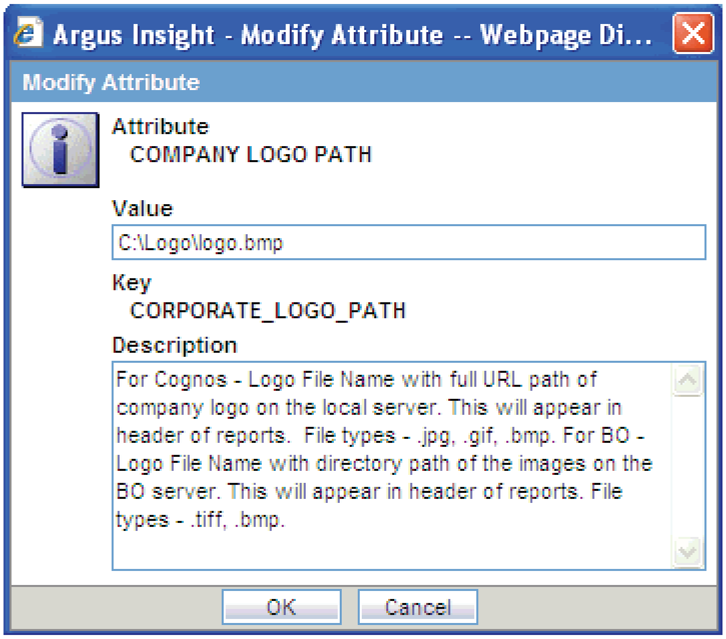
   C:\apr_logo.gif

   To ensure the logo fits in the report layout, the size of the image must be 155 pixels (width) by 53 pixels (height).
6. Click **OK** to save your changes and return to the List Maintenance tab.

#### 4.2.5.2 Specifying the Image for Your Company Logo

To specify the logo image the prints in the header of an Argus Insight report:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **COMPANY LOGO PATH** from the Attributes group.
4. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COMPANY LOGO PATH

Value
C:\Logo\logo.bmp

Key
CORPORATE_LOGO_PATH

Description
For Cognos - Logo File Name with full URL path of company logo on the local server. This will appear in header of reports. File types - .jpg, .gif, .bmp. For BO - Logo File Name with directory path of the images on the BO server. This will appear in header of reports. File types - .tiff, .bmp.

5. Click the **Value** field and enter the image location for your company logo. The specified logo prints in the header of reports.

   - For Cognos, enter the full URL to the location of your company logo on the local server. Cognos supports JPG, GIF, and BMP images. For example:

     ```
     http://argusinsightwebserver:8084/apr_logo.jpg
     ```

   - For BusinessObjects, enter the full directory path to the location of your company logo on the BusinessObjects Server. BusinessObjects supports TIFF and BMP images. For example:

     ```
     C:\Logo\logo.bmp
     ```

   **Note:** The recommendations for the logo image are as follows:

   - The preferred size of the logo file is 10 KB. Because this logo appears on every page of the reports generated in Argus Insight, Oracle recommends that you limit the size of the logo file.
   - The dimensions of the logo should be approximately 300 (width) by 100 (height) pixels to fit in the space provided for the logo in the reports.

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

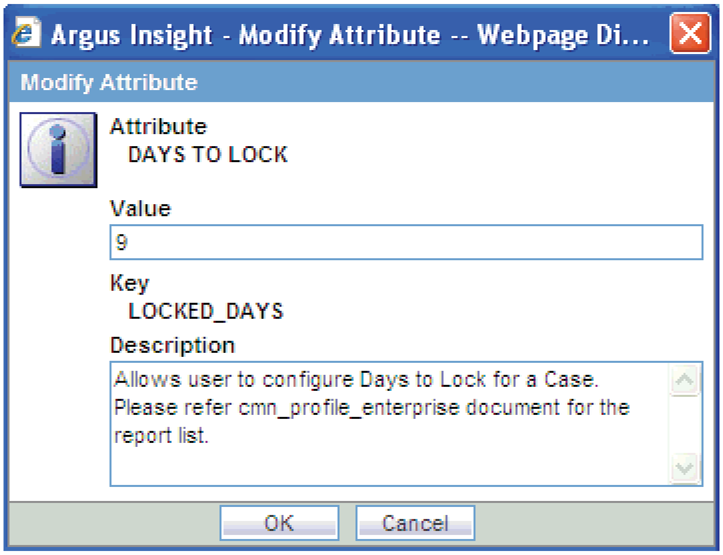
### 4.2.6 Setting the DAYS TO LOCK Attribute

**Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.

This attribute should be configured for all the Workflow related Reports of Management Category.

To define the DAYS TO LOCK attribute:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **DAYS TO LOCK** from the Attributes group.
4. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
DAYS TO LOCK

Value
9

Key
LOCKED_DAYS

Description
Allows user to configure Days to Lock for a Case. Please refer cmn_profile_enterprise document for the report list.

5. Click the **Value** field, and enter the number of days per your business needs or configuration.
6. Click **OK** to save your changes and return to the List Maintenance tab.

## 4.2.7 Setting the Follow-up Attribute

---

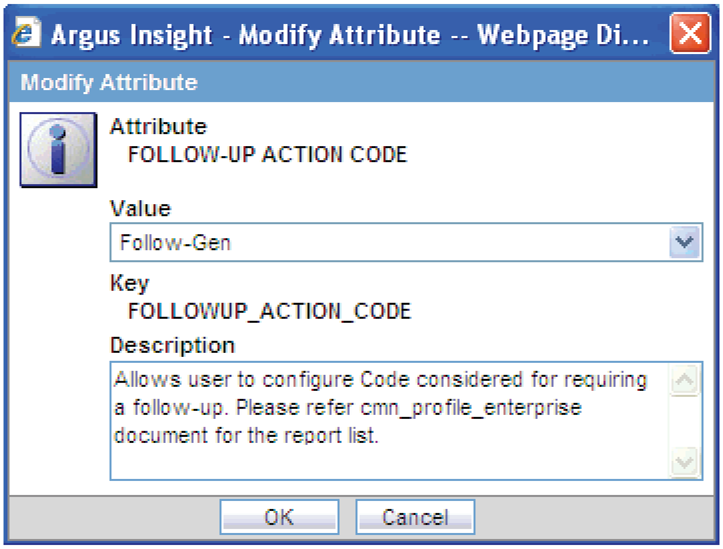
**Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.

This attribute should be configured for the Follow-up Status Listing Report.

---

To define the FOLLOW UP ACTION CODE attribute:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **FOLLOW-UP ACTION CODE** from the Attributes group.
4. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
FOLLOW-UP ACTION CODE

Value
Follow-Gen

Key
FOLLOWUP_ACTION_CODE

Description
Allows user to configure Code considered for requiring a follow-up. Please refer cmn_profile_enterprise document for the report list.

5. Click the **Value** field, and select the appropriate choice for your business needs or configuration.
6. Click **OK** to save your 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 following Cognos-specific attributes:

- COGNOS AUTHENTICATION ENTERPRISE
- COGNOS SERVER
- POPULATE DLL SLL REPORTS TABLE DATA

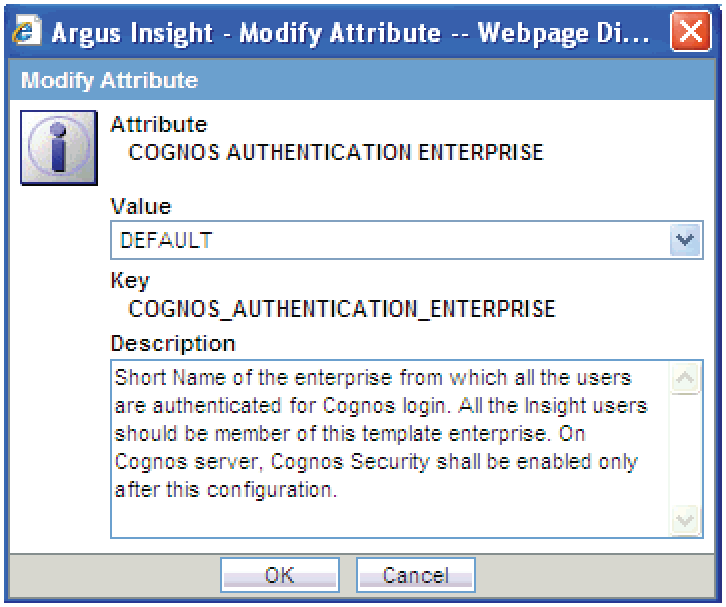
---

**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. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Select **COGNOS AUTHENTICATION ENTERPRISE** from the Attributes group.
   a. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COGNOS AUTHENTICATION ENTERPRISE

Value
DEFAULT

Key
COGNOS_AUTHENTICATION_ENTERPRISE

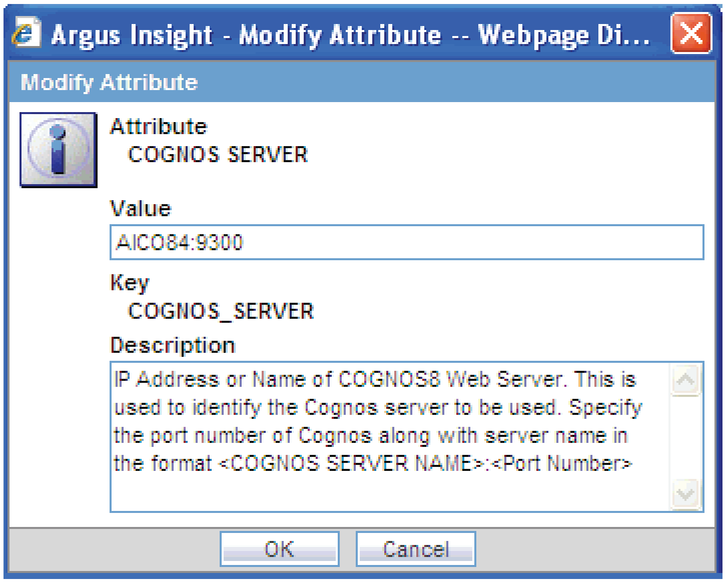
Description
Short Name of the enterprise from which all the users are authenticated for Cognos login. All the Insight users should be member of this template enterprise. On Cognos server, Cognos Security shall be enabled only after this configuration.

   b. Click the **Value** field, and select the Enterprise Short Name from which all users are authenticated for Cognos login.

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

4. Select **COGNOS SERVER** from the Attributes group. Argus Insight uses this attribute to identify which Cognos 8 Web Server to use.

   a. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COGNOS SERVER

Value
AICO84:9300

Key
COGNOS_SERVER

Description
IP Address or Name of COGNOS8 Web Server. This is used to identify the Cognos server to be used. Specify the port number of Cognos along with server name in the format <COGNOS SERVER NAME>:<Port Number>

   b. Click the **Value** field, and enter the name of the Cognos 8 Server and the port number. Use the following format:

   *Cognos8_Server_Name*:*Port_Number*

   For example: srv001:9300

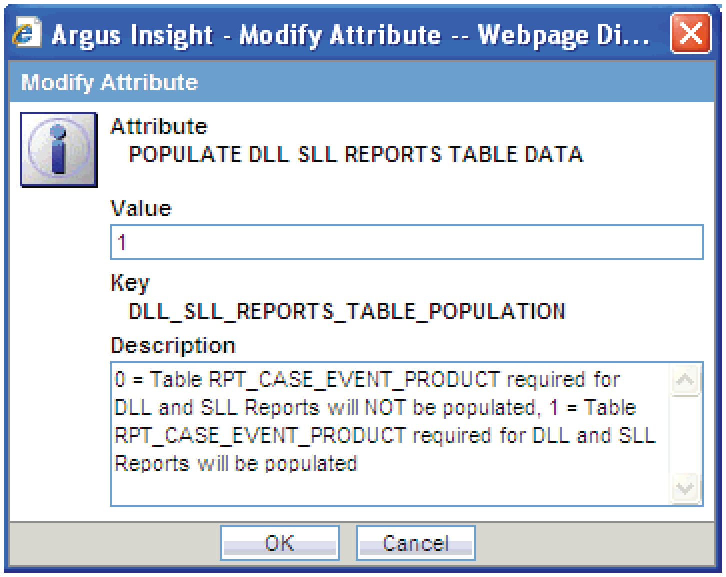
   Port 9300 is the default port for the Cognos 8 application.

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

5. Select **POPULATE DLL SLL REPORTS TABLE DATA** from the Attributes group.

> **Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.
>
> This attribute should be configured for the Detail Line Listing Report and the Simple Line Listing Report.

   a. Click **Modify.** The following Modify Attribute dialog box opens:


Argus Insight - Modify Attribute -- Webpage Di...
Modify Attribute
Attribute
POPULATE DLL SLL REPORTS TABLE DATA
Value
1
Key
DLL_SLL_REPORTS_TABLE_POPULATION
Description
0 = Table RPT_CASE_EVENT_PRODUCT required for DLL and SLL Reports will NOT be populated, 1 = Table RPT_CASE_EVENT_PRODUCT required for DLL and SLL Reports will be populated
OK
Cancel

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

      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

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

## 4.2.9 Setting the Attributes Specific ONLY to BusinessObjects

If you are using BusinessObjects as your Business Intelligence tool with Argus Insight, you need to complete the following tasks to define those attributes that are required for **BusinessObjects configurations only**:

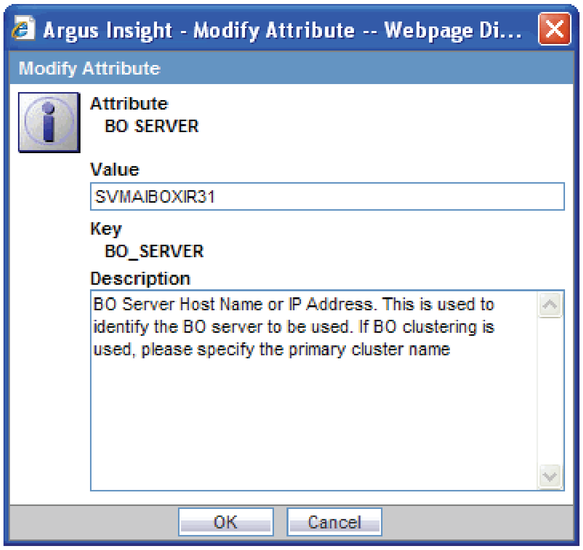
- Setting the Attributes for the BusinessObjects Servers
- Setting the Attributes for the BusinessObjects Users
- Setting the Attributes for BusinessObjects Reports
- Setting the Populating Data Attributes Required for BusinessObjects Only

### 4.2.9.1 Setting the Attributes for the BusinessObjects Servers

To define the attributes required for the BusinessObjects Servers:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.

2. Select **Profile Switches** from the List Maintenance Items group.
3. Define the BusinessObjects Server that Argus Insight uses:
   a. Select **BO SERVER** from the Attributes group.
   b. Click **Modify.**



Attribute
BO SERVER

Value
SVMAIBOXIR31

Key
BO_SERVER

Description
BO Server Host Name or IP Address. This is used to identify the BO server to be used. If BO clustering is used, please specify the primary cluster name

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

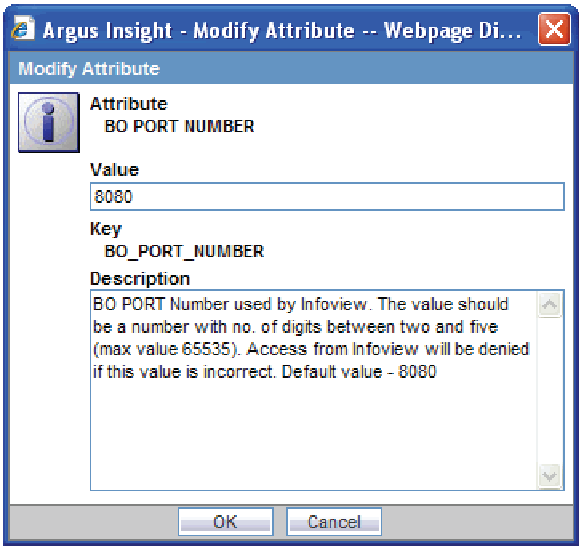
   In addition, specify the cluster name if you are using the BusinessObjects clustering feature.

---

**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 Report Writer. These problems may be caused due to the session interference of Argus Insight and BusinessObjects web application.

---

   d. Click **OK** to save your changes and return to the List Maintenance tab.
4. Define the BusinessObjects port number that InfoView uses:
   a. Select **BO PORT NUMBER** from the Attributes group.
   b. Click **Modify.**



Attribute
BO PORT NUMBER

Value
8080

Key
BO_PORT_NUMBER

Description
BO PORT Number used by Infoview. The value should be a number with no. of digits between two and five (max value 65535). Access from Infoview will be denied if this value is incorrect. Default value - 8080

- **c.** Click the **Value** field, and enter the port number used by InfoView.

  You can enter any whole number from 10 to 65535 for the port number. The default value is 8080.

  ---

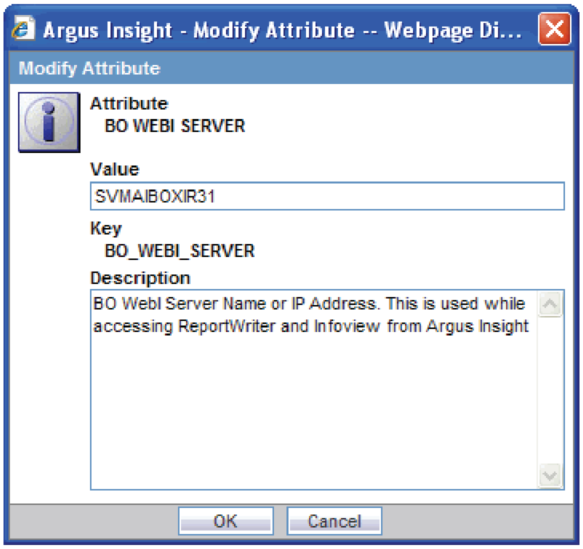
  **Note:** If the port number is incorrect, you will not be able to access InfoView from Argus Insight.

  ---

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

**5.** Define the BusinessObjects WEBI Server that the system uses to access the Report Writer and InfoView from Argus Insight:

- **a.** Select **BO WEBI SERVER** from the Attributes group.
- **b.** Click **Modify.**



Attribute
BO WEBI SERVER

Value
SVMAIBOXIR31

Key
BO_WEBI_SERVER

Description
BO WebI Server Name or IP Address. This is used while accessing ReportWriter and Infoview from Argus Insight

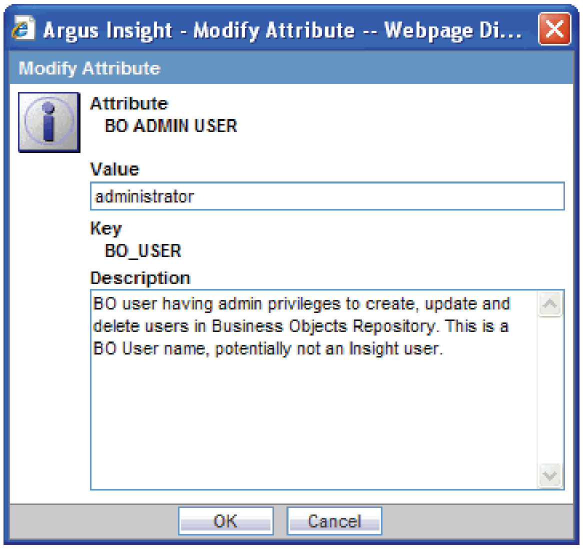
- **c.** Click the **Value** field, and enter either the host name or the IP address of the BusinessObjects WEBI Server. The system uses this value to access the Report Writer and InfoView from Argus Insight.

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

### 4.2.9.2 Setting the Attributes for the BusinessObjects Users

To define the attributes required for the BusinessObjects users:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Define the BusinessObjects administrator user:
   a. Select **BO ADMIN USER** from the Attributes group.
   b. Click **Modify.**



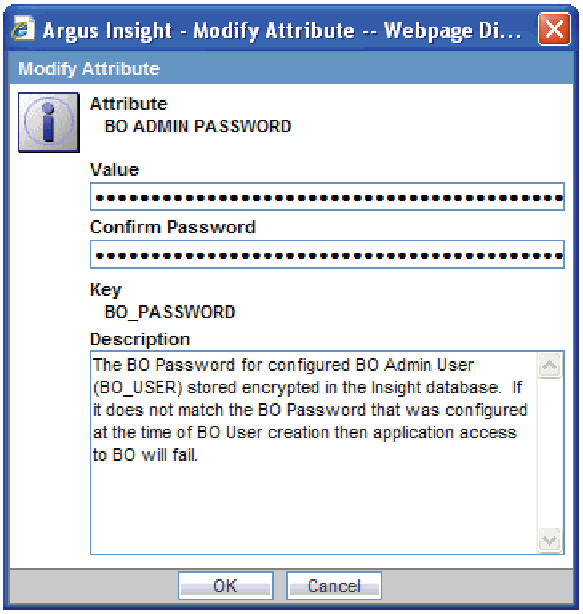
Attribute
BO ADMIN USER

Value
administrator

Key
BO_USER

Description
BO user having admin privileges to create, update and delete users in Business Objects Repository. This is a BO User name, potentially not an Insight user.

   c. Click the **Value** field, and enter the name of the BusinessObjects user that has administrator privileges to create, update, and delete users in the BusinessObjects repository. This user is a BusinessObjects user, but not necessarily an Argus Insight user.
   d. Click **OK** to save your changes and return to the List Maintenance tab.
4. Define the password for the BusinessObjects administrator user:
   a. Select **BO ADMIN PASSWORD** from the Attributes group.
   b. Click **Modify.**



Attribute
BO ADMIN PASSWORD

Value
••••••••••••••••••••••••••••••••••••••••••••

Confirm Password
••••••••••••••••••••••••••••••••••••••••••••

Key
BO_PASSWORD

Description
The BO Password for configured BO Admin User (BO_USER) stored encrypted in the Insight database. If it does not match the BO Password that was configured at the time of BO User creation then application access to BO will fail.

c. Click the **Value** field, and enter the password for the BusinessObjects administrator user (BO ADMIN USER) that you defined in the previous step.

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

---

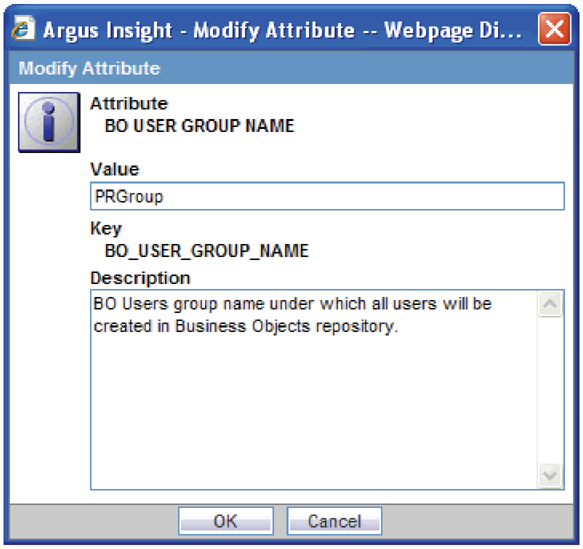
**Note:** Ensure that you update this password whenever you change the password for the BusinessObjects administrator user on the BusinessObjects Server.

---

5. Define a name for the BusinessObjects user group:

a. Select **BO USER GROUP NAME** from the Attributes group.

b. Click **Modify.**



Attribute
BO USER GROUP NAME

Value
PRGroup

Key
BO_USER_GROUP_NAME

Description
BO Users group name under which all users will be created in Business Objects repository.

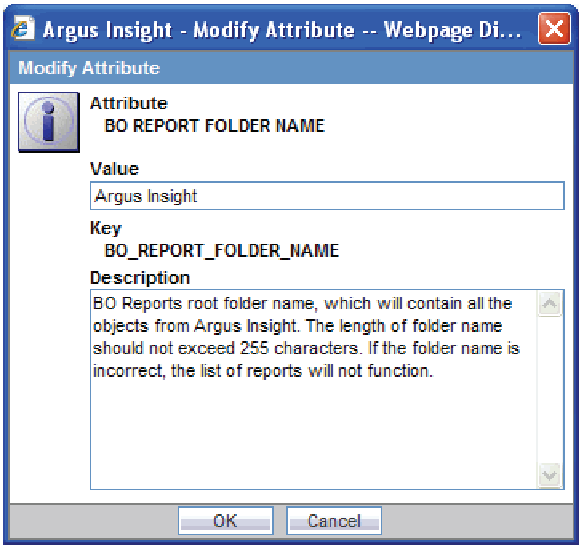
c. Click the **Value** field, and enter a name for the BusinessObjects User Group under which all users will be created in the BusinessObjects repository.

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

### 4.2.9.3 Setting the Attributes for BusinessObjects Reports

To define the attributes related to the reports you use in BusinessObjects:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Define the name for the BusinessObjects report folder:
   a. Select **BO REPORT FOLDER NAME** from the Attributes group.
   b. Click **Modify.**



Attribute
BO REPORT FOLDER NAME

Value
Argus Insight

Key
BO_REPORT_FOLDER_NAME

Description
BO Reports root folder name, which will contain all the objects from Argus Insight. The length of folder name should not exceed 255 characters. If the folder name is incorrect, the list of reports will not function.

   c. Click the **Value** field, and enter a name for the report folder that will contain all the objects from Argus Insight.

   The maximum length of the folder name is 255 characters. If the folder name does not match the name of the BusinessObjects Reports root folder, then the report listing will not be visible in Argus Insight.

   d. Click **OK** to save your changes and return to the List Maintenance tab.
4. Define the column number that contains the supplier name:

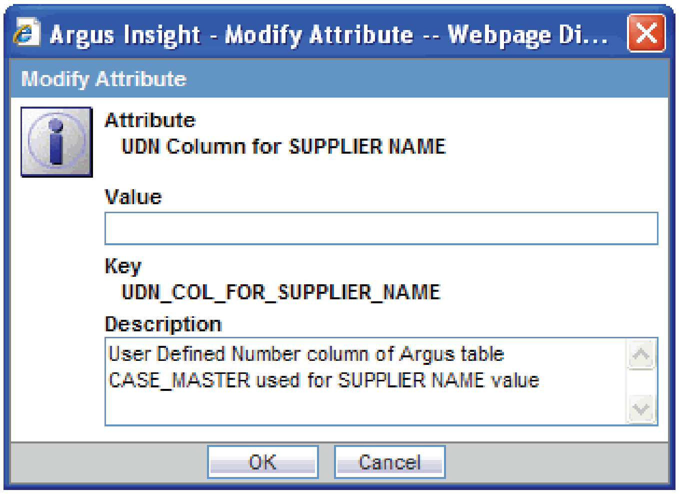
---

**Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.

This attribute should be configured for the Supplier Performance Report.

---

   a. Select **UDN Column for SUPPLIER NAME** from the Attributes group.
   b. Click **Modify.**



Attribute
UDN Column for SUPPLIER NAME

Value

Key
UDN_COL_FOR_SUPPLIER_NAME

Description
User Defined Number column of Argus table CASE_MASTER used for SUPPLIER NAME value

c. Click the **Value** field, and enter the number of the column in the Argus Insight CASE_MASTER table that contains the SUPPLIER NAME value.

---

**Note:** You need to configure the UDN Column for SUPPLIER NAME attribute *only if* you use the Supplier Performance Report.

---

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

5. Define the CASE REFERENCE TYPE ID attribute.

---

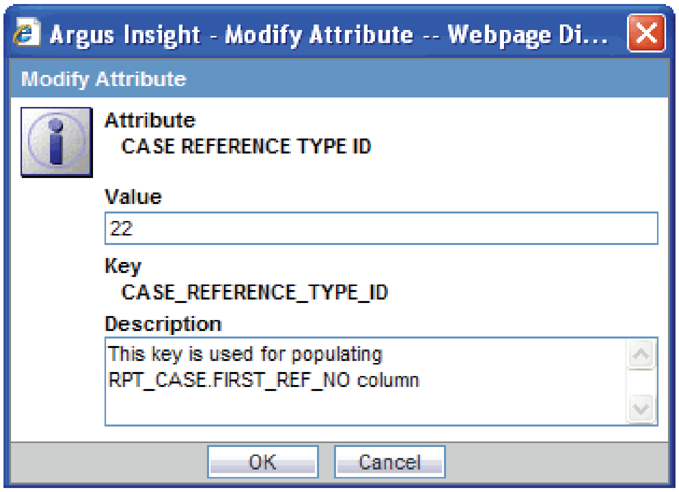
**Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.

This attribute should be configured for the Manufacturing Monthly Report.

---

a. Select **CASE REFERENCE TYPE ID** from the Attributes group.

b. Click **Modify.**



Attribute
CASE REFERENCE TYPE ID

Value
22

Key
CASE_REFERENCE_TYPE_ID

Description
This key is used for populating RPT_CASE.FIRST_REF_NO column

c. Click the **Value** field, and enter the number of your Case Reference Type ID, as per your business requirements. Argus Insight uses this value to populate the RPT_CASE.FIRST_REF_NO column.

> **Note:** You need to configure the CASE REFERENCE TYPE ID attribute *only if* you use the Monthly Manufacturing Report.

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

### 4.2.9.4 Setting the Populating Data Attributes Required for BusinessObjects Only

This section describes how to configure the POPULATE RPT_REG_REPORTS COLUMNS attribute required for BusinessObjects only.

For information about the other populating data attributes that are used by both BusinessObjects and Cognos, see Section 4.2.2, "Setting the Populate Data Attributes."

> **Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.
>
> This attribute should be configured for the Regulatory Submission and Distribution Compliance Report.

To define the POPULATE RPT_REG_REPORTS COLUMNS attribute:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.
3. Define the POPULATE RPT_REG_REPORTS COLUMNS attribute.
    a. Select **POPULATE RPT_REG_REPORTS COLUMNS** from the Attributes group.
    b. Click **Modify.**
    c. Click the **Value** field, and enter one of the following numeric values:

        0 = Do not populate the extra columns of the RPT_REG_REPORTS table.

        1 = Populate the extra columns of the RPT_REG_REPORTS table, which is required by the BusinessObjects version of the Regulatory Submission and Distribution Compliance report. Set this value to 1 only if you use this Argus Insight report and BusinessObjects.

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

## 4.2.10 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:

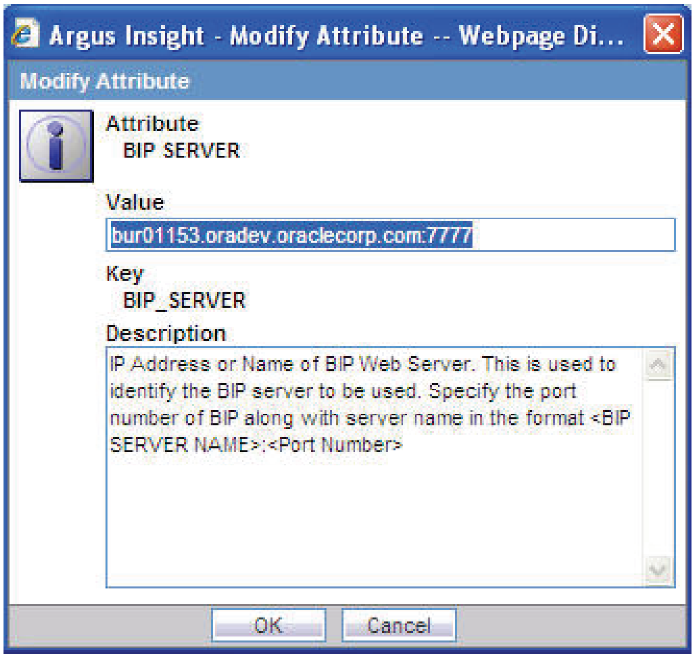
- BIP SERVER
- KEEP REPORT DATA

To define the attributes required for BIP, execute the following steps:

1. Click the **List Maintenance** tab on the ADMINISTRATION TOOLS page.
2. Select **Profile Switches** from the List Maintenance Items group.

3. Select **BIP SERVER** from the Attributes group.

   a. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
BIP SERVER

Value
bur01153.oradev.oraclecorp.com:7777

Key
BIP_SERVER

Description
IP Address or Name of BIP Web Server. This is used to identify the BIP server to be used. Specify the port number of BIP along with server name in the format <BIP SERVER NAME>:<Port Number>

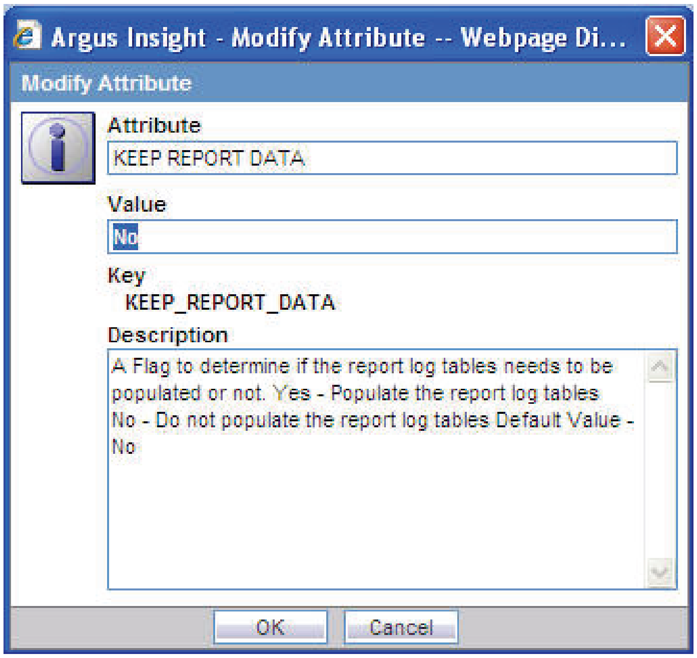
   b. Enter the IP Address or Name of the BIP Web Server in the **Value** field. Specify the port number of BIP along with server name in the following format:

      <BIP SERVER NAME>:<Port Number>

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

4. Select **KEEP REPORT DATA** from the Attributes group. This attribute is used to determine if the report log tables needs to be populated or not.

   a. Click **Modify.** The following **Modify Attribute** dialog box opens:



Attribute
KEEP REPORT DATA

Value
No

Key
KEEP_REPORT_DATA

Description
A Flag to determine if the report log tables needs to be populated or not. Yes - Populate the report log tables No - Do not populate the report log tables Default Value - No

b. Enter **Yes** or **No** in the **Value** field.

   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 your changes and return to the **List Maintenance** tab.

## 4.3 Mapping Case Workflow States

Workflow is company-specific and your company may not use all the Workflow states.

---

**Note:** The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.2.

This attribute should be configured for the Regulatory Submission and Distribution Compliance Report, Supplier Performance Report, Process Performance Workflow Report, and all the Workflow related Reports of Management Category.

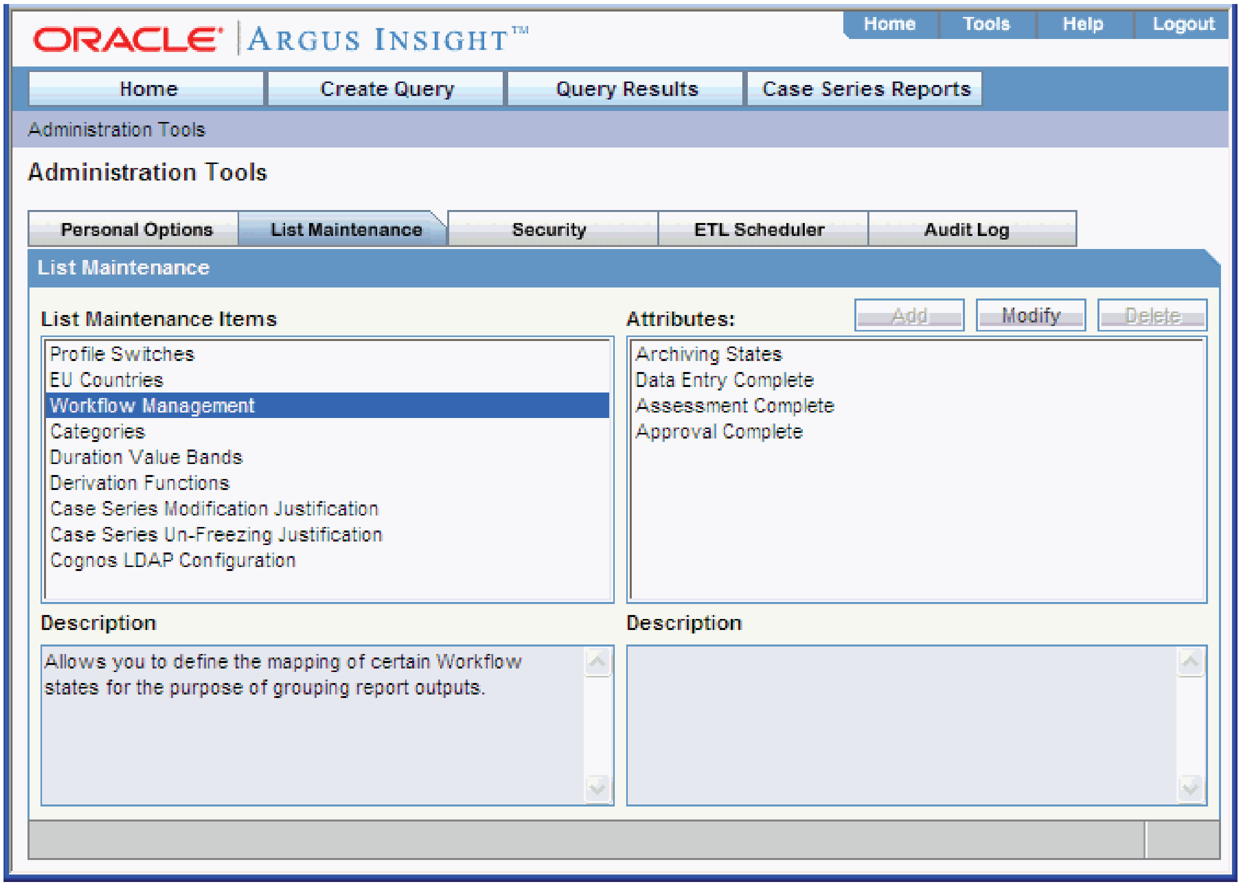
---

To configure workflow management for the Argus Insight application:

1. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
2. Click the **List Maintenance** tab.
3. Select **Workflow Management** from the List Maintenance Items group.

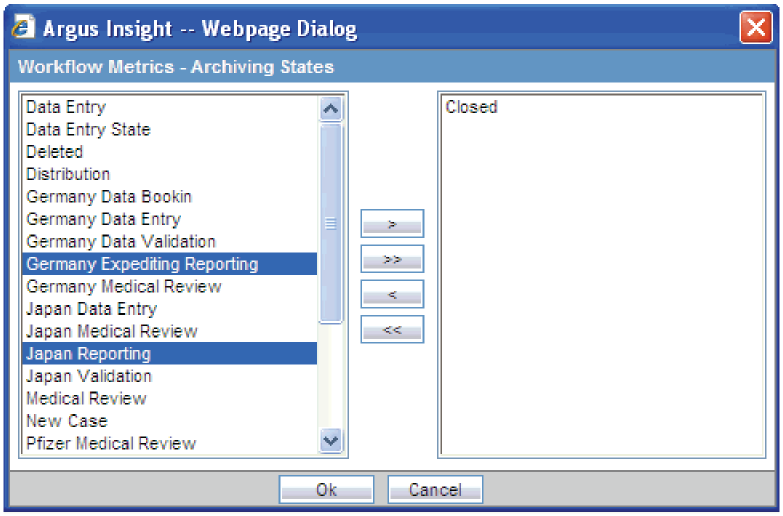
   The system updates the Attributes group with the following entries that you can modify:

   - Archiving States
   - Data Entry Complete
   - Assessment Complete
   - Approval Complete



Allows you to define the mapping of certain Workflow states for the purpose of grouping report outputs.

4. Select **Archiving States** from the Attributes group, and click **Modify.** The following dialog box opens:



   a. Select **Germany Expediting Reporting, Japan Reporting,** and **US-Reporting** from the list on the left.

   b. Click the right arrow (>) to add them as Archiving States.

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

5. Select **Data Entry Complete** from the Attributes group, and click **Modify.**

   a. Select **Germany Data Validation, Japan Validation**, and **US-Validation** from the list on the left.
   b. Click the right arrow (>) to add them as Data Entry Complete.
   c. Select **Closed** from the list on the right.
   d. Click the left arrow (<) to remove the Closed entry.
   e. Click **OK** to save your changes and return to the List Maintenance tab.

6. Select **Assessment Complete** from the Attributes group, and click **Modify.**
   a. Select **Germany Medical Review, Japan Medical Review,** and **US Medical Review** from the list on the left.
   b. Click the right arrow (>) to add them as Assessment Complete.
   c. Select **Closed** from the list on the right.
   d. Click the left arrow (<) to remove the Closed entry.
   e. Click **OK** to save your changes and return to the List Maintenance tab.
7. Select **Approval Complete** from the Attributes group, and click **Modify.**
   a. Select **Germany Medical Review, Japan Medical Review,** and **US Medical Review** from the list on the left.
   b. Click the right arrow (>) to add them as Approval Complete.
   c. Select **Closed** from the list on the right.
   d. Click the left arrow (<) to remove the Closed entry.
   e. Click **OK** to save your changes and return to the List Maintenance tab.

## 4.4 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.

---

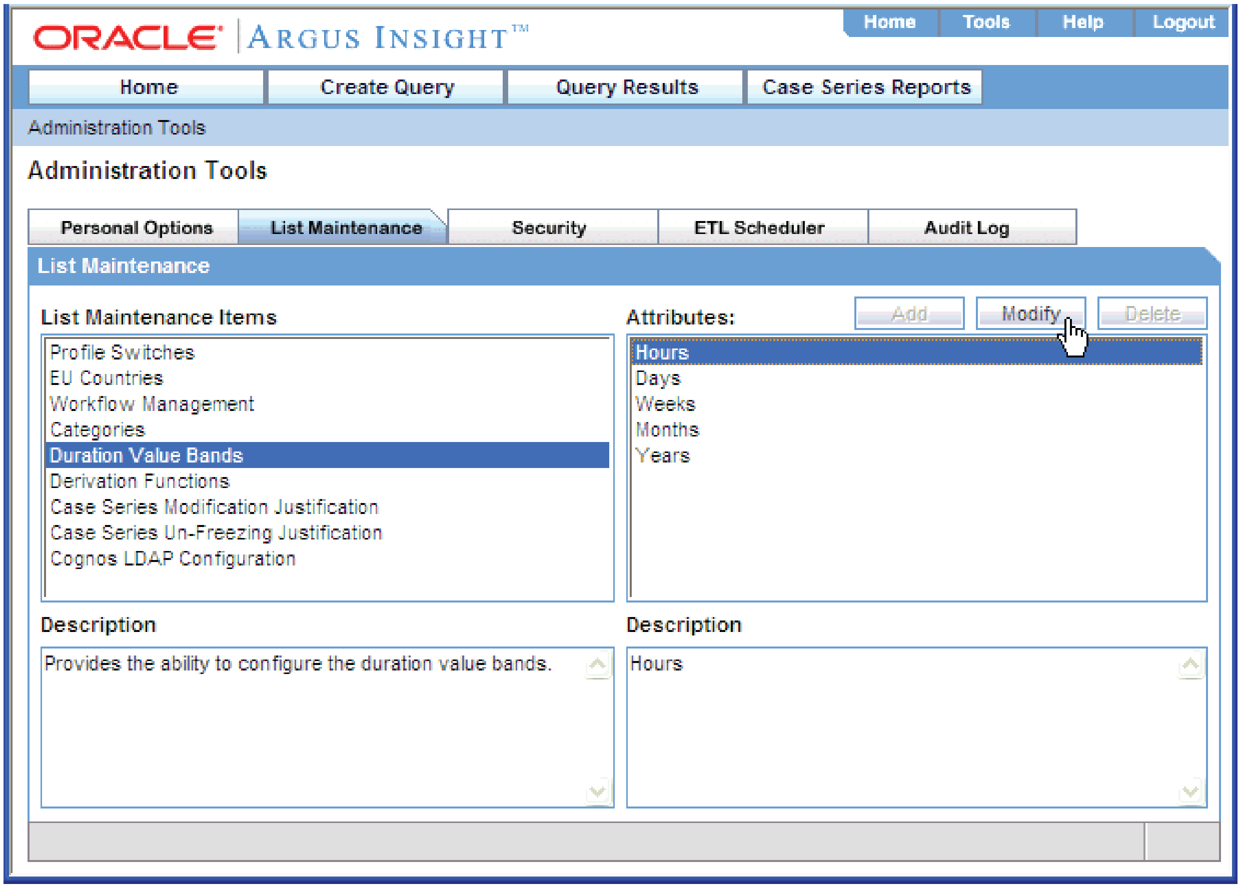
**Note:** Duration Value Band configuration must be done before running the Initial ETL.

If Duration Value Bands are modified after Initial ETL, you must re-run the Initial ETL.

---

To modify a duration value band:

1. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
2. Click the **List Maintenance** tab.
3. Select **Duration Value Bands** from the List Maintenance Items group. 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.



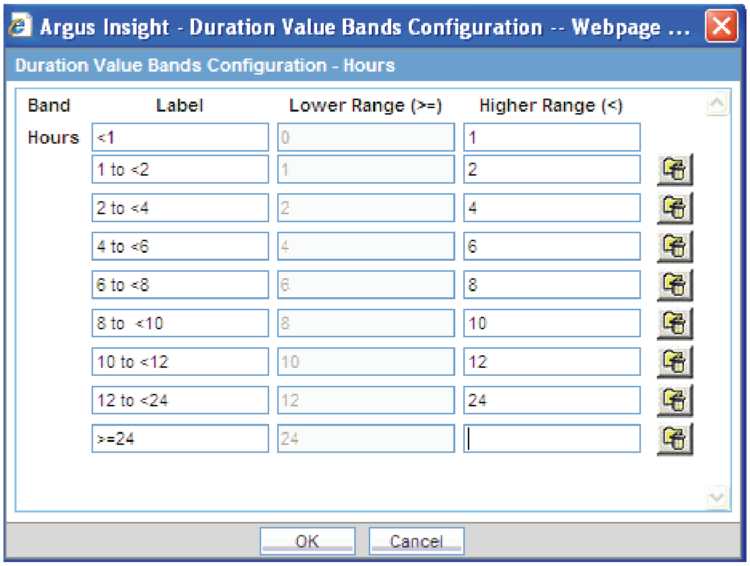
Provides the ability to configure the duration value bands.

Hours

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 displays 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, as appropriate:

   - 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 your changes.

## 4.5 Configuring Derivation Functions

Argus Insight lets you 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, you can create a new List Maintenance item called **Report Type 1** and derive to this item all the cases that have the **Report Type** attribute defined as **Spontaneous, Literature,** or **Compassionate Use.** As a result, Report Type 1 appears as an option in the query tool interface corresponding to the Report Type attribute. When you select Report Type 1 from the Report Type list and execute your query, the system returns only those cases that have the Report Type attribute specified as Spontaneous, Literature, or Compassionate Use.

You can specify more than one attribute. For example, you can create a further specialized List Maintenance item called **Report Type 1 US** and derive to this item 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.**

---

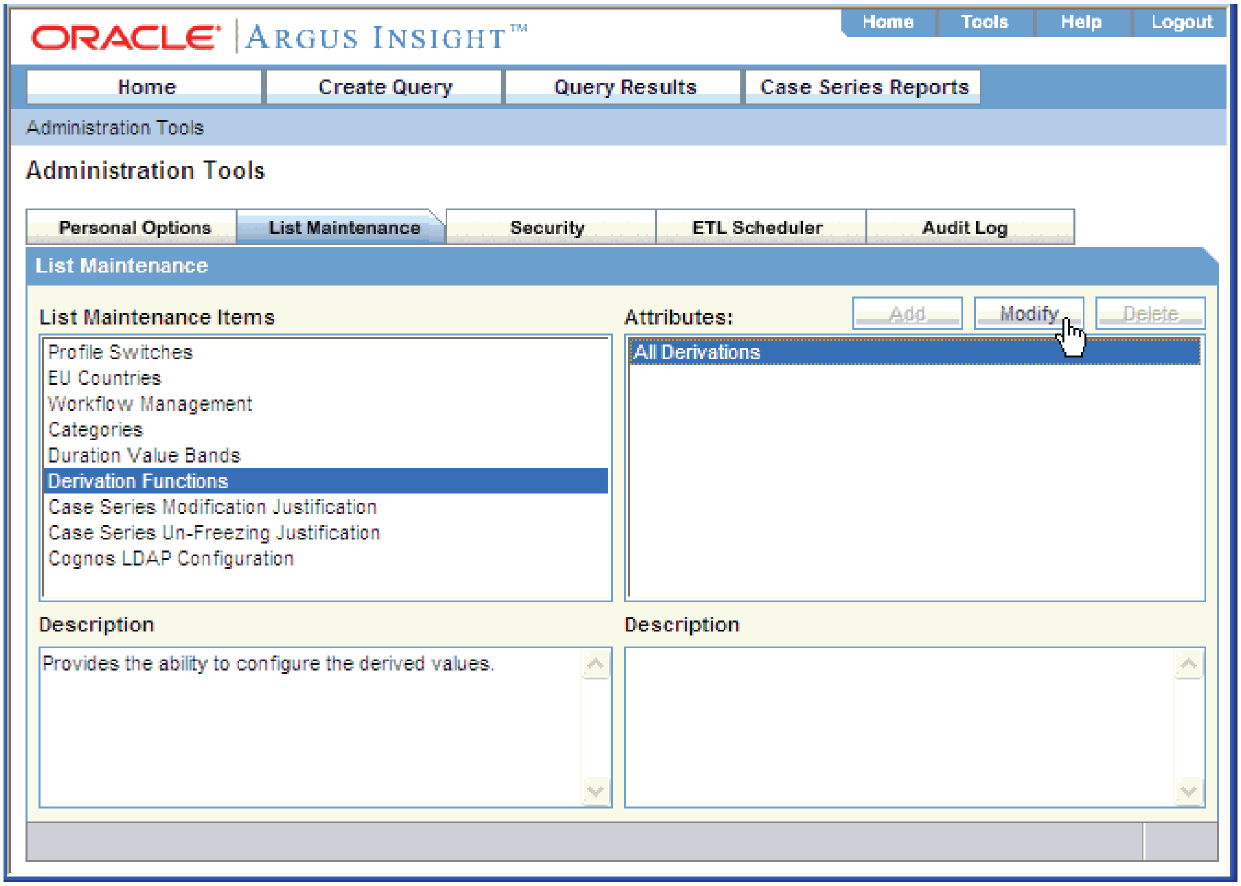
**Note:** There can be situations where two different List Maintenance items you create contain similar attributes in the SQL criteria. In this case, you can assign a priority level to individual List Maintenance items. The priority level determines which List Maintenance item SQL executes first.

---

## 4.5.1 Opening the Derivation Fields Dialog Box

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

1. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
2. Click the **List Maintenance** tab.
3. Select **Derivation Functions** from the List Maintenance Items group.



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

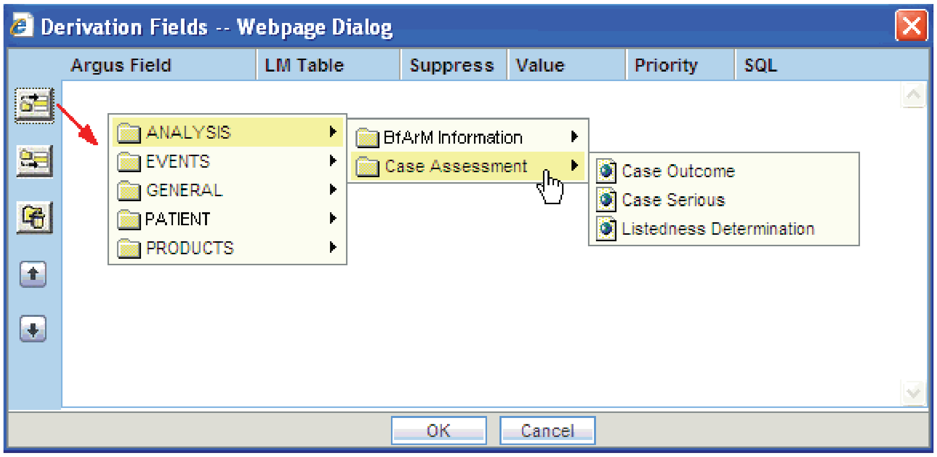
All Derivations

Description

Provides the ability to configure the derived values.

Description

4. Select **All Derivations** from the Attributes group, and click **Modify.** The Derivation Fields dialog box opens.



## 4.5.2 Icons in the Derivation Fields Dialog Box

Table 4–1 describes the icons in the Derivation Fields dialog box that you can use to add, delete, and reorder derivation field elements (rows).

*Table 4–1 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 |

## 4.5.3 Field Mapping Derivation Rules

Table 4–2 lists the available field mapping derivation rules for Argus Insight.

*Table 4–2 Field Mapping Derivation Rules*

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

*Table 4–2 (Cont.) Field Mapping Derivation Rules*

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

---

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

---

## 4.5.4 Fields and Check Boxes in the Derivation Fields Dialog Box

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

### 4.5.4.1 LM Table

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

### 4.5.4.2 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.

---

### 4.5.4.3 Value

The Value field captures the value for the new derivation field. For the following four 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 that you 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

### 4.5.4.4 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.

### 4.5.4.5 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 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:

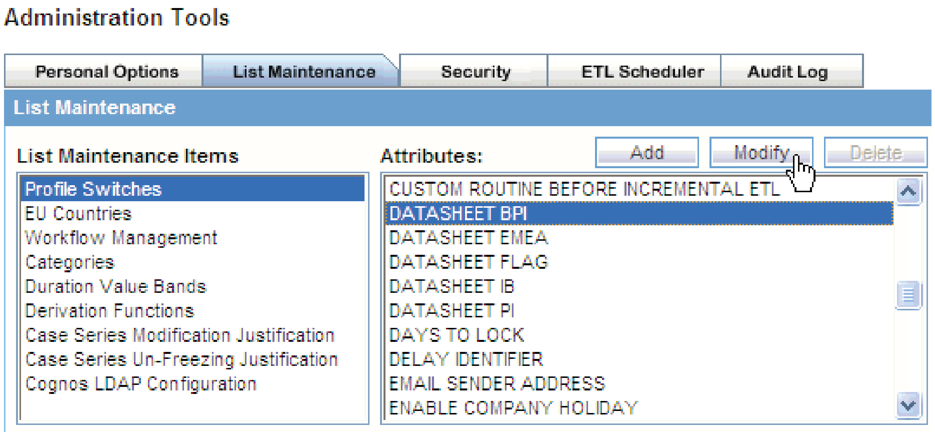
  **Correct:** SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  **Incorrect:** SELECT DISTINCT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

## 4.6 Configuring the Product Datasheet

To configure the product datasheet:

1. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
2. Click the **List Maintenance** tab.
3. Select **Profile Switches** from the List Maintenance Items group.



4. Select and modify the following profile switches in the Attributes group:

   - DATASHEET BPI
   - DATASHEET EMEA
   - DATASHEET IB
   - DATASHEET PI

   These profile switches let you configure the user-defined fields for assessment of each datasheet on the Product tab.

## 4.7 Configuring the Argus Insight Scheduling Service

To configure the Argus Insight scheduling service:

1. Log in to the Argus Insight Web Server.
2. Click **Start** and then select **Run.**
3. Type **services.msc** in the text box and click **OK.** The Services window opens.
4. Right-click **Argus Insight Service** and then select **Properties.** The Argus Insight Service Properties dialog box opens.
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 your changes and close the dialog box.

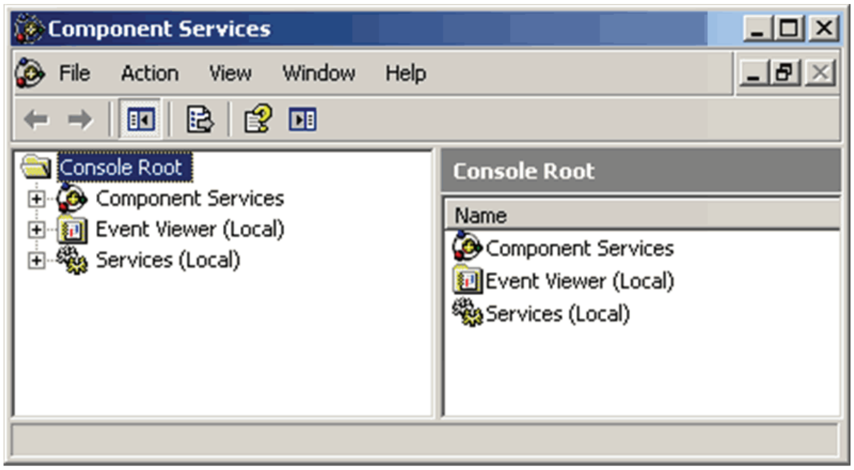
> **Note:** To change the interval of different service tasks, modify the entries in the Service.config file located in the Bin folder of Argus Insight. All the times in the Service.config file are specified in seconds.

**IMPORTANT!** Ensure that the user who runs this service has administrator privileges. If the user does not have administrator privileges, either the Scheduled CIOMS Reports might not return or an LDAP user might not be able to log in to the Argus Insight application.

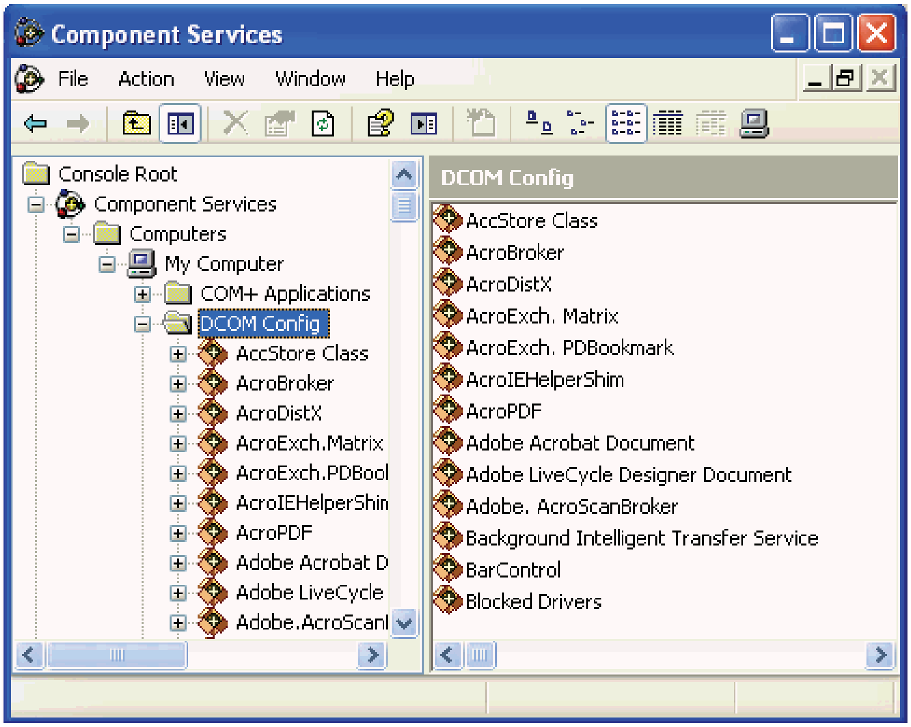
## 4.8 Configuring the CIOMS and MedWatch Reports

These are required settings because PwReports.exe file is responsible for LDAP authentication along with CIOMS and MedWatch reports.

1. Log in to the Argus Insight Web Server.
2. Click **Start** and then select **Run.**
3. Type **dcomcnfg** in the text box and click **OK.** The Component Services window opens.

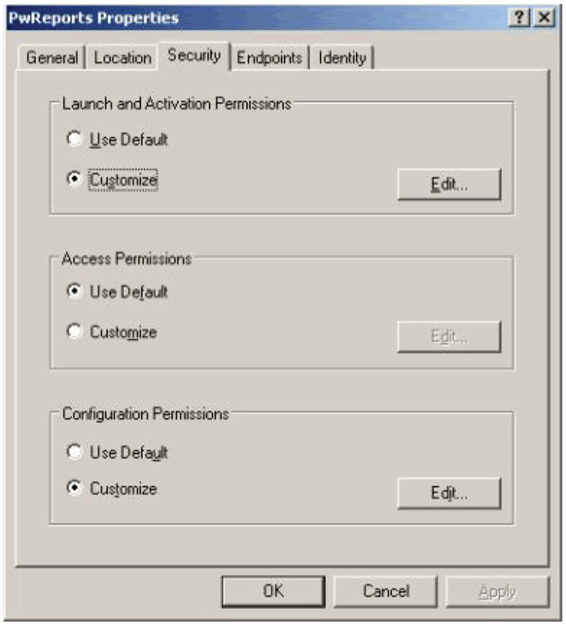


4. Navigate to **Console Root, Component Services, Computers, My Computer,** and then select **DCOM Config.**



5. Right-click **PwReports** and select **Properties.** The PwReports Properties dialog box opens.

6. Click the **Security** tab.



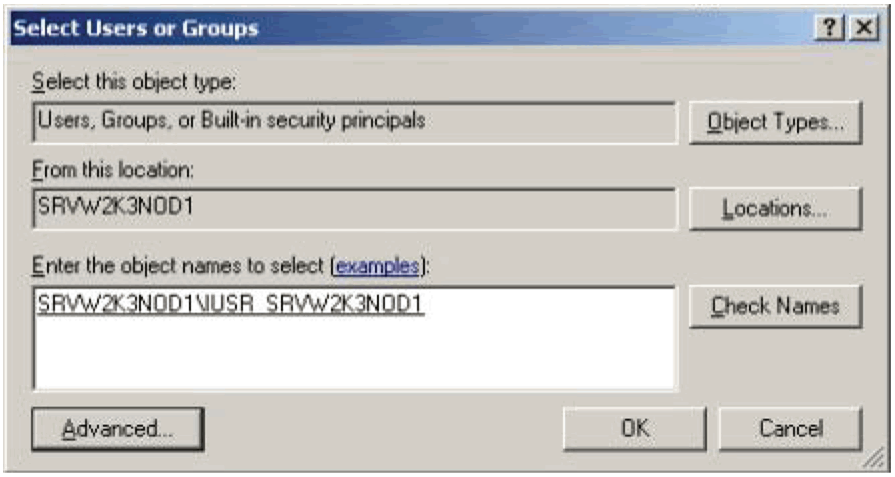
Launch and Activation Permissions
○ Use Default
● Customize

Access Permissions
● Use Default
○ Customize

Configuration Permissions
○ Use Default
● Customize

7. Look in the Launch and Activation Permissions group, select **Customize,** and then click **Edit.** The Launch Permission dialog box opens.

8. Click **Add.** The Select Users or Groups dialog box opens.



Select this object type:
Users, Groups, or Built-in security principals

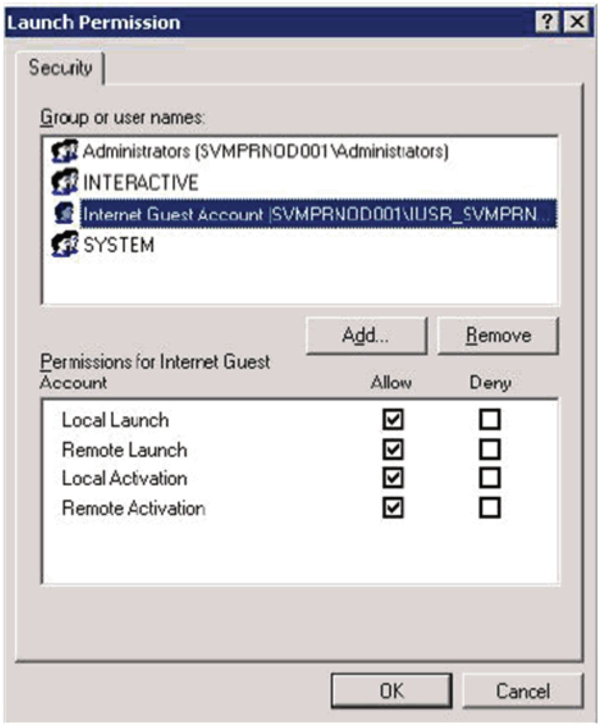
From this location:
SRVW2K3NOD1

Enter the object names to select (examples):
SRVW2K3NOD1\IUSR_SRVW2K3NOD1

a. In the **Enter the object names to select** field, add the following information:

   *machine_name*\IUSR

b. Click **OK.** The system returns to the Launch Permission dialog box:



Group or user names:
- Administrators (SVMPRNOD001\Administrators)
- INTERACTIVE
- Internet Guest Account (SVMPRNOD001\IUSR_SVMPRN...
- SYSTEM

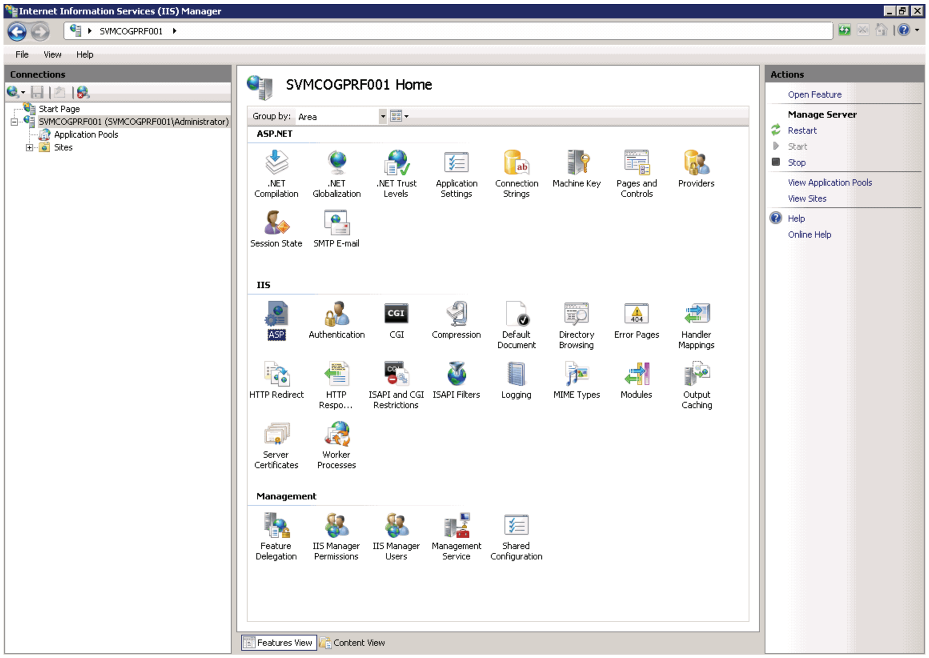
| Permissions for Internet Guest Account | Allow | Deny |
|---|---|---|
| Local Launch | ☑ | ☐ |
| Remote Launch | ☑ | ☐ |
| Local Activation | ☑ | ☐ |
| Remote Activation | ☑ | ☐ |

9. Complete the Launch Permission dialog box as follows:
   a. Select the newly created **Internet Guest Account.**
   b. Grant the listed permissions to the account by selecting all the check boxes in the Allow column.
   c. Click **OK.**
10. Exit the Component Services program.

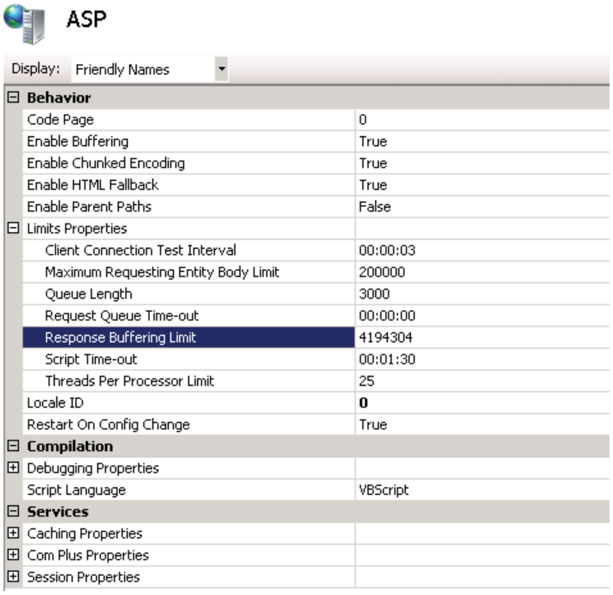
## 4.9 Configuring the IIS File Download Limit

To configure the IIS file download limit for Windows 2008:

1. Go to the Internet Information Services (IIS) Manager.



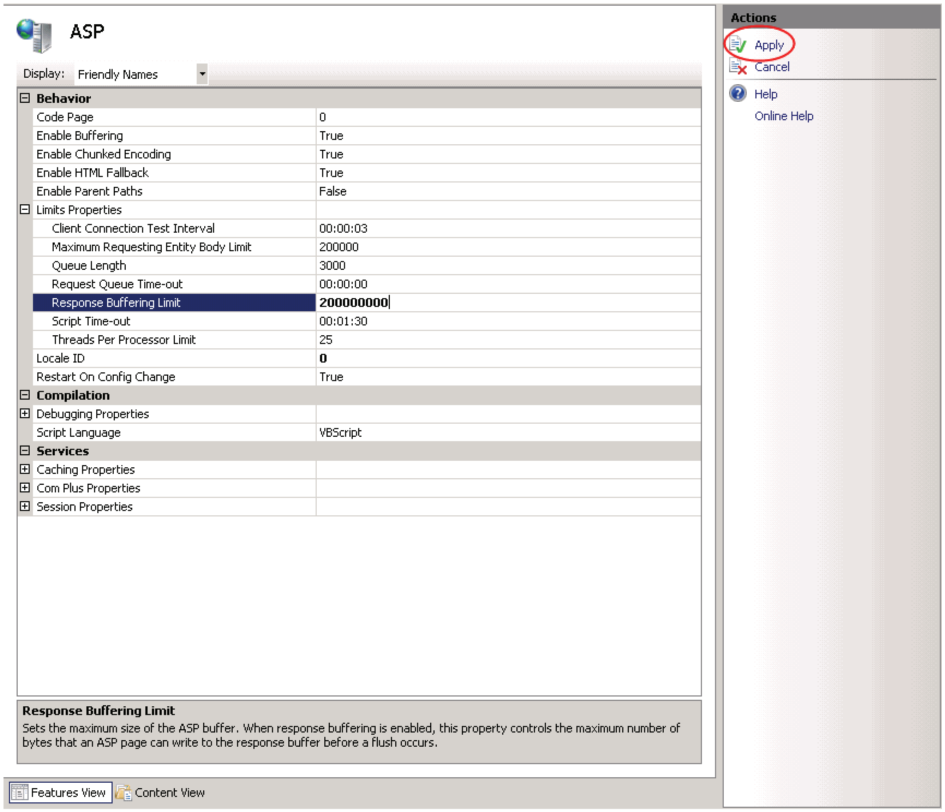
2. Double-click **ASP** in the right pane. The ASP dialog box opens.



Display: Friendly Names

| | |
|---|---|
| **Behavior** | |
| Code Page | 0 |
| Enable Buffering | True |
| Enable Chunked Encoding | True |
| Enable HTML Fallback | True |
| Enable Parent Paths | False |
| Limits Properties | |
| Client Connection Test Interval | 00:00:03 |
| Maximum Requesting Entity Body Limit | 200000 |
| Queue Length | 3000 |
| Request Queue Time-out | 00:00:00 |
| Response Buffering Limit | 4194304 |
| Script Time-out | 00:01:30 |
| Threads Per Processor Limit | 25 |
| Locale ID | **0** |
| Restart On Config Change | True |
| **Compilation** | |
| Debugging Properties | |
| Script Language | VBScript |
| **Services** | |
| Caching Properties | |
| Com Plus Properties | |
| Session Properties | |

3. Expand **Limit Properties** and change the **Response Buffering Limit** from its default value of 4 MB to a large value such as 200000000 (200 MB).



Display: Friendly Names

| | |
|---|---|
| **Behavior** | |
| Code Page | 0 |
| Enable Buffering | True |
| Enable Chunked Encoding | True |
| Enable HTML Fallback | True |
| Enable Parent Paths | False |
| Limits Properties | |
| Client Connection Test Interval | 00:00:03 |
| Maximum Requesting Entity Body Limit | 200000 |
| Queue Length | 3000 |
| Request Queue Time-out | 00:00:00 |
| Response Buffering Limit | **200000000** |
| Script Time-out | 00:01:30 |
| Threads Per Processor Limit | 25 |
| Locale ID | **0** |
| Restart On Config Change | True |
| **Compilation** | |
| Debugging Properties | |
| Script Language | VBScript |
| **Services** | |
| Caching Properties | |
| Com Plus Properties | |
| Session Properties | |

**Response Buffering Limit**
Sets the maximum size of the ASP buffer. When response buffering is enabled, this property controls the maximum number of bytes that an ASP page can write to the response buffer before a flush occurs.

4. Click **Apply** to save the changed value.
5. Restart the IIS service.
   a. Click **Start** and select **Run.**
   b. Type **iisreset -start** in the text box.
   c. Click **OK.**

## 4.9.1 Configuring the ASPMaxRequestEntityAllowed Value

Defining a value for the ASPMaxRequestEntityAllowed 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 ASPMaxRequestEntityAllowed setting in the MetaBase.xml file. Increasing the setting ensures that the ASP can post that much data onto the server.

To change the value of the ASPMaxRequestEntityAllowed setting:

1. Stop the Internet Information Services (IIS):

   ```
   iisreset /stop
   ```

2. Navigate to the following folder:

   \WINDOWS\system32\inetsrv

3. Open the **MetaBase.xml** file for editing.
4. Find the following line in the file:

```
ASPMaxRequestEntityAllowed=
```

5. Set this value to the lowest possible value that allows for the functionality you need. A common value is **500000.** The maximum value is 1,073,741,824 bytes.
6. Save the file.
7. Restart the Internet Information Services (IIS):

   ```
   iisreset /start
   ```

Alternatively, you can use DOS commands to change the value of the ASPMaxRequestEntityAllowed setting:

1. Open the DOS command prompt.
2. Change to the following directory:

   ```
   cd drive:\inetpub\adminscripts
   ```

   where *drive* is the hard disk where IIS is installed.
3. Enter the following command:

   ```
   cscript adsutil.vbs set w3svc/ASPMaxRequestEntityAllowed value
   ```

   where *value* is the lowest possible value that allows for the functionality you need. A common value is **500000.** The maximum value is 1,073,741,824 bytes.
4. Restart the Internet Information Services (IIS):

   ```
   iisreset /start
   ```

## 4.10 Using Export and Import to Copy Configuration Data

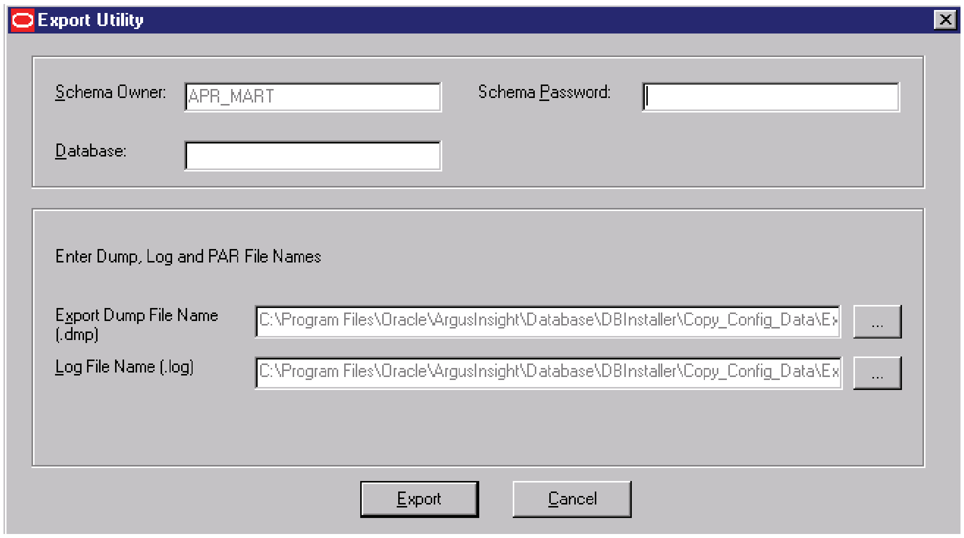
Before configuring export and import functions, be aware of the following:

- 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 Insight data mart will also be copied and applied on the new Argus Instance which will be associated with the new 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 ensure that all the enterprises which are part of the source Argus Insight database, have been created in the Target Argus Insight database.

### 4.10.1 Exporting Data

To export data:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Export Data.** The Export Utility dialog box opens.



Schema Owner: APR_MART

Schema Password:

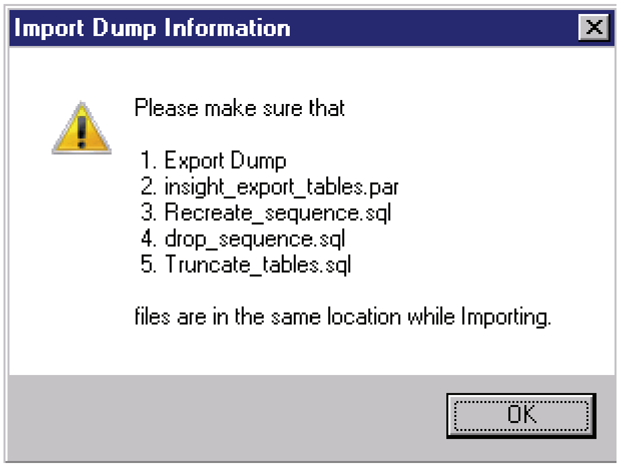
Database:

Enter Dump, Log and PAR File Names

Export Dump File Name (.dmp): C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\Copy_Config_Data\Ex

Log File Name (.log): C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\Copy_Config_Data\Ex

3. Enter the name of the schema owner, the schema password, and the name of database.
4. Enter the complete directory path and file name for the export dump file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Export Dump File Name** field. When the Export Dump File dialog box opens, navigate to the appropriate location, enter the file name in the **File name** field, and then click **Save.** The system returns to the Export Utility dialog box.
5. Enter the complete directory path and file name for the log file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Log File Name** field. When the Log File dialog box opens, navigate to the appropriate location, enter the file name in the **File name** field, and then click **Save.** The system returns to the Export Utility dialog box.
6. Click **Export** to continue with the data export. This displays the **Import Dump Information** dialog box, as shown in the following figure:

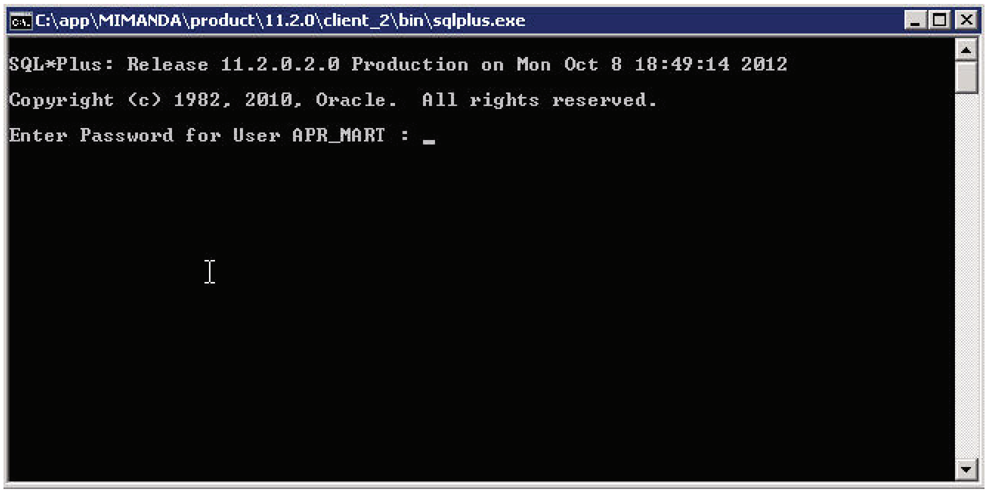


Please make sure that

1. Export Dump
2. insight_export_tables.par
3. Recreate_sequence.sql
4. drop_sequence.sql
5. Truncate_tables.sql

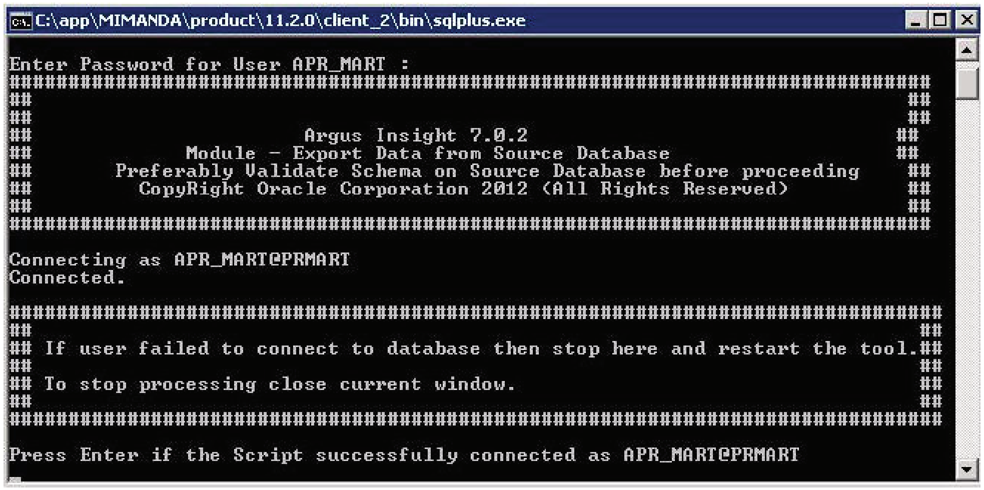
files are in the same location while Importing.

7. Verify the list of files and Click **OK**. This displays the following command screen:



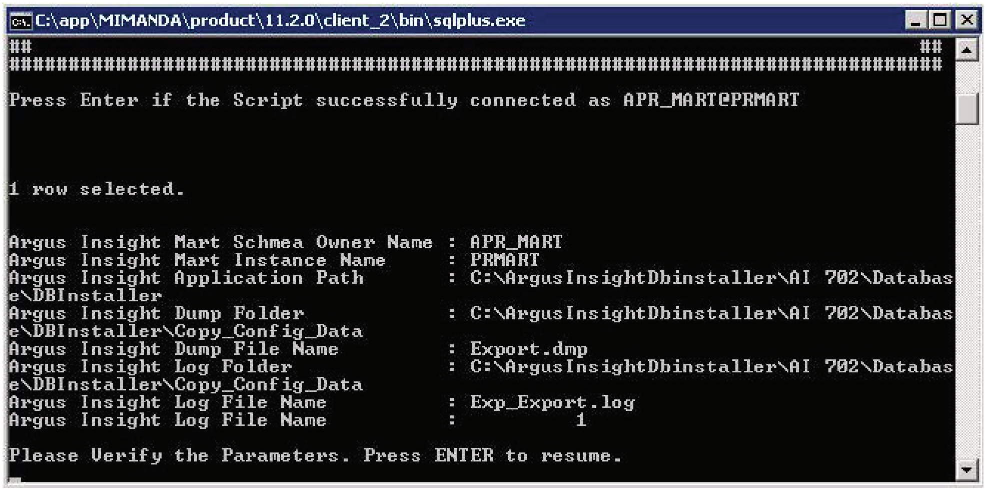
```
SQL*Plus: Release 11.2.0.2.0 Production on Mon Oct 8 18:49:14 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

Enter Password for User APR_MART : _
```

8. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



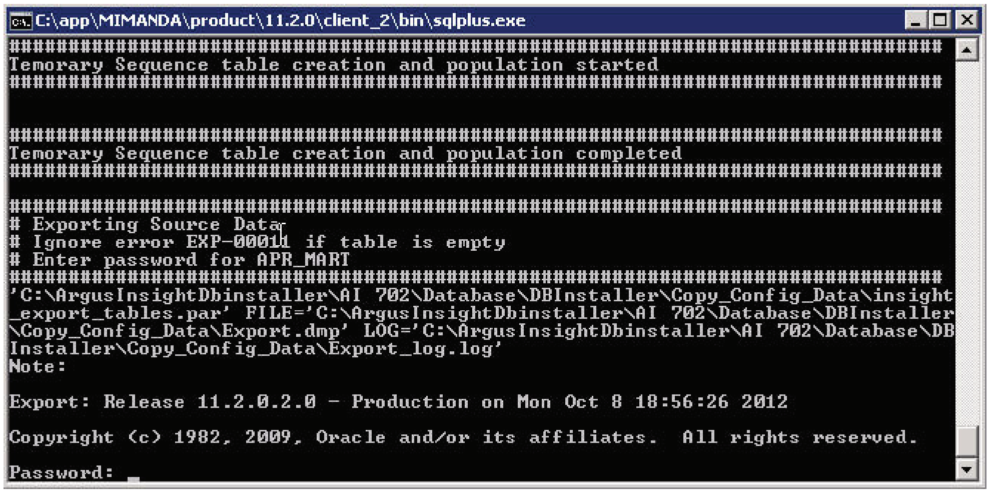
```
Enter Password for User APR_MART :
##############################################################################
##                                                                          ##
##                                                                          ##
##                       Argus Insight 7.0.2                               ##
##             Module - Export Data from Source Database                   ##
##       Preferably Validate Schema on Source Database before proceeding    ##
##         CopyRight Oracle Corporation 2012 (All Rights Reserved)          ##
##                                                                          ##
##############################################################################

Connecting as 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
```

9. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name> and press **Enter**. This displays the following command screen:



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

Press Enter if the Script successfully connected as APR_MART@PRMART



1 row selected.


Argus Insight Mart Schmea Owner Name : APR_MART
Argus Insight Mart Instance Name     : PRMART
Argus Insight Application Path       : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller
Argus Insight Dump Folder            : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller\Copy_Config_Data
Argus Insight Dump File Name         : Export.dmp
Argus Insight Log Folder             : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller\Copy_Config_Data
Argus Insight Log File Name          : Exp_Export.log
Argus Insight Log File Name          :          1

Please Verify the Parameters. Press ENTER to resume.
```

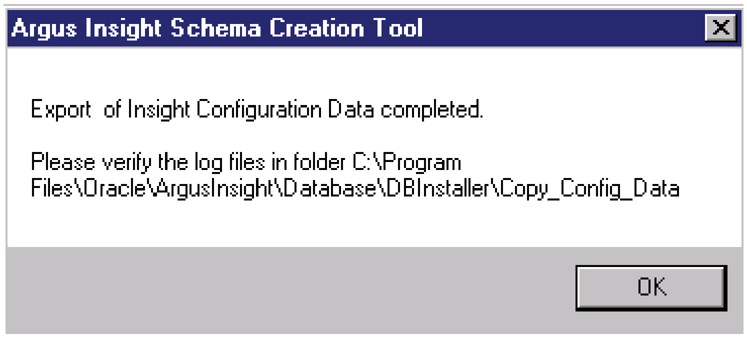
10. Verify the details mentioned on the command screen and press **Enter**. This displays the following command screen:



```
###############################################################################
Temorary Sequence table creation and population started
###############################################################################


###############################################################################
Temorary Sequence table creation and population completed
###############################################################################

###############################################################################
# Exporting Source Data
# Ignore error EXP-00011 if table is empty
# Enter password for APR_MART
###############################################################################
'C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\Copy_Config_Data\insight
_export_tables.par' FILE='C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller
\Copy_Config_Data\Export.dmp' LOG='C:\ArgusInsightDbinstaller\AI 702\Database\DB
Installer\Copy_Config_Data\Export_log.log'
Note:

Export: Release 11.2.0.2.0 - Production on Mon Oct 8 18:56:26 2012

Copyright (c) 1982, 2009, Oracle and/or its affiliates.  All rights reserved.

Password: _
```

11. Enter the password for the **APR_MART** user and press **Enter**. This displays a **commit complete** message along with the confirmation that the data has been exported successfully. Press **Enter** to continue.

    The system displays a message when the Argus Insight configuration data has been exported:



Export of Insight Configuration Data completed.

Please verify the log files in folder C:\Program Files\Oracle\ArgusInsight\Database\DBInstaller\Copy_Config_Data

12. Click **OK** to close the dialog box. Be sure to review the log files for information about the export as well as export errors, if any.

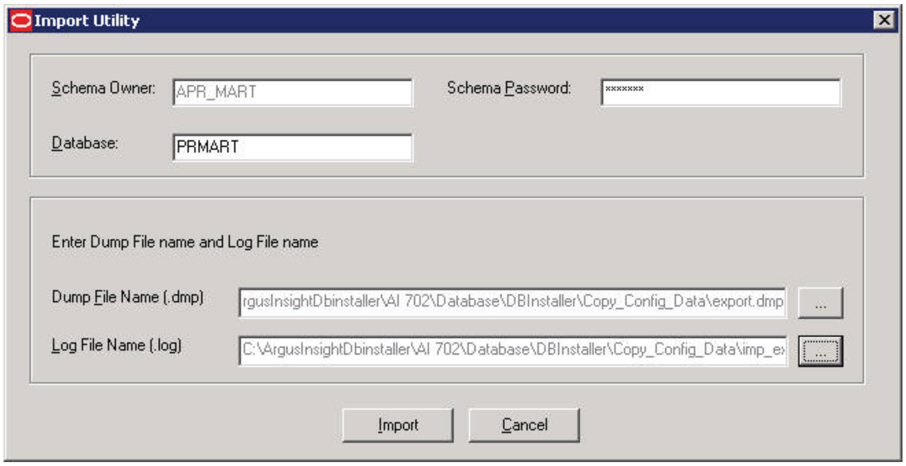
    Log files are in the following folder:

    \Program Files\Oracle\ArgusInsight\Database\DBInstaller\Copy_Config_Data

### 4.10.2 Importing Data

To import data:

1. Start the Argus Insight Schema Creation Tool.
2. Click **Import Data.** The **Import Utility** dialog box opens.



Schema Owner: APR_MART

Schema Password: xxxxxxx

Database: PRMART

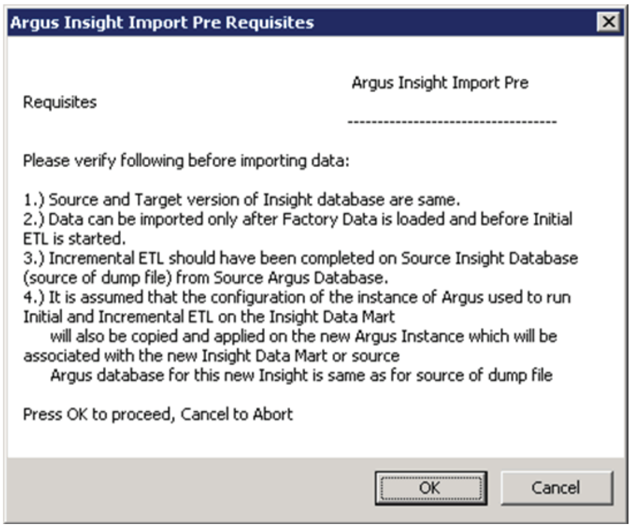
Enter Dump File name and Log File name

Dump File Name (.dmp) rgusInsightDbinstaller\AI 702\Database\DBInstaller\Copy_Config_Data\export.dmp

Log File Name (.log) C:\ArgusInsightDbinstaller\AI 702\Database\DBInstaller\Copy_Config_Data\imp_ex

3. Enter the name of the schema owner, the schema password, and the name of database.
4. Enter the complete directory path and file name for the dump file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Dump File Name** field. When the Import Dump File dialog box opens, navigate to the appropriate location, enter the file name in the **File name** field, and then click **Open.** The system returns to the Import Utility dialog box.
5. Enter the complete directory path and file name for the log file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Log File Name** field. When the Log File dialog box opens, navigate to the appropriate location, enter the file name in the **File name** field, and then click **Open.** The system returns to the Import Utility dialog box.
6. Click **Import** to continue with the data import.

   The system opens a dialog box that lists the prerequisites to importing data.



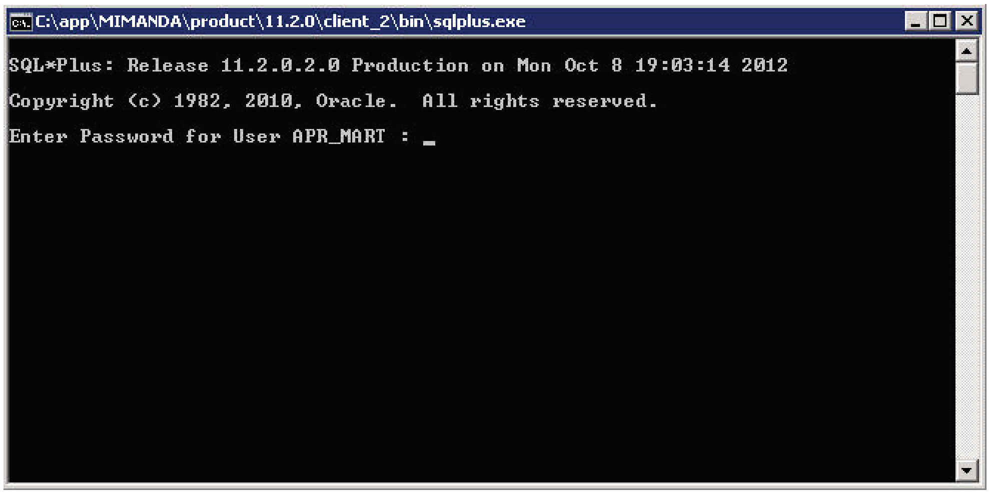
Argus Insight Import Pre
Requisites
-----------------------------------

Please verify following before importing data:

1.) Source and Target version of Insight database are same.
2.) Data can be imported only after Factory Data is loaded and before Initial ETL is started.
3.) Incremental ETL should have been completed on Source Insight Database (source of dump file) from Source Argus Database.
4.) It is assumed that the configuration of the instance of Argus used to run Initial and Incremental ETL on the Insight Data Mart
    will also be copied and applied on the new Argus Instance which will be associated with the new Insight Data Mart or source
    Argus database for this new Insight is same as for source of dump file

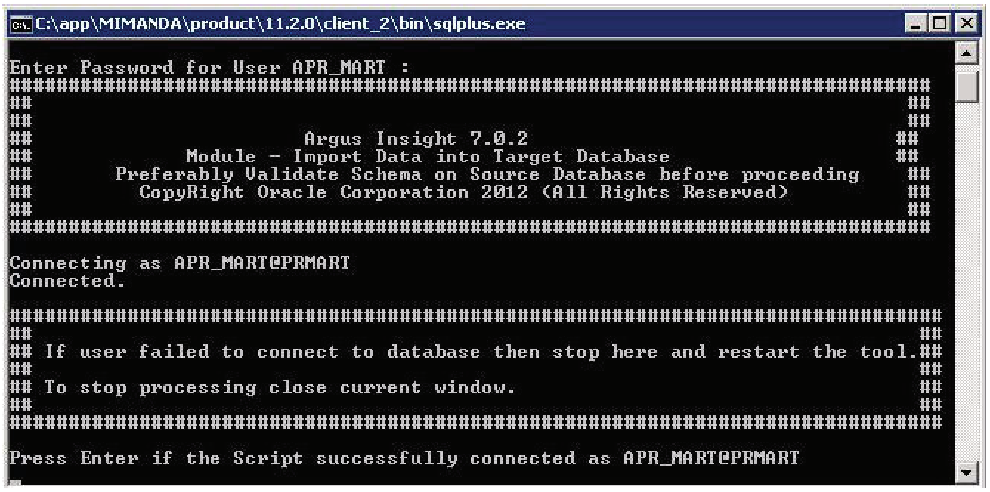
Press OK to proceed, Cancel to Abort

7. Review the prerequisites and verify that your system complies with the requirements.
   - If you have not met all the prerequisites, click **Cancel** to stop the data import. Complete all prerequisites before restarting the data import process.
   - If you have met all the prerequisites, click **OK.** The system displays the following command screen:



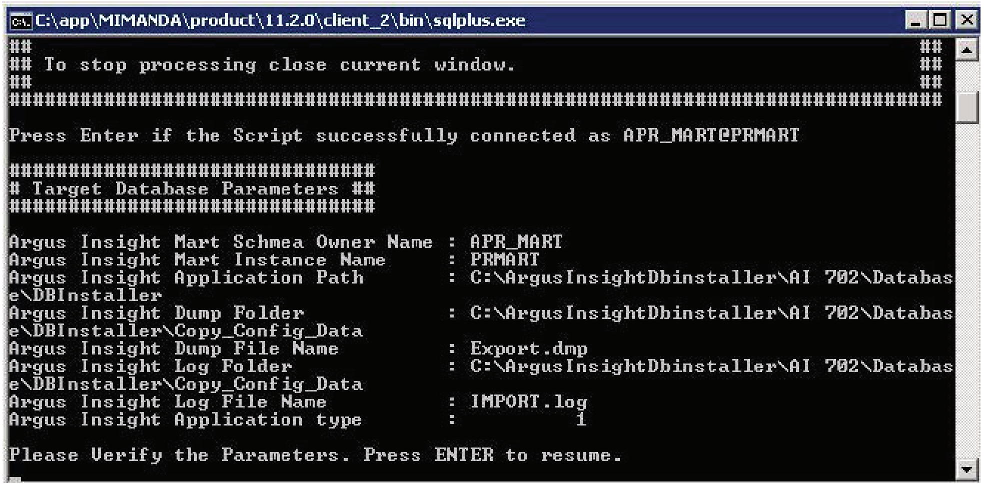
```
SQL*Plus: Release 11.2.0.2.0 Production on Mon Oct 8 19:03:14 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

Enter Password for User APR_MART : _
```

8. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



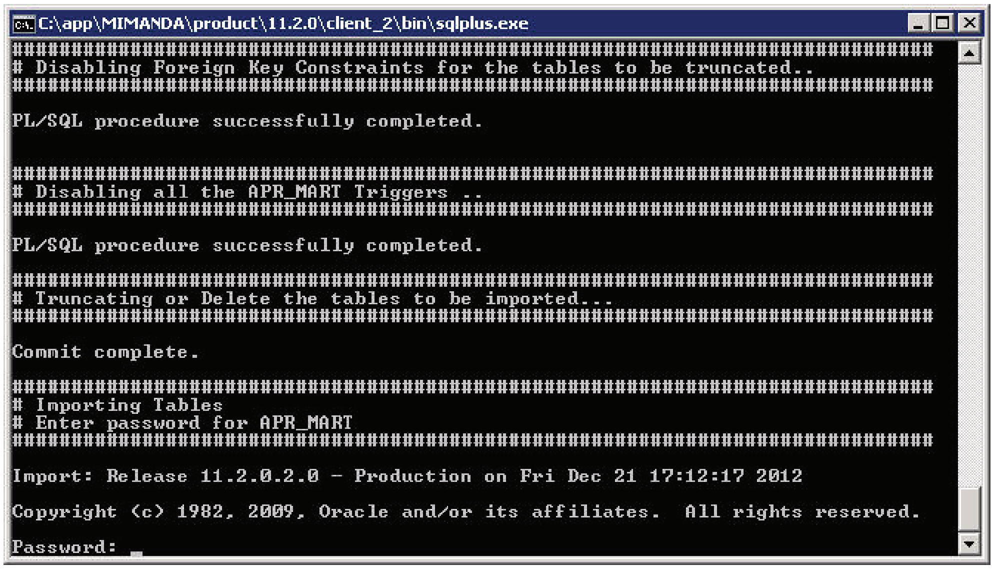
```
Enter Password for User APR_MART :
###############################################################################
##                                                                           ##
##                                                                           ##
##                       Argus Insight 7.0.2                                ##
##             Module - Import Data into Target Database                    ##
##       Preferably Validate Schema on Source Database before proceeding     ##
##         CopyRight Oracle Corporation 2012 (All Rights Reserved)           ##
##                                                                           ##
###############################################################################

Connecting as 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
```

9. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name> and press **Enter**. This displays the following command screen:



```
##                                                                          ##
## To stop processing close current window.                                 ##
##                                                                          ##
##############################################################################

Press Enter if the Script successfully connected as APR_MART@PRMART

###############################
# Target Database Parameters ##
###############################

Argus Insight Mart Schmea Owner Name : APR_MART
Argus Insight Mart Instance Name     : PRMART
Argus Insight Application Path       : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller
Argus Insight Dump Folder            : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller\Copy_Config_Data
Argus Insight Dump File Name         : Export.dmp
Argus Insight Log Folder             : C:\ArgusInsightDbinstaller\AI 702\Databas
e\DBInstaller\Copy_Config_Data
Argus Insight Log File Name          : IMPORT.log
Argus Insight Application type       :          1

Please Verify the Parameters. Press ENTER to resume.
```

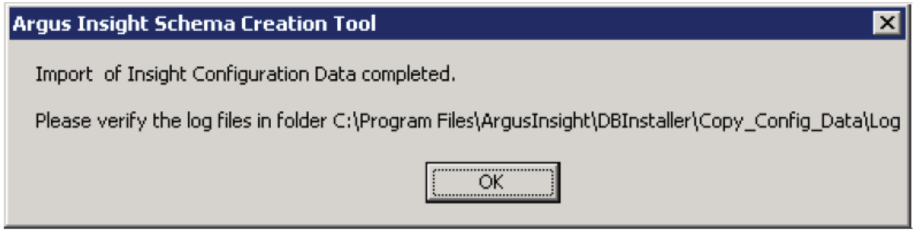
10. Verify the details on the command screen and press **Enter**. This displays the following command screen:



```
#############################################################################
# Disabling Foreign Key Constraints for the tables to be truncated..
#############################################################################

PL/SQL procedure successfully completed.


#############################################################################
# Disabling all the APR_MART Triggers ..
#############################################################################

PL/SQL procedure successfully completed.

#############################################################################
# Truncating or Delete the tables to be imported...
#############################################################################

Commit complete.

#############################################################################
# Importing Tables
# Enter password for APR_MART
#############################################################################

Import: Release 11.2.0.2.0 - Production on Fri Dec 21 17:12:17 2012

Copyright (c) 1982, 2009, Oracle and/or its affiliates.  All rights reserved.

Password: _
```

11. Enter the password for the **APR_MART** user and press **Enter**. This displays a confirmation message that the data has been imported successfully along with the location of the log file.

12. Press **Enter** to continue. When the Argus Insight configuration data has been imported, the system displays the following message:



Import of Insight Configuration Data completed.

Please verify the log files in folder C:\Program Files\ArgusInsight\DBInstaller\Copy_Config_Data\Log

13. Click **OK** to close the dialog box. Be sure to review the log files for information about the import as well as import errors, if any.

    Log files are in the following folder:

\Program Files\ArgusInsight\DBInstaller\Copy_Config_Data\Log

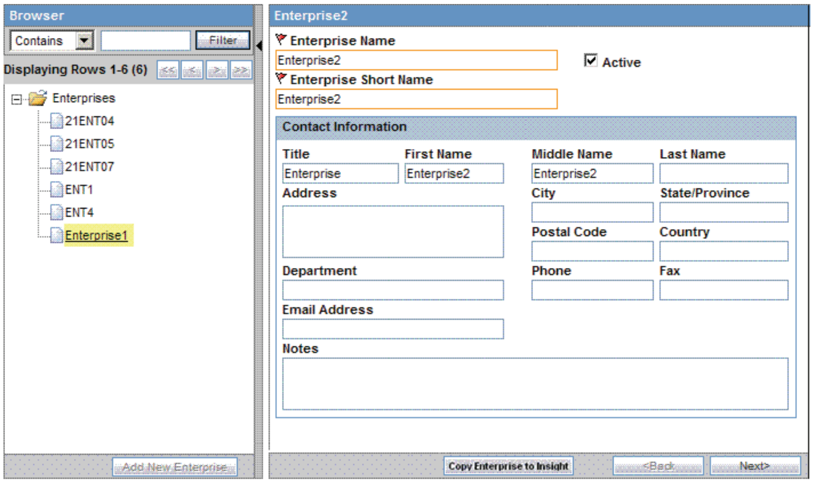
## 4.11 Using Argus Safety to Configure Enterprises for Argus Insight

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. Select an enterprise from the Enterprises folder in the left pane. The Enterprises folder includes only those enterprises that you have privilege to access:



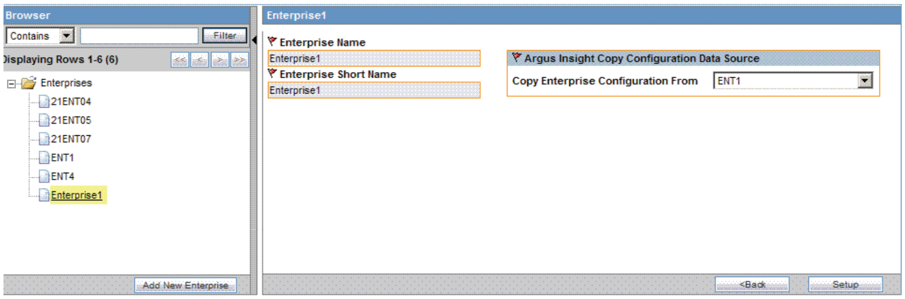
Enterprise Name: Enterprise2
☑ Active
Enterprise Short Name: Enterprise2
Title: Enterprise
First Name: Enterprise2
Middle Name: Enterprise2
Last Name:

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 system opens the following screen:



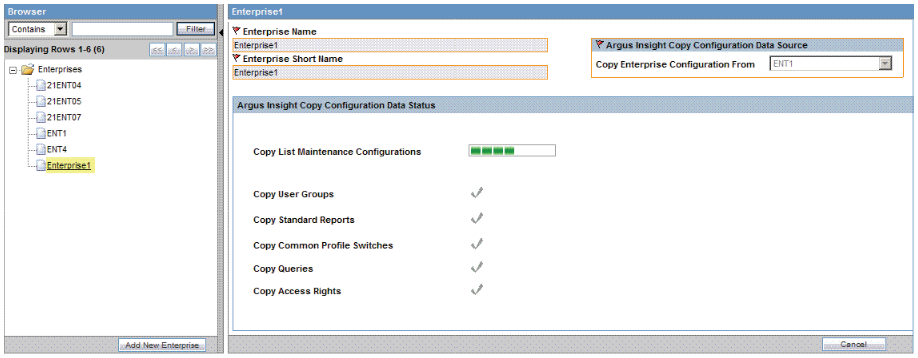
Enterprise Name: Enterprise1
Enterprise Short Name: Enterprise1
Copy Enterprise Configuration From: ENT1

4. Use the **Copy Enterprise Configuration From** field to 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 system begins to copy the configuration and displays status information 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.

## 4.12 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 that Auto extend is set to ON for all the data files in the database that are related to *staging* and *MART.*

In addition, note that:

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

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

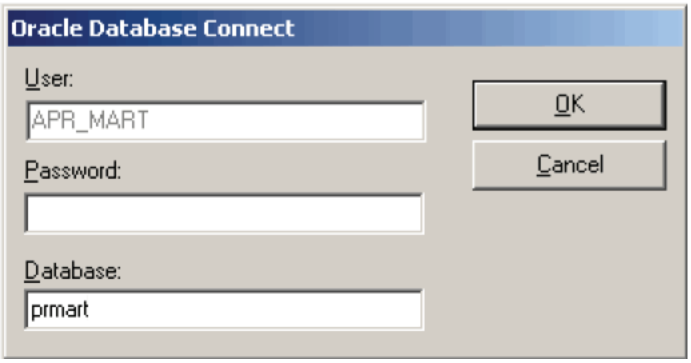
  Ignore this warning for all MedDRA tables.
- **Do not** run incremental ETL for more than 50,000 cases. Run the Initial ETL again if the number of cases exceeds 50,000.

## 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 opens.



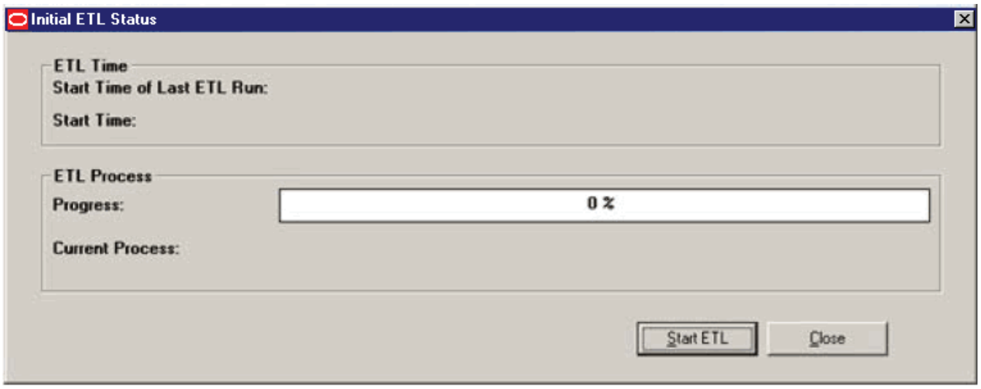
User: APR_MART

Password:

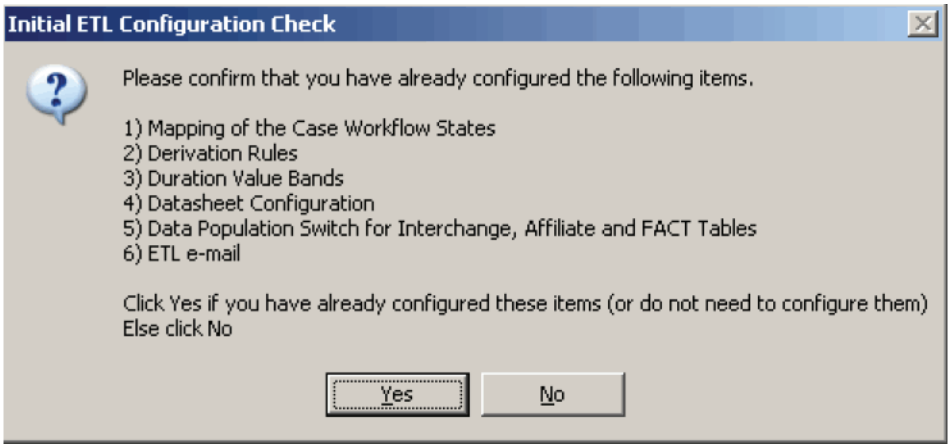
Database: prmart

5. Connect to the Oracle Database:
   - a. In the **Password** field, type the password for the APR_MART user.
   - b. In the **Database** field, type the name of your Argus Insight database.
   - c. Click **OK.**

   The Initial ETL Status dialog box opens.



6. Click **Start ETL** to start the initial process of extracting, transforming, and loading data. The system prompts for confirmation that you have completed the required configuration steps.

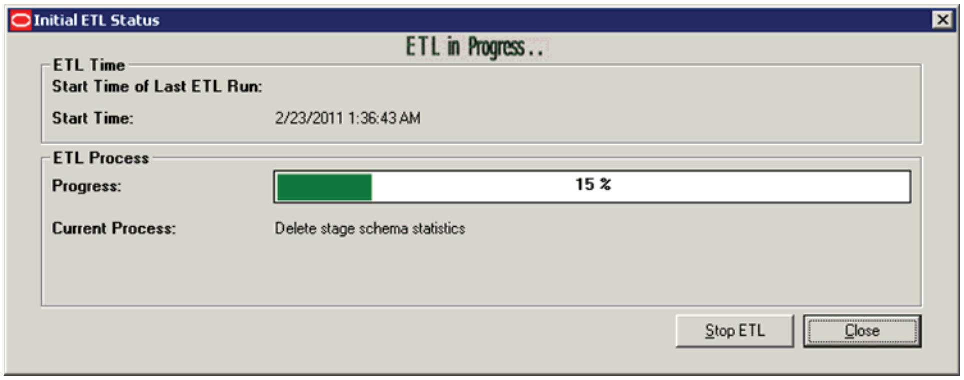


Please confirm that you have already configured the following items.

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 system displays a status dialog box showing the start time of the ETL, the progress bar, and the current process in execution.



Start Time of Last ETL Run:

Start Time: 2/23/2011 1:36:43 AM

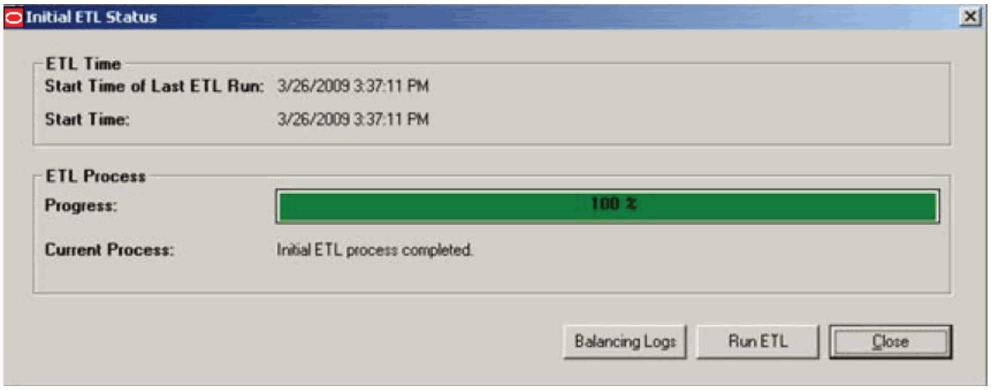
Progress: 15 %

Current Process: Delete stage schema statistics

While the ETL is in progress, you can:

- Click **Close** to close the dialog box and exit from the Schema Creation Tool. Closing the dialog box does not affect the execution of the ETL process.
- Click **Stop ETL** to halt the ETL process. For more information about this option, see Section 5.2.3, "Stopping the Execution of ETL."

The system displays a status message when the initial ETL process is completed.



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM

Start Time: 3/26/2009 3:37:11 PM

Progress: 100 %

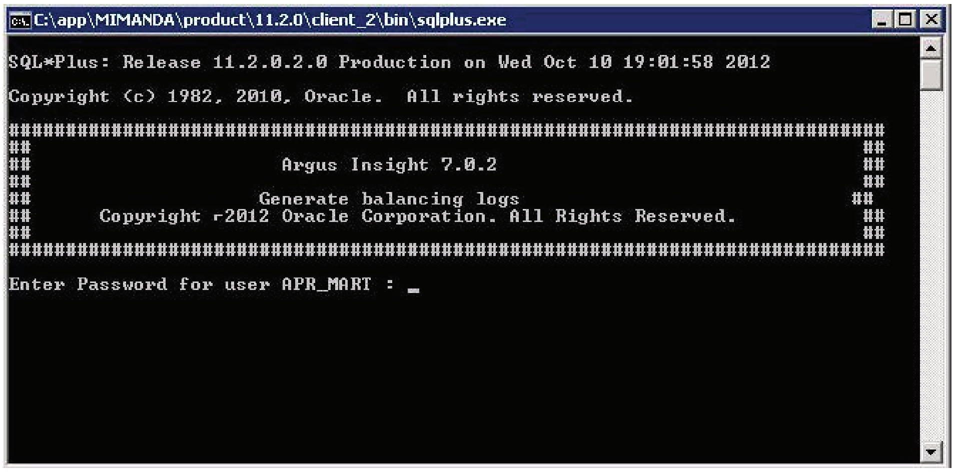
Current Process: Initial ETL process completed.

### 5.2.1 Generating the Balance Logs

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

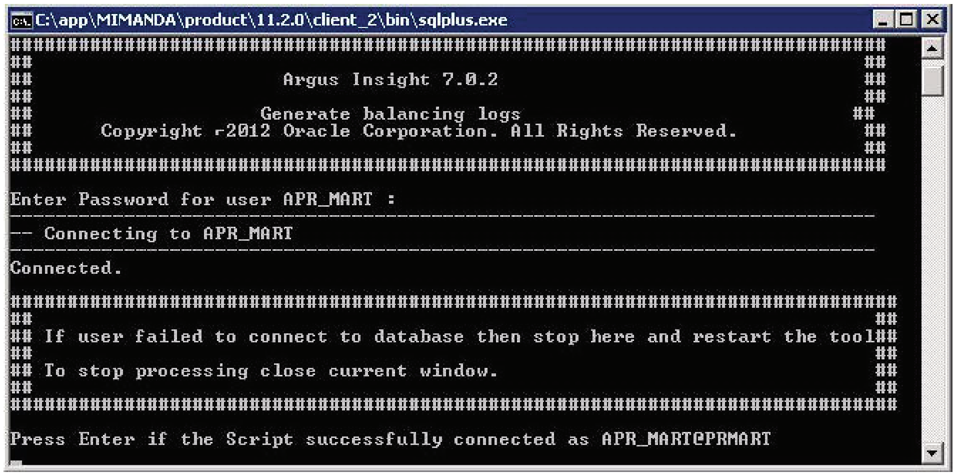
To generate the balance logs:

1. Wait until the system displays the dialog box that reports the initial ETL completed successfully.
2. Click **Balancing Logs.** The system prompts for confirmation that you want to generate balancing logs for the completed Initial ETL.
3. Click **OK**. This displays the following command screen:



```
SQL*Plus: Release 11.2.0.2.0 Production on Wed Oct 10 19:01:58 2012

Copyright (c) 1982, 2010, Oracle.  All rights reserved.

##############################################################################
##                                                                          ##
##                      Argus Insight 7.0.2                                 ##
##                                                                          ##
##                    Generate balancing logs                              ##
##      Copyright r2012 Oracle Corporation. All Rights Reserved.            ##
##                                                                          ##
##############################################################################

Enter Password for user APR_MART : _
```

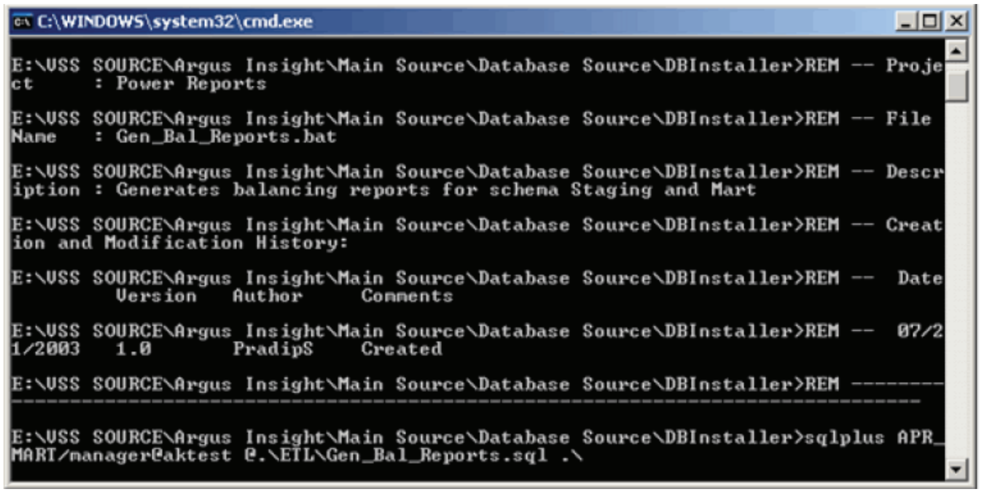
4. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



```
##############################################################################
##                                                                          ##
##                      Argus Insight 7.0.2                                 ##
##                                                                          ##
##                    Generate balancing logs                              ##
##      Copyright r2012 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 that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name> and press **Enter**.

   The system opens a command window and generates the balancing logs.



```
E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM -- Proje
ct      : Power Reports

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM -- File
Name    : Gen_Bal_Reports.bat

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM -- Descr
iption : Generates balancing reports for schema Staging and Mart

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM -- Creat
ion and Modification History:

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM --  Date
         Version   Author      Comments

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM --  07/2
1/2003    1.0        PradipS     Created

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>REM --------
-----------------------------------------------------------------------------

E:\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller>sqlplus APR_
MART/manager@aktest @.\ETL\Gen_Bal_Reports.sql .\
```

When the logs are generated, the system displays a dialog box that lists the location and names of the log files.

6. Click **OK** to close the dialog box.
7. Open and verify the contents of each Balancing Report.

   The Balancing Reports are located in the following folder:

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

   The log files are named:

   - 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

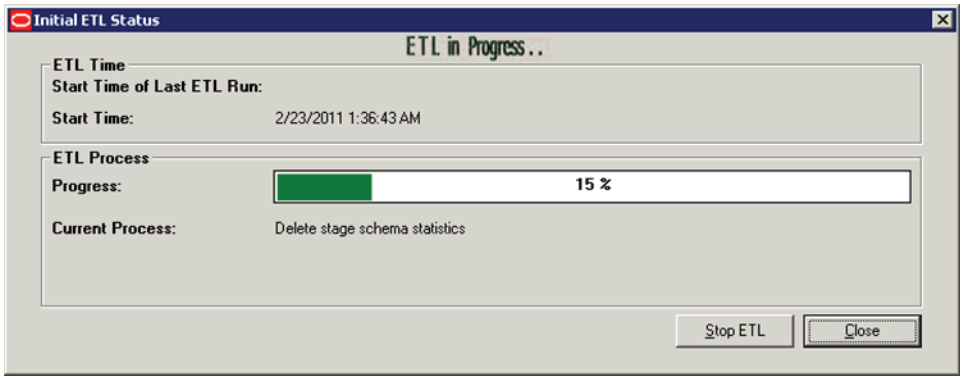
## 5.2.2 Closing the Initial ETL Status Dialog Box

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

1. Click **Close.** The system prompts for confirmation that you want to close the Schema Creation Tool application.
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:

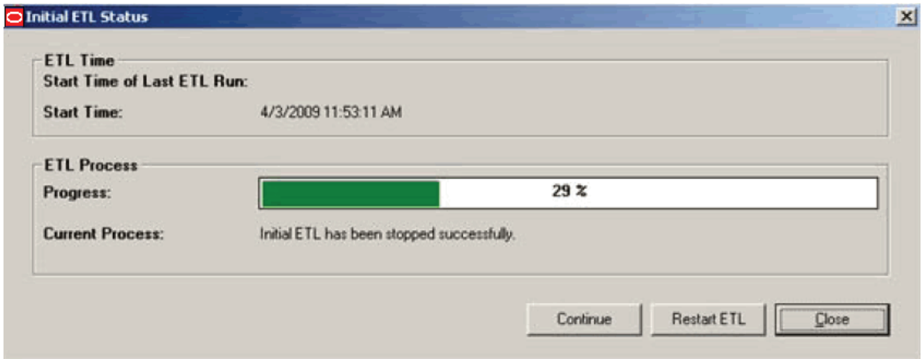
Start Time: 2/23/2011 1:36:43 AM

Progress: 15 %

Current Process: Delete stage schema statistics

To halt the execution of the initial ETL process:

1. Click **Stop ETL.** The system prompts for confirmation that you want to stop the ETL currently in progress.
2. Click **OK.** The system halts the ETL process and returns to the Initial ETL Status dialog box:



Start Time of Last ETL Run:

Start Time: 4/3/2009 11:53:11 AM

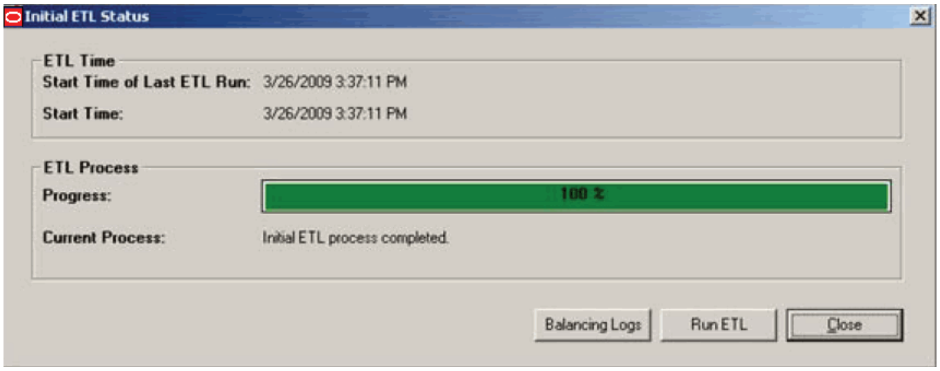
Progress: 29 %

Current Process: Initial ETL has been stopped successfully.

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



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM

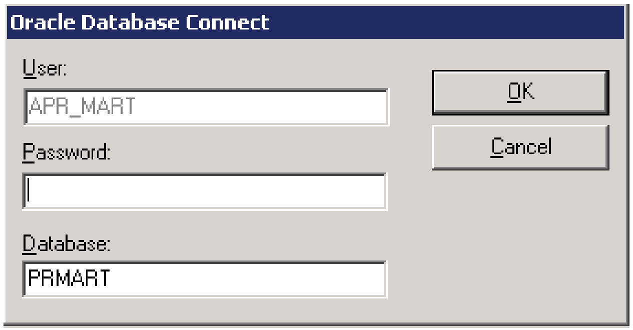
Start Time: 3/26/2009 3:37:11 PM

Progress: 100 %

Current Process: Initial ETL process completed.

To start the ETL process from the beginning:

1. Click **Run ETL.** The system prompts for confirmation that you want to start the initial ETL from the beginning?
2. Click **OK.** The Oracle Database Connect dialog box opens.



User: APR_MART

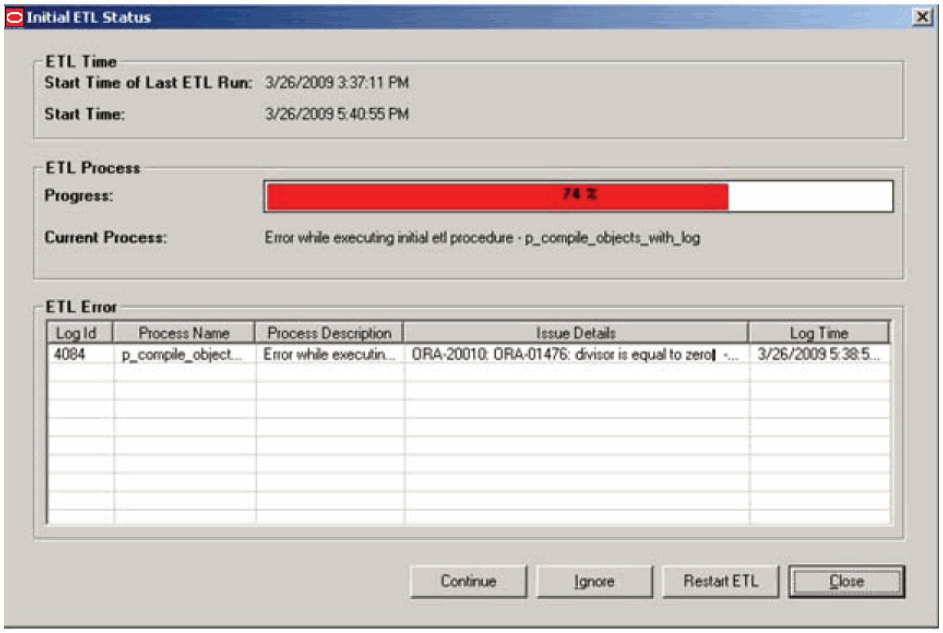
Password:

Database: PRMART

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: 3/26/2009 3:37:11 PM
Start Time: 3/26/2009 5:40:55 PM
Progress: 74 %
Current Process: Error while executing initial etl procedure - p_compile_objects_with_log

| Log Id | Process Name | Process Description | Issue Details | Log Time |
|---|---|---|---|---|
| 4084 | p_compile_object... | Error while executin... | ORA-20010: ORA-01476: divisor is equal to zero -... | 3/26/2009 5:38:5... |

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

- Click **Continue** to continue the failed Initial ETL process.
- Click **Ignore** to ignore the failed Initial ETL process.
- Click **Modify Attributes** of ETL Data Exclusion if PRE_REQ_CHECK_FLAG switch is set to ABORT.

---

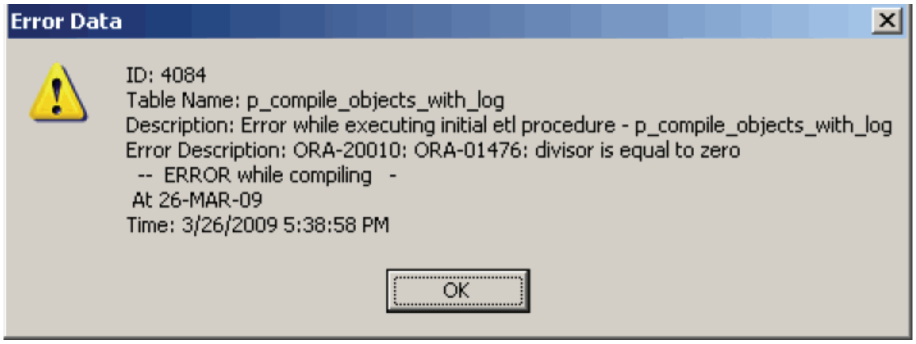
**Note:** These modifications must be done before running the Initial ETL process.

---

### 5.4.1 Continuing the Failed Initial ETL Process

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

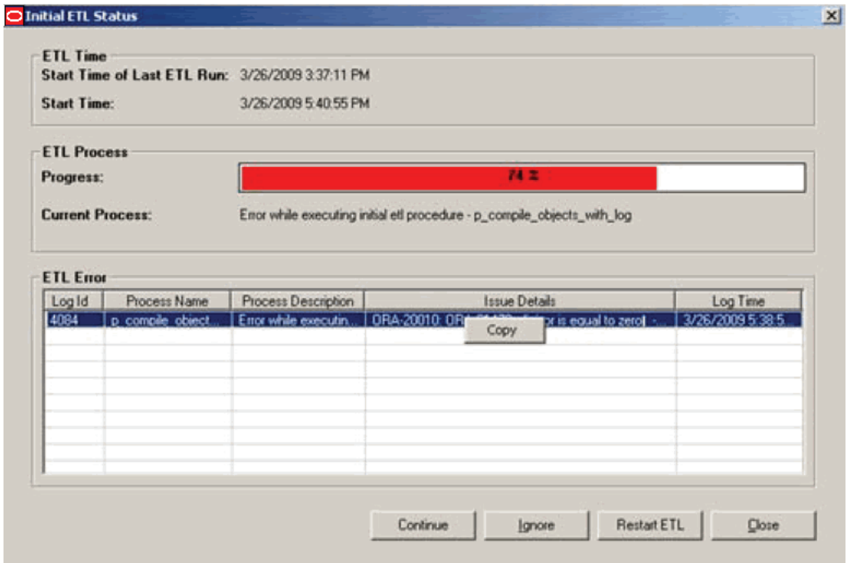
1. Double-click on the ETL error. The system opens a dialog box that contains details of the error.



ID: 4084
Table Name: p_compile_objects_with_log
Description: Error while executing initial etl procedure - p_compile_objects_with_log
Error Description: ORA-20010: ORA-01476: divisor is equal to zero
-- ERROR while compiling -
At 26-MAR-09
Time: 3/26/2009 5:38:58 PM

2. Review the error information, and then click **OK.**

3. Right-click on the ETL Error, and click **Copy** to copy the error data.



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM

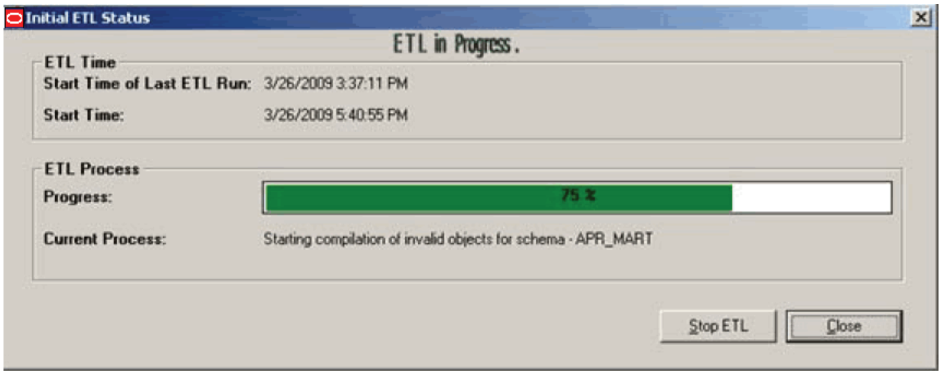
Start Time: 3/26/2009 5:40:55 PM

Progress: 74 %

Current Process: Error while executing initial etl procedure - p_compile_objects_with_log

| Log Id | Process Name | Process Description | Issue Details | Log Time |
|---|---|---|---|---|
| 4084 | p_compile_object... | Error while executin... | ORA-20010: OR r is equal to zero - ... | 3/26/2009 5:38:5... |

4. Click **Continue** to continue the failed ETL process. The system prompts for confirmation that you want to start the initial ETL from the stopped process.
5. Click **OK.** The system continues with the ETL process (if no errors are found).



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM

Start Time: 3/26/2009 5:40:55 PM

Progress: 75 %

Current Process: Starting compilation of invalid objects for schema - APR_MART

## 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. The system prompts for confirmation that you want to skip the failed process and continue executing the Initial ETL with the next process.
2. Click **OK.** The system starts the Initial ETL from the next process and continues with the ETL process (if no errors are found).

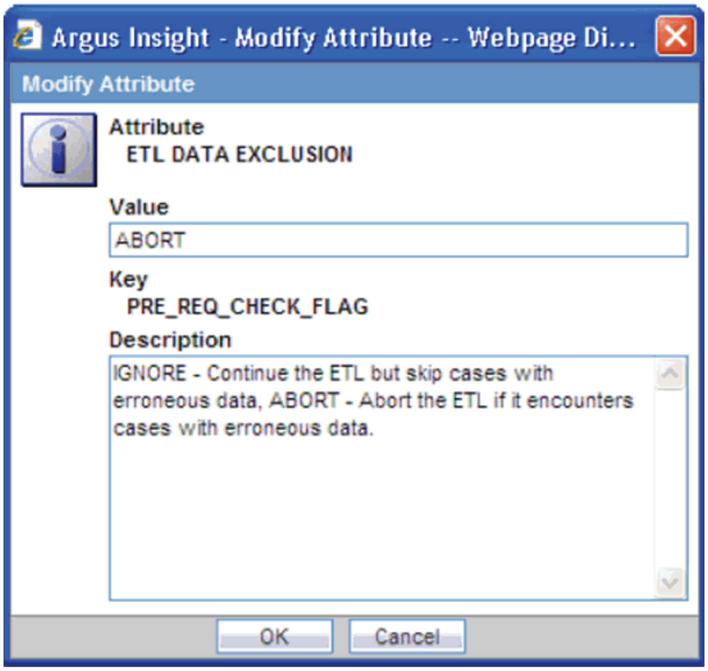
## 5.4.3 Modifying the Attributes of ETL Data Exclusion

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. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page to open the ADMINISTRATION TOOLS page.

3. Click the **List Maintenance** tab.
4. Select **Profile Switches** from the List Maintenance Items group. The system updates the Attributes group with the profile switches you can modify.
5. Select **ETL Data Exclusion** and click **Modify.** The following Modify Attribute dialog box opens:



Attribute
ETL DATA EXCLUSION

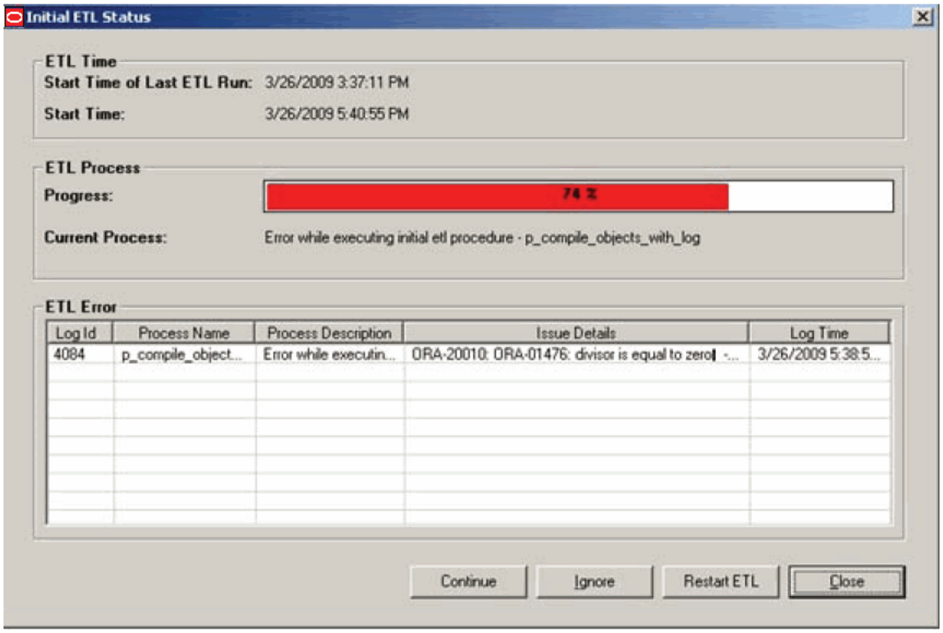
Value
ABORT

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 your changes and return to the List Maintenance tab.

## 5.5 Restarting the Initial ETL Process



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM

Start Time: 3/26/2009 5:40:55 PM

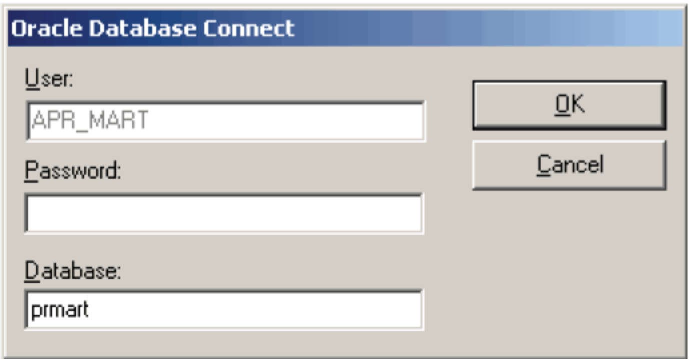
Progress: 74 %

Current Process: Error while executing initial etl procedure - p_compile_objects_with_log

| Log Id | Process Name | Process Description | Issue Details | Log Time |
|---|---|---|---|---|
| 4084 | p_compile_object... | Error while executin... | ORA-20010: ORA-01476: divisor is equal to zero -... | 3/26/2009 5:38:5... |

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

1. Click **Restart ETL.** The system prompts for confirmation that you want to start the initial ETL from the beginning.
2. Click **OK.** The Oracle Database Connect dialog box opens.

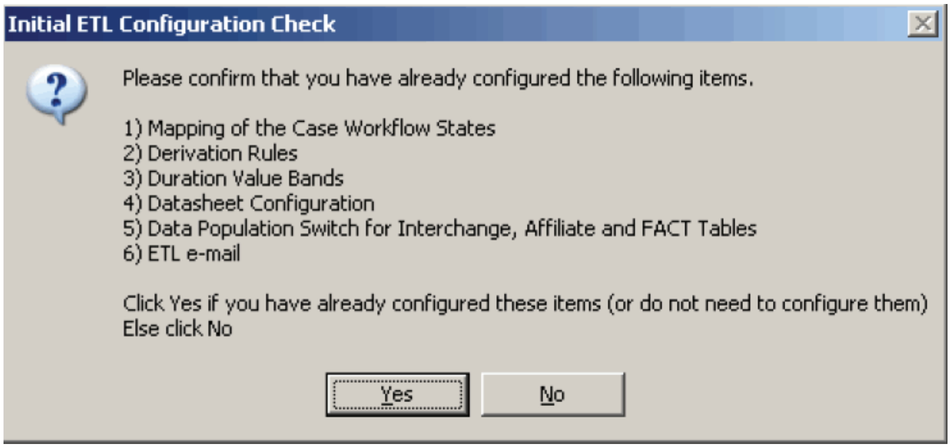


User: APR_MART

Password:

Database: prmart

3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the APR_MART user.
   b. In the **Database** field, type 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. The system prompts for confirmation that you have completed the required configuration steps.

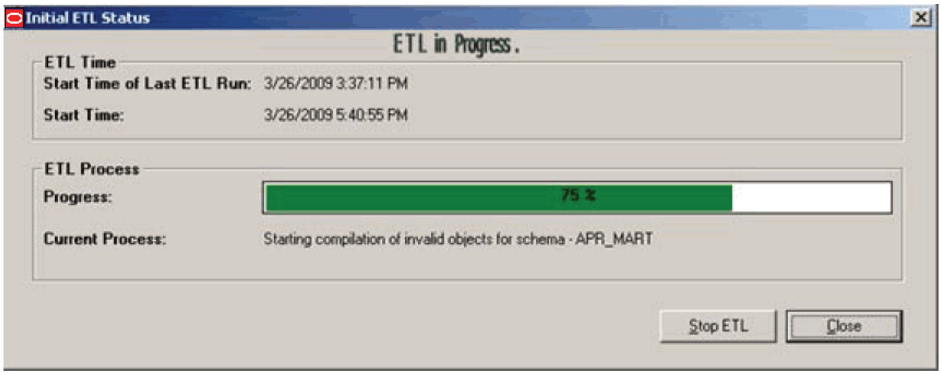


Please confirm that you have already configured the following items.

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

5. Click **Yes** if these items have already been configured. The system displays a status dialog box showing the start time of the ETL, the progress bar, and the current process in execution:



Start Time of Last ETL Run: 3/26/2009 3:37:11 PM
Start Time: 3/26/2009 5:40:55 PM
Progress: 75 %
Current Process: Starting compilation of invalid objects for schema - APR_MART

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

# 6

# Configuring the Cognos 8 Environment

This chapter describes how to configure the Cognos 8 environment. You must configure the Cognos 8 environment in the order specified in this guide.

This chapter includes the following topics:

- Upgrading Cognos Server for Argus Insight 7.0.2
- Setting Up Cognos Server and Configuration for New Installation

If you are using BusinessObjects XI instead of Cognos 8, see Chapter 7 for information about configuring the BusinessObjects environment for Argus Insight.

Before attempting to configure the environment, verify that you have installed all required hardware and software. For more information, see Section 1.2, "Software and Hardware Requirements."

## 6.1 Upgrading Cognos Server for Argus Insight 7.0.2

This section describes the following tasks that you must complete if you are upgrading your Cognos Server for Argus Insight 7.0.2:

- Configuring Custom Java Authentication
- Deleting Folders and Reports
- Importing the Content Repository for an Upgrade

### 6.1.1 Configuring Custom Java Authentication

To configure custom Java authentication:

1. Go to IBM Cognos Administration and stop the Cognos services.
2. Navigate to the following folder:

   \\*Cognos_Server**Argus_Insight_Install_Path*\Java Authentication\JDBC_PowerReports
3. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from that folder to the following location on the Cognos 8 Server:

   \\*Cognos_8_Install_Path*\ c8\webapps\p2pd\WEB-INF\lib
4. Define the configuration parameters:
   a. Navigate to the following folder:

      \\*Cognos_8_Install_Path*\ c8\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. |

d. Save and close the file.

5. Navigate to the following folder:

   Program Files\cognos\c8\bin\jre\1.5.0\lib\security

6. Backup the following two JAR files:
   - local_policy.jar
   - US_export_policy.jar
7. Go to the following URL:

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   **Note:** You will need the user ID and password from IBM Cognos to download the files required in next step.

8. Log in to the IBM site.
9. Select the **Unrestricted JCE Policy files for SDK for all newer versions (1.4.2+)** option and click **Continue.**
10. Click **I agree** to agree to the license terms and then check **I confirm.**
11. Click the **Download Now** link.
12. Download the files and extract into a folder.
13. Locate the following two JAR files in the extract folder:
    - local_policy.jar
    - US_export_policy.jar
14. Copy those jar files into the following folder:

    Program Files\cognos\c8\bin\jre\1.5.0\lib\security

15. Go to IBM Cognos Administration and restart the Cognos services.

### 6.1.2 Deleting Folders and Reports

**Note:** The standard reports of Argus Insight 7.0.1 can be integrated with Argus Insight 7.0.2.

If you are upgrading from Argus Insight 7.0.1 to Argus Insight 7.0.2, you may want to delete folders and reports that are no longer supported out of the box.

You can delete all the reports except the reports listed in the following table:

*Table 6–1 Reports for Argus Insight 7.0.2*

| Report Name | Folder/Category |
|---|---|
| Detailed Line Listing by Case Number | General |
| SAE Clinical Trial Detail Listing | General |
| SAE Clinical Trial Narratives | General |
| Quick Signal | Pharmacovigilance |
| Study Reconciliation Report | General |

You can also delete all  empty subfolders of the Argus Insight folder.

### 6.1.3 Importing the Content Repository for an Upgrade

Execute the following steps to import the Content Repository for an upgrade:

1. Copy the **ContentStore.zip** file from the location mentioned below:

   \\Cognos_ 8_Server_Name\Argus_Insight_Install_Path\Cognos 8\Contentstore

2. Paste the file to the following location on the Cognos 8 Server:

   \\Cognos_8_Install_Path\ c8\Deployment

3. Skip to Section 6.2.6, "Importing the Content Repository" to complete the final steps for the upgrade.

## 6.2 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.

If you are upgrading from Argus Insight 7.0.1, see Section 6.1, "Upgrading Cognos Server for Argus Insight 7.0.2" for the installation procedures.

### 6.2.1 Configuring IIS 7.0 on the Cognos 8 Server

This section describes the following tasks that you must complete to configure Internet Information Services 7.0 (IIS 7.0) on the Cognos 8 Server:

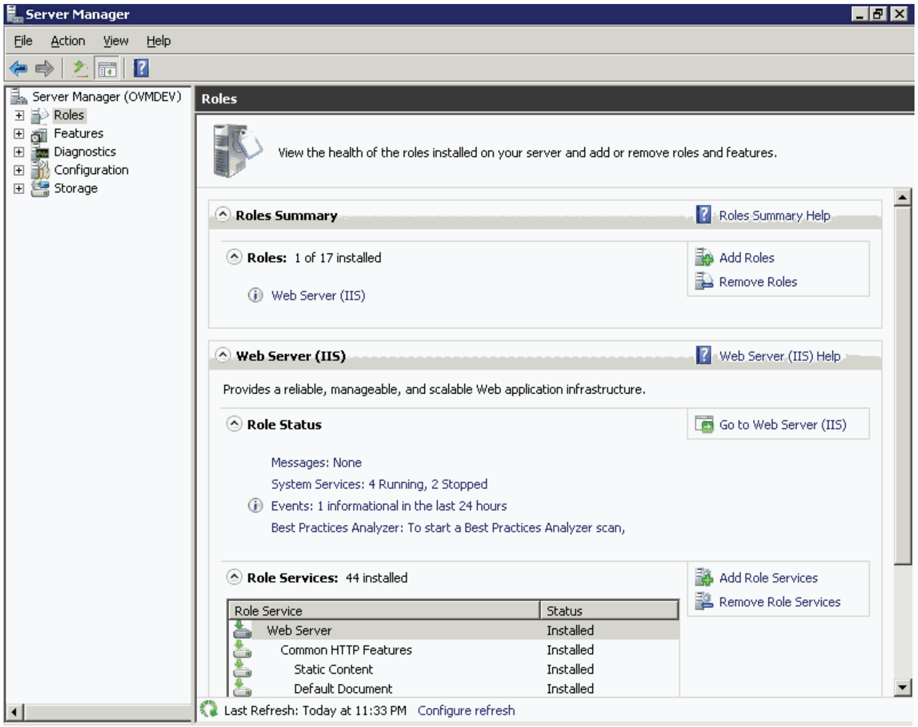
- Checking that CGI or ISAPI Is Enabled in IIS
- Creating the Cognos 8 Virtual Directories
- Editing ISAPI or CGI Extensions
- Adding the Module Mapping
- Editing the Module Mapping
- Allowing CGI Application to Use Execute

#### 6.2.1.1 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 window opens.



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.

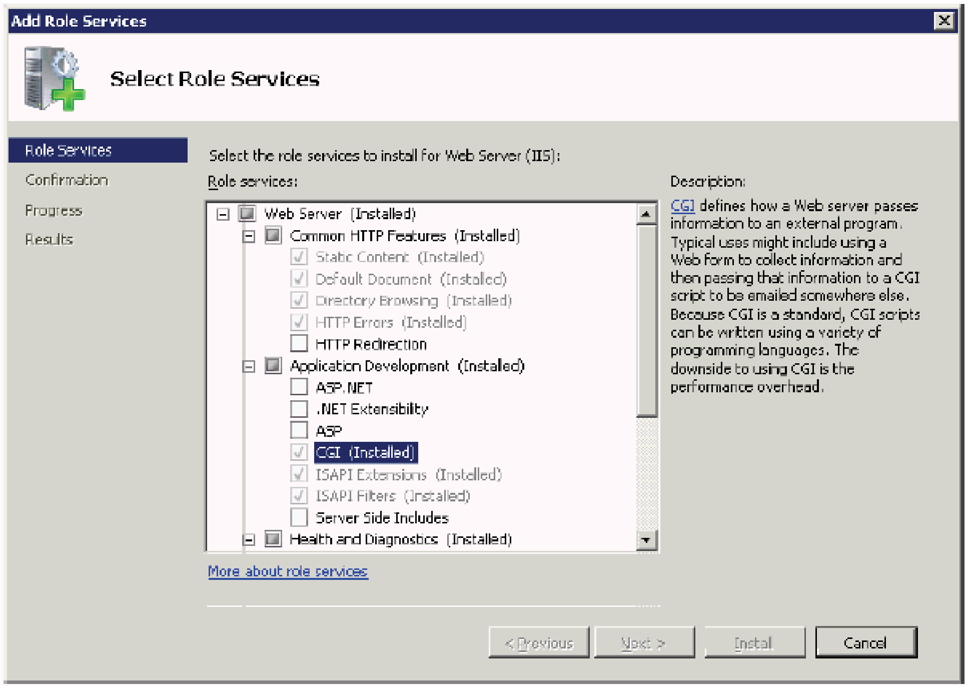
Messages: None
System Services: 4 Running, 2 Stopped
Events: 1 informational in the last 24 hours
Best Practices Analyzer: To start a Best Practices Analyzer scan,

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. Click the **Add Role Services** link to the right of the Role Services section. The Add Role Services dialog box opens.



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).**

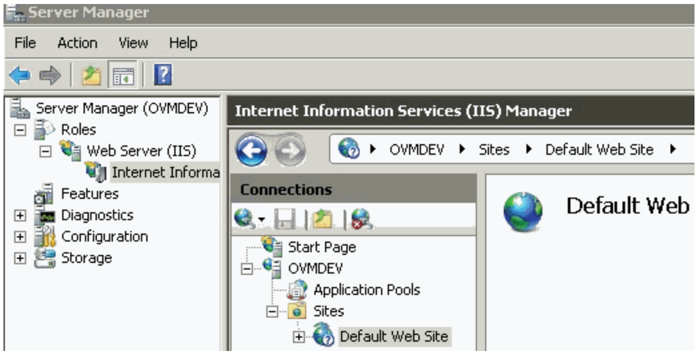
5. Verify that the CGI and ISAPI Extensions are listed as **(Installed).**

- 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 window.

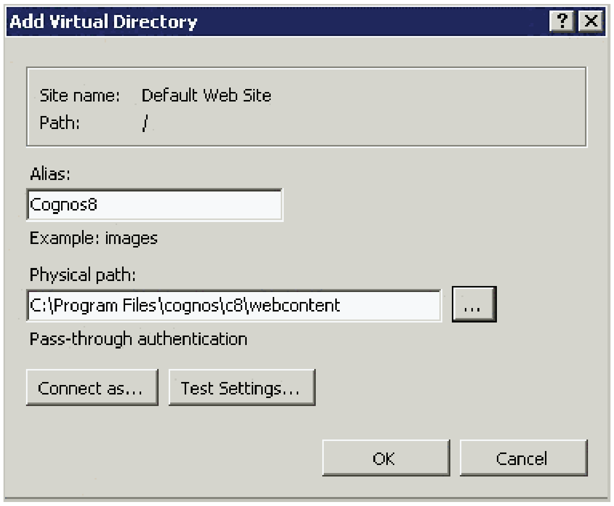
### 6.2.1.2 Creating the Cognos 8 Virtual Directories

To create the Cognos 8 virtual directories:

1. Navigate to **Roles, Web Server (IIS),** and select **Internet Information Services (IIS) Manager.**
2. Expand the server node in the Connections pane.
3. Expand **Sites.**



4. Right-click **Default Web Site,** and select **Add Virtual Directory.** The Add Virtual Directory dialog box opens.



Site name: Default Web Site
Path: /
Alias: Cognos8
Physical path: C:\Program Files\cognos\c8\webcontent

   a. In the **Alias** field, enter **Cognos 8.**
   b. In the **Physical path** field, enter the complete path to the Cognos 8 Web content directory. The default path is:

      *drive:*\Program Files\cognos\c8\webcontent

   c. Click **OK.**

5. Right-click your newly-created Cognos 8 virtual directory and select **Add Virtual Directory.** The Add Virtual Directory dialog box opens.

a. In the **Alias** field, enter **cgi-bin.**

b. In the **Physical path** field, enter the complete path to the Cognos 8 cgi-bin directory. The default path is:

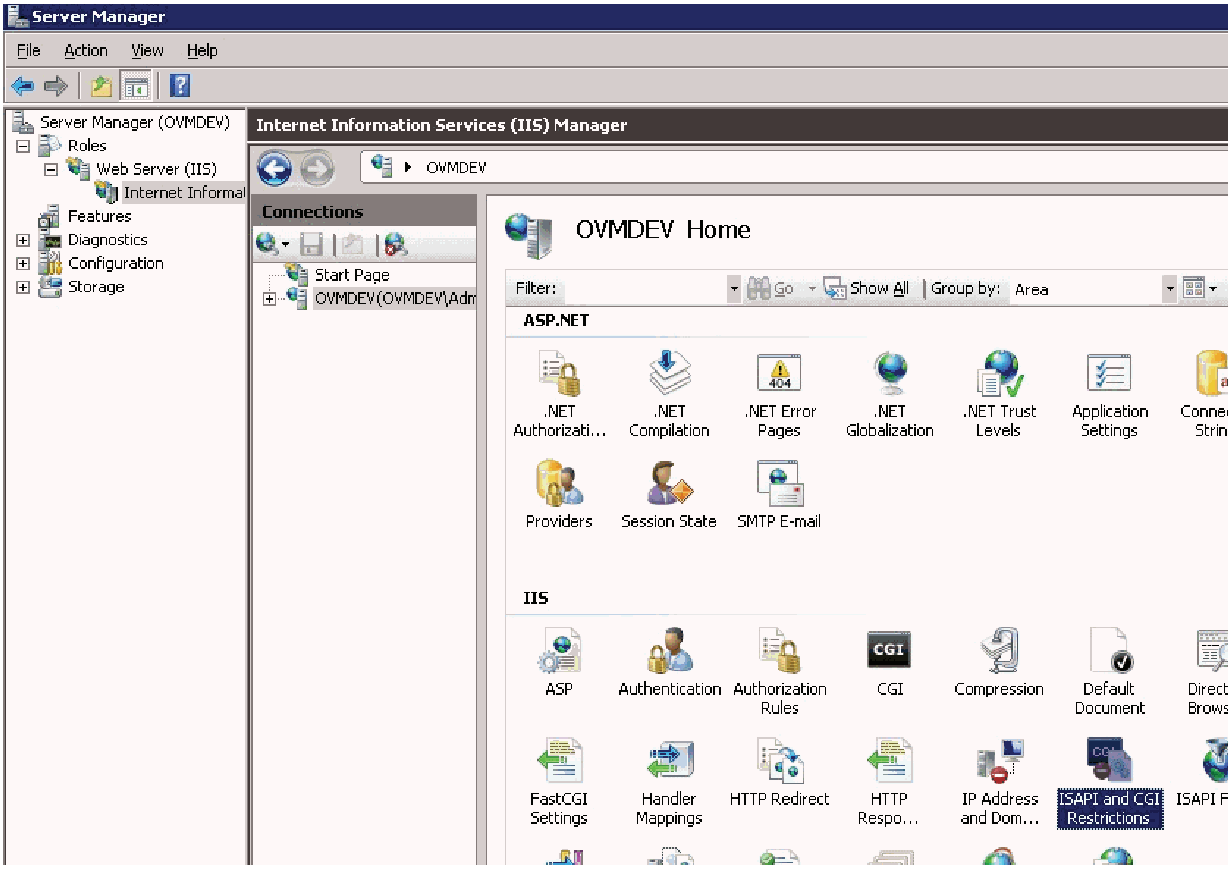
   *drive:*\Program Files\cognos\c8\cgi-bin

c. Click **OK.**

### 6.2.1.3 Editing ISAPI or CGI Extensions

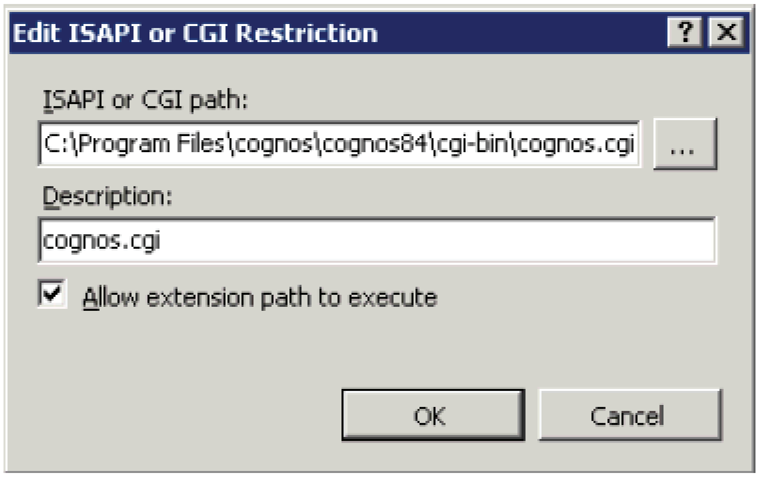
To edit the ISAPI or CGI extensions:

1. Select the server node in the Connections pane.



2. Double-click the **ISAPI and CGI Restrictions** icon.

3. Click the **Add** link in the Actions pane. The Edit ISAPI or CGI Restriction dialog box opens.



C:\Program Files\cognos\cognos84\cgi-bin\cognos.cgi

cognos.cgi

☑ 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\cognos\c8\cgi-bin\cognosisapi.dll

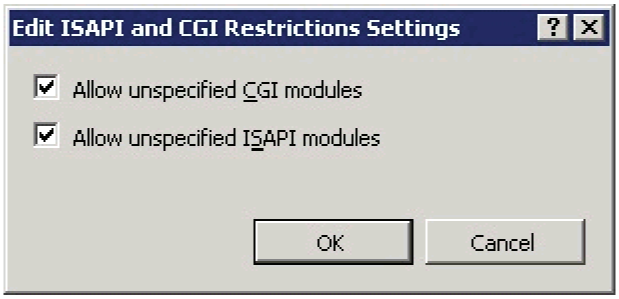
*drive:*\Program Files\cognos\c8\cgi-bin\cognos.cgi

b. Select the **Allow extension path to execute** check box.

c. Click **OK.**

### Alternative Method

1. Select the server node in the Connections pane.
2. Double-click the **ISAPI and CGI Restrictions** icon.
3. Click the **Edit Feature Settings** link in the Actions pane. The Edit ISAPI and CGI Restriction Settings dialog box opens.



☑ Allow unspecified CGI modules

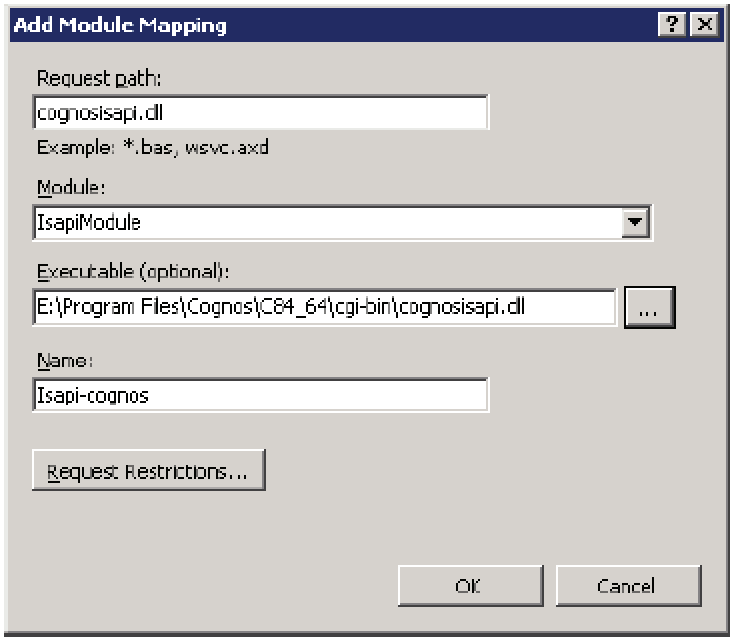
☑ Allow unspecified ISAPI modules

4. Select the **Allow unspecified CGI Modules** check box.
5. Click **OK.**

### 6.2.1.4 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 the **cgi-bin** virtual directory.
3. Double-click the **Handler Mappings** icon.
4. Click the **Add Module Mapping** link in the Actions pane. The Add Module Mapping dialog box opens.



Request path: cognosisapi.dll

Module: IsapiModule

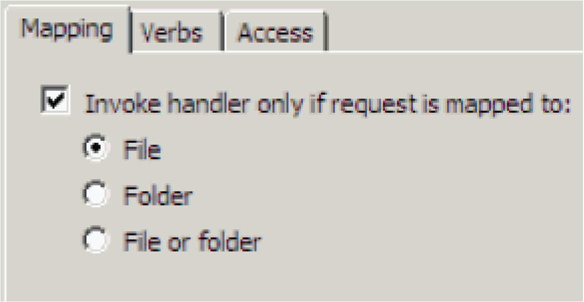
Executable (optional): E:\Program Files\Cognos\C84_64\cgi-bin\cognosisapi.dll

Name: Isapi-cognos

   a. In the **Request path** field, enter either *.cgi or *.dll depending on which one you need.
   b. In the **Module** field, select either **CGIModule** or **IsapiModule** from the list.
   c. In the **Executable** field, you enter a value depending on the module you are using.

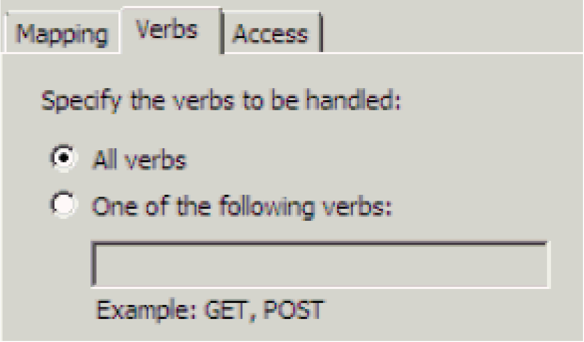
      If you are using an ISAPI Module, you must enter the complete path to the cognosisapi.dll. You can click the ellipsis icon to browse to the file location.

      If you are using a CGI Module, you do not need to enter a value into 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.**



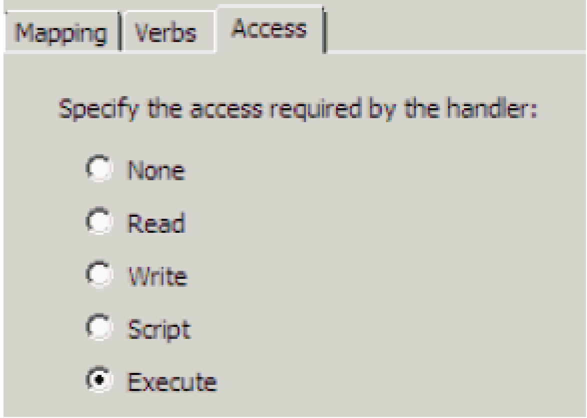
☑ Invoke handler only if request is mapped to:
● File
○ Folder
○ File or folder

b. Click the **Verbs** tab, and select **All verbs.**



Specify the verbs to be handled:
● All verbs
○ One of the following verbs:
Example: GET, POST

c. Click the **Access** tab, and select **Specify the access required by the handler: Execute.**

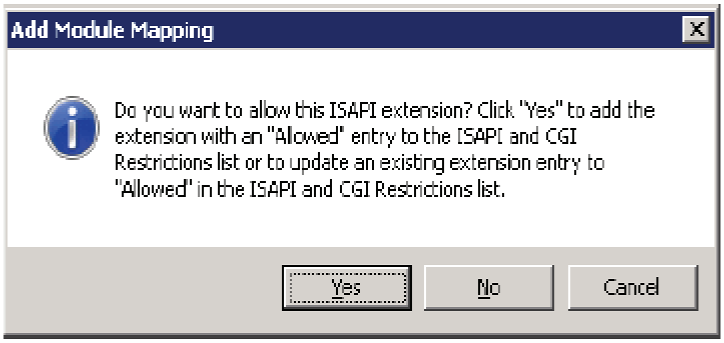


Specify the access required by the handler:
○ None
○ Read
○ Write
○ Script
● Execute

d. Click **OK** to save your changes. The system returns to the Add Module Mapping dialog box.

6. Click **OK.**

Depending on the method used in Section 6.2.1.3, "Editing ISAPI or CGI Extensions," the system may display the following message:



Add Module Mapping

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.** Your new module mapping should be added to the Module Mapping List.

### 6.2.1.5 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 6.2.1.4, "Adding the Module Mapping").

To edit the module mapping:

1. Navigate to the following folder:

   *COGNOS_HOME*/c8/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 depending on whether you are using CGI or ISAPI.

   **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\Cognos\C84_64\
   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:**

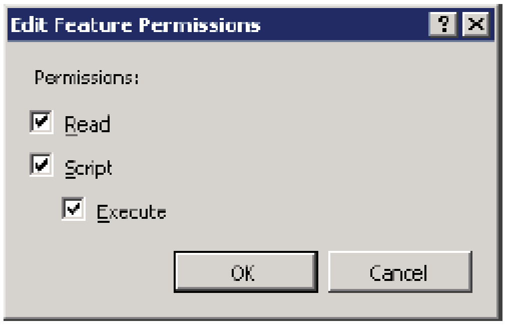
   ```
   <add name="ISAPI-Cognos" path="cognosisapi.dll" verb="*"
   modules="IsapiModule" scriptProcessor="E:\Program Files\Cognos\C84_64\
   cgi-bin\cognosisapi.dll" resourceType="Unspecified"
   requireAccess="Execute" preCondition="bitness32" allowPathInfo="true"/>
   ```

5. Save your changes and close the web.config file.

#### 6.2.1.6 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** virtual directory.
3. Double-click the **Handler Mappings** icon.
4. Click the **Edit Feature Permissions** link in the Actions pane. The Edit Features Permissions dialog box opens.



Permissions:

☑ Read

☑ Script

☑ Execute

5. Select the **Execute** check box.
6. Click **OK.**

### 6.2.2 Configuring the Java Database Components

To configure the Java Database Components (JDBC) in the Cognos 8 environment:

1. Navigate to the following Oracle installation path:

   *Oracle_Installation_Path*\product\*Oracle_Version*\client_1\sqldeveloper\jdbc\lib

2. Copy the **ojdbc5.jar** file to the following location on the Cognos 8 environment:

   *Cognos_Installation_Path*\c8\webapps\p2pd\web-inf\lib

### 6.2.3 Copying the Authentication Settings for Report Writer

To copy the authentication settings for Report Writer:

1. Navigate to the following location on the Argus Insight Web Server:

   \\*Argus_Insight_Installation_Path*\ArgusInsight\ASP\Reports

2. Copy the PR.asp file to the following location on the Cognos 8 Server:

   \\*Cognos_8_Installation*\cognos\c8\cgi-bin

### 6.2.4 Configuring Custom Java Authentication

To configure custom Java authentication:

1. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from this location:

   \\*Cognos_Server*\*Argus_Insight_Install_Path*\Java Authentication\JDBC_PowerReports

   To this location on the Cognos 8 Server:

   \\*Cognos_8_Install_Path*\ c8\webapps\p2pd\WEB-INF\lib

2. Copy the **JDBC_Config_PowerReports.properties** file from this location:

   \\*Cognos_Server**Argus_Insight_Install_Path*\Java Authentication\JDBC_PowerReports

   To this location on the Cognos 8 Server:

   \\*Cognos_8_Install_Path*\ c8\Configuration

3. Define the configuration parameters:

   a. Go to the Cognos Server.

   b. Open the JDBC_Config_PowerReports.properties file for editing.

   c. Modify the existing values of the following parameters:

   | 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. |

   d. Save and close the file.

4. Copy the **ContentStore.zip** file from this location:

   \\*Cognos_ 8_Server_Name**Argus_Insight_Install_Path*\Cognos 8\Contentstore

   To this location on the Cognos 8 Server:

   \\*Cognos_8_Install_Path*\ c8\Deployment

5. Navigate to the following folder:

   Program Files\cognos\c8\bin\jre\1.5.0\lib\security

6. Backup the following two JAR files:

   - local_policy.jar
   - US_export_policy.jar

7. Go to the following URL:

   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk

   > **Note:** You will need the user ID and password from IBM Cognos to download the files required in next step.

8. Log in to the IBM site.

9. Select the **Unrestricted JCE Policy files for SDK for all newer versions (1.4.2+)** option and click **Continue.**

10. Click **I agree** to agree to the license terms and then check **I confirm.**

11. Click the **Download Now** link.

12. Download the files and extract into a folder.

13. Locate the following two JAR files in the extract folder:

    - local_policy.jar

  - US_export_policy.jar

14. Copy those jar files into the following folder:

    Program Files\cognos\c8\bin\jre\1.5.0\lib\security

### 6.2.5 Configuring the Cognos 8 Environment

This section describes the following tasks that you must complete to configure the Cognos 8 environment:

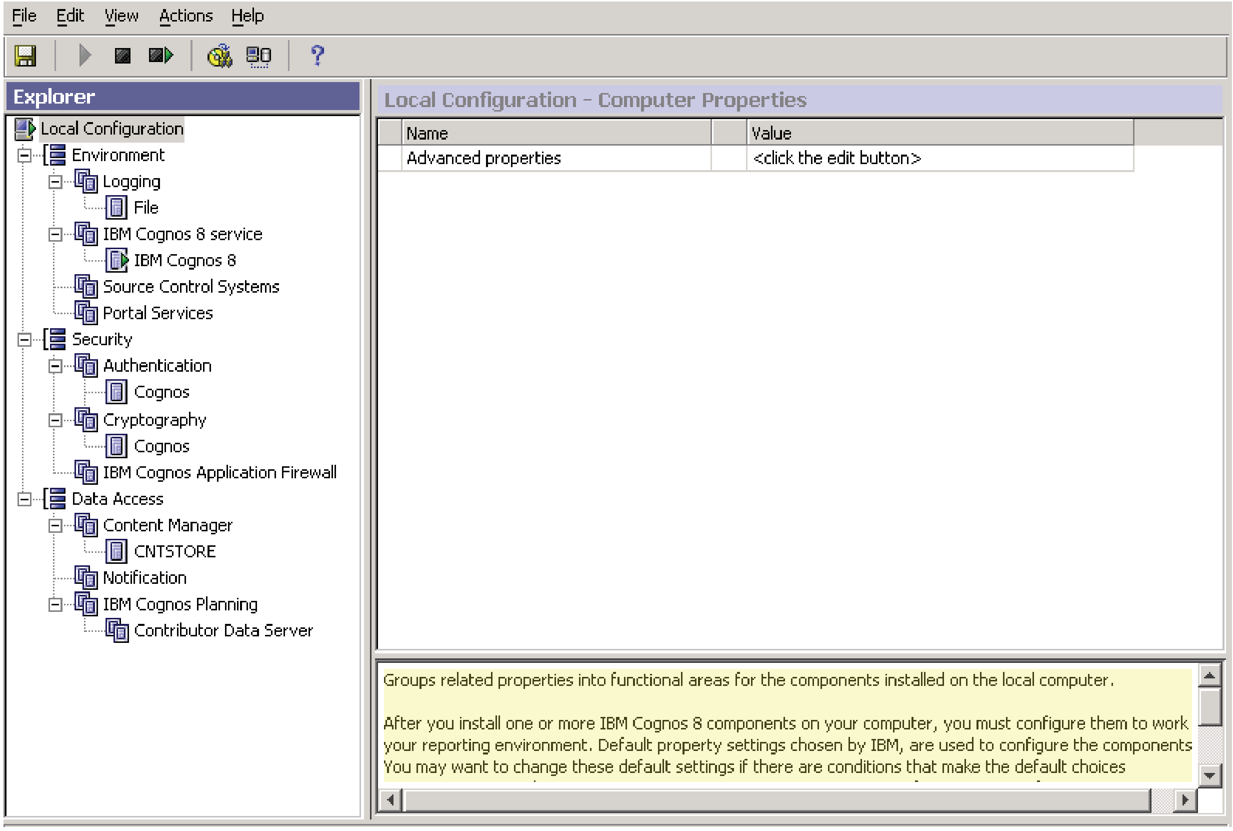
- Opening the IBM Cognos 8 Configuration Window
- Setting the Environment Properties for Cognos 8
- Setting the Security Properties for Cognos 8
- Setting the Data Access Properties for Cognos 8
- Creating the Namespace for Argus Insight Authentication
- Saving Your Configuration and Starting the Cognos 8 Service

#### 6.2.5.1 Opening the IBM Cognos 8 Configuration Window

You use the options in the IBM Cognos 8 Configuration window to define environment group and logging properties, security properties, and data access properties.

To open the IBM Cognos 8 Configuration window:

1. Click **Start.**
2. Navigate to **All Programs, IBM Cognos 8,** and then select **IBM Cognos Configuration.** The IBM Cognos Configuration window opens.



| 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 8 components on your computer, you must configure them to work your reporting environment. Default property settings chosen by IBM, are used to configure the components You may want to change these default settings if there are conditions that make the default choices

---

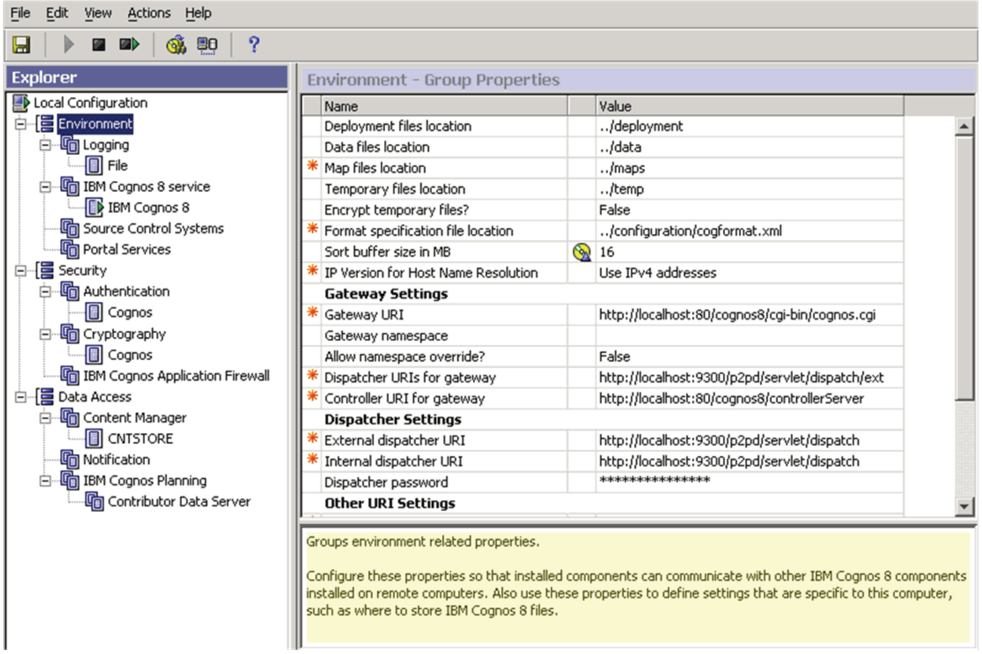
**Note:** The windows displayed during the Cognos 8 configuration are labeled either IBM Cognos 8 or Cognos 8. Both labels refer to the same Cognos configuration.

---

### 6.2.5.2 Setting the Environment Properties for Cognos 8

To define the environment group properties and the environment logging properties:

1. Open the IBM Cognos 8 Configuration window.
2. Select **Environment.** The system displays the Environment - Group Properties in the right pane.



Environment - Group Properties

| Name | Value |
|---|---|
| Deployment files location | ../deployment |
| Data files location | ../data |
| * Map files location | ../maps |
| Temporary files location | ../temp |
| Encrypt temporary files? | False |
| * Format specification file location | ../configuration/cogformat.xml |
| Sort buffer size in MB | 16 |
| * IP Version for Host Name Resolution | Use IPv4 addresses |
| **Gateway Settings** | |
| * Gateway URI | http://localhost:80/cognos8/cgi-bin/cognos.cgi |
| Gateway namespace | |
| Allow namespace override? | False |
| * Dispatcher URIs for gateway | http://localhost:9300/p2pd/servlet/dispatch/ext |
| * Controller URI for gateway | http://localhost:80/cognos8/controllerServer |
| **Dispatcher Settings** | |
| * External dispatcher URI | http://localhost:9300/p2pd/servlet/dispatch |
| * Internal dispatcher URI | http://localhost:9300/p2pd/servlet/dispatch |
| Dispatcher password | *************** |
| **Other URI Settings** | |

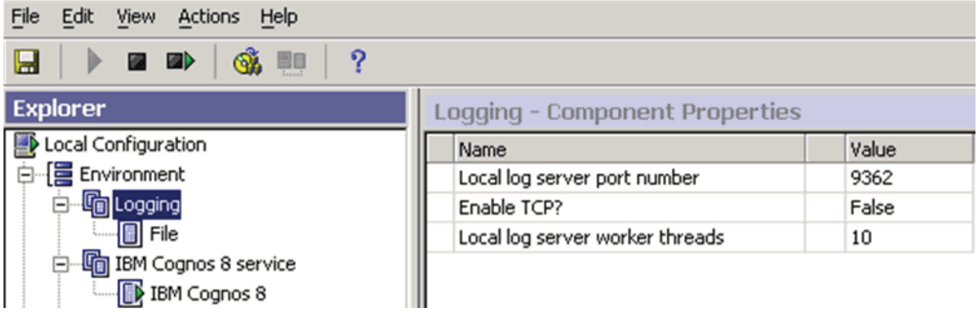
Groups environment related properties.

Configure these properties so that installed components can communicate with other IBM Cognos 8 components installed on remote computers. Also use these properties to define settings that are specific to this computer, such as where to store IBM Cognos 8 files.

3. Set the following environment properties to the required value:

| Environment Property | Required Value |
|---|---|
| Sort buffer size in MB | 16 |
| Gateway URI | http://localhost:80/cognos8/cgi-bin/cognos.cgi |
| Dispatcher URIs for gateway | http://localhost:9300/p2pd/servlet/dispatch/ext |
| Controller URI for gateway | http://localhost:80/cognos8/controllerServer |
| External dispatcher URI | http://localhost:9300/p2pd/servlet/dispatch |
| Internal dispatcher URI | http://localhost:9300/p2pd/servlet/dispatch |
| Content Manager URIs | http://localhost:9300/p2pd/servlet |
| Dispatcher URI for external applications | http://localhost:9300/p2pd/servlet/dispatch |

4. Navigate to **Environment** and select **Logging.** The system displays the properties for the Logging component.



Logging - Component Properties

| Name | Value |
|---|---|
| Local log server port number | 9362 |
| Enable TCP? | False |
| Local log server worker threads | 10 |

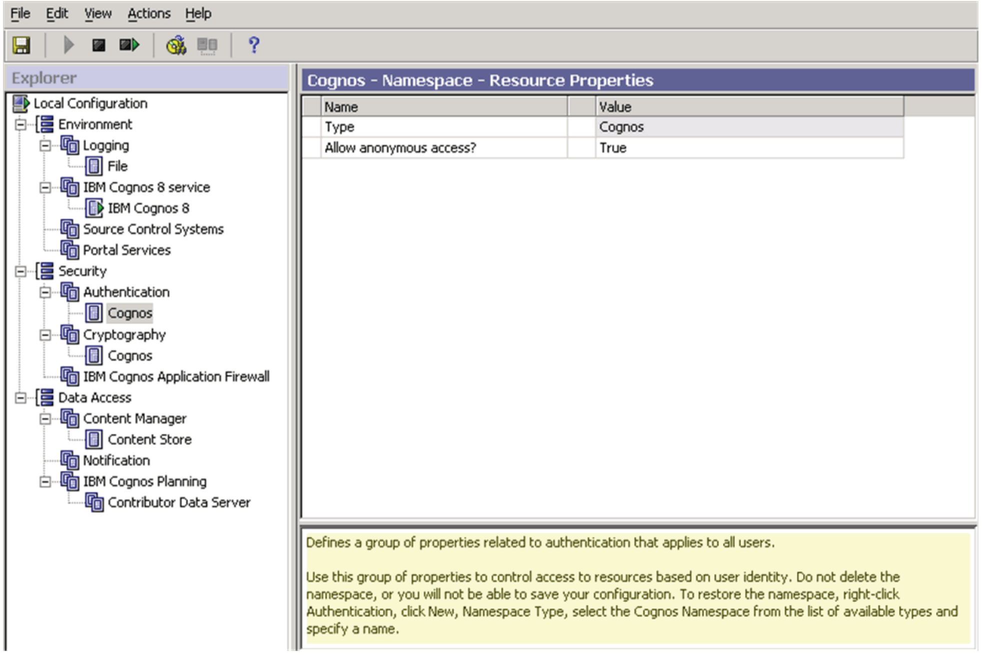
5. Set the following logging properties to the required value:

| Logging Property | Required Value |
|---|---|
| Local log server port number | 9362 |
| Enable TCP? | False |
| Local log server worker threads | 10 |

### 6.2.5.3 Setting the Security Properties for Cognos 8

To define the security properties:

1. Open the IBM Cognos 8 Configuration window.
2. Navigate to **Security, Authentication,** and select **Cognos.**



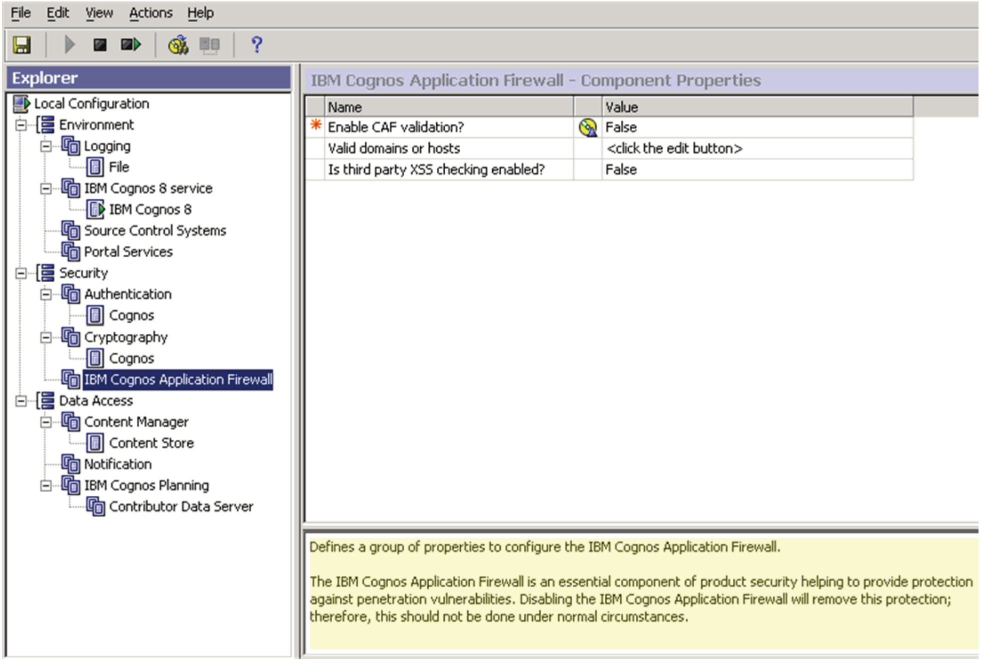
Cognos - Namespace - Resource Properties

| Name | Value |
|---|---|
| Type | Cognos |
| Allow anonymous access? | True |

Defines a group of properties related to authentication that applies to all users.

Use this group of properties to control access to resources based on user identity. Do not delete the namespace, or you will not be able to save your configuration. To restore the namespace, right-click Authentication, click New, Namespace Type, select the Cognos Namespace from the list of available types and specify a name.

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.

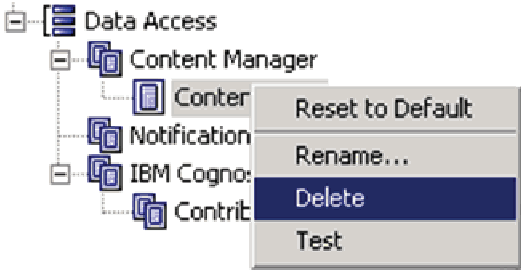
The IBM Cognos Application Firewall is an essential component of product security helping to provide protection against penetration vulnerabilities. Disabling the IBM Cognos Application Firewall will remove this protection; therefore, this should not be done under normal circumstances.

5. Set the **Enable CAF validation?** property to **False.**

### 6.2.5.4 Setting the Data Access Properties for Cognos 8

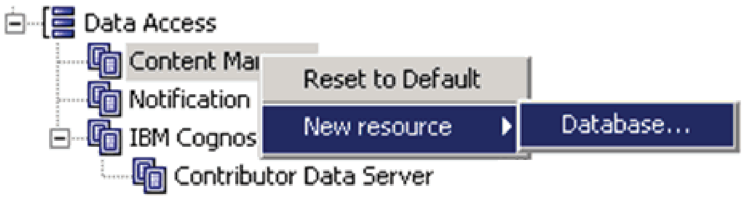
To define the data access properties:

1. Open the IBM Cognos 8 Configuration window.
2. Navigate to **Data Access, Content Manager,** right-click **Content Store,** and then select **Delete** from the menu.



The system prompts for confirmation that you want to delete the Content Store.

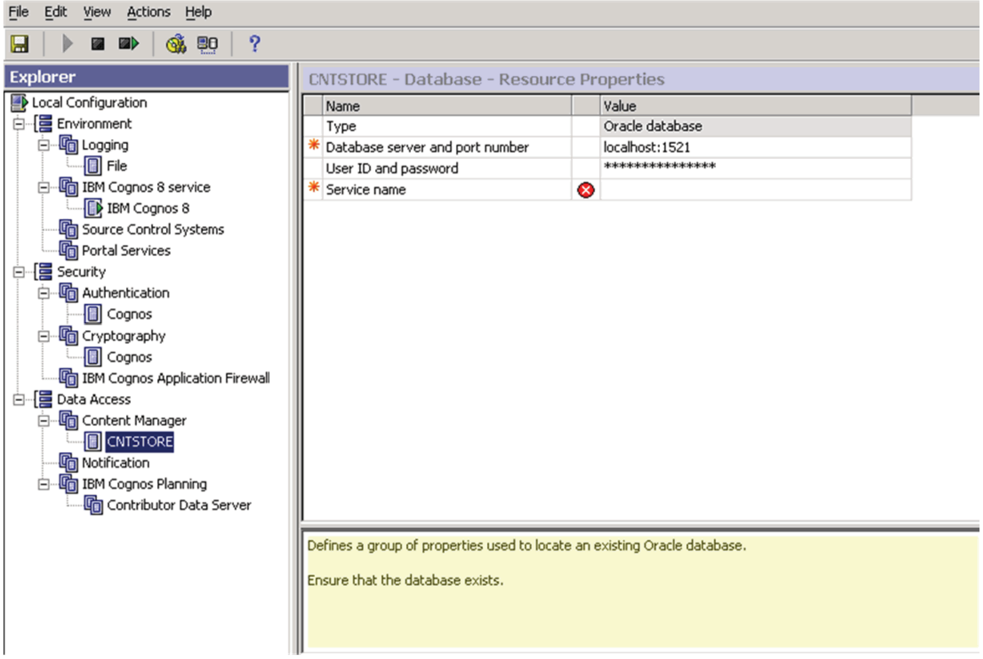
3. Click **Yes.**
4. Navigate to **Data Access,** right-click **Content Manager,** select **New resource,** and then select **Database.**



5. Complete the New Resource - Database dialog box as follows:

- In the **Name** field, type **CNTSTORE.** This is the name of the database resource.
- In the **Type** field, select **Oracle database.**
- Click **OK.**

The system returns to the IBM Cognos Configuration window, selects the newly-created CNTSTORE resource database, and displays the resource properties for the database.



CNTSTORE - Database - Resource Properties

| | Name | Value |
|---|---|---|
| | Type | Oracle database |
| * | Database server and port number | localhost:1521 |
| | User ID and password | *************** |
| * | Service name | ⊗ |

Defines a group of properties used to locate an existing Oracle database.

Ensure that the database exists.

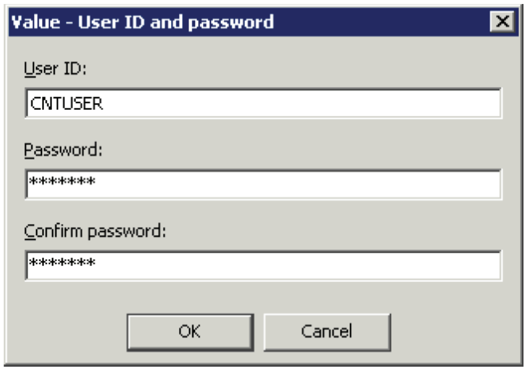
6. Enter the value for the **Database server and port number** as:

   *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 opens.



User ID: CNTUSER

Password: ********

Confirm password: ********

   a. In the **User ID** field, type the ID for the content store database user.

   b. In the **Password** field, type the password for the content store database user.

c. In the **Confirm password** field, re-enter the password for verification.

d. Click **OK.**

---

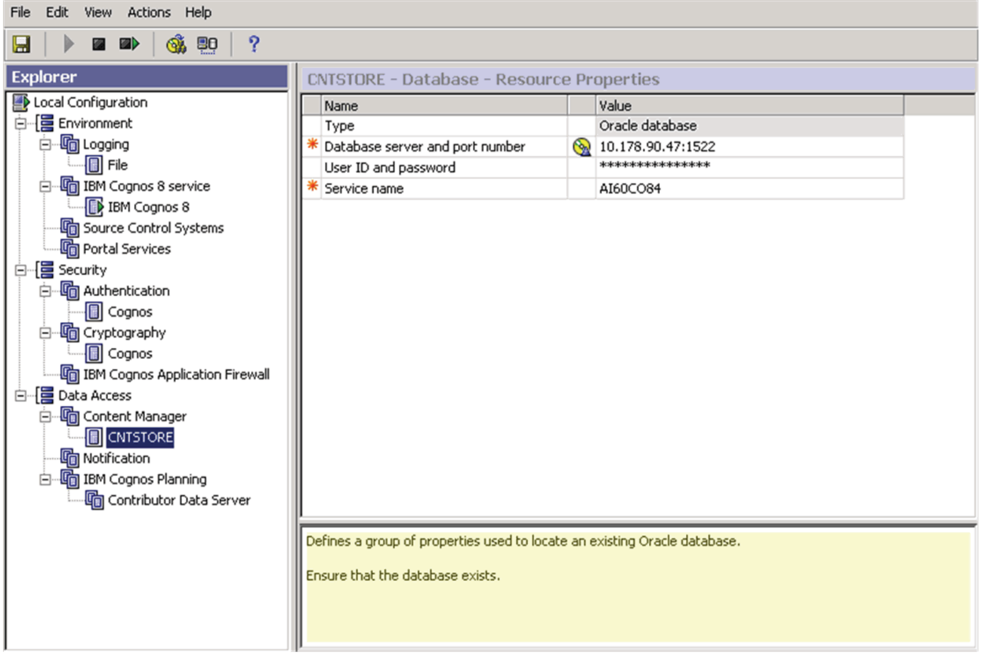
**Note:** The contents store database user is created in the Cognos content store database. This user is given grants of Connect, Resource, and Create View, along with Unlimited Tablespace Grant.

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 8 server.

---

8. Enter the database instance name for the Cognos 8 repository in the **Service name** field.



CNTSTORE - Database - Resource Properties

| | Name | Value |
|---|---|---|
| | Type | Oracle database |
| * | Database server and port number | 10.178.90.47:1522 |
| | User ID and password | *************** |
| * | Service name | AI60CO84 |

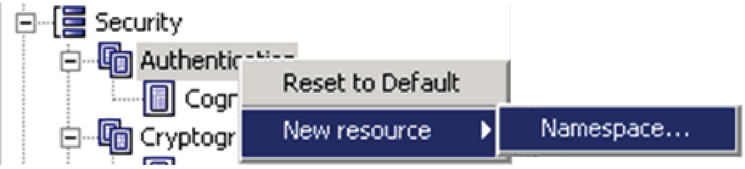
Defines a group of properties used to locate an existing Oracle database.

Ensure that the database exists.

### 6.2.5.5 Creating the Namespace for Argus Insight Authentication

To create the namespace for Argus Insight authentication:

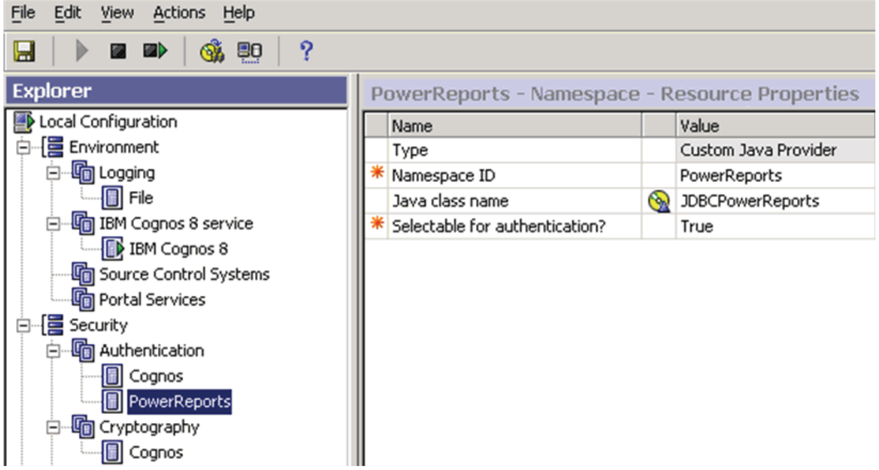
1. Open the IBM Cognos 8 Configuration window.
2. Navigate to **Security,** right-click **Authentication,** click **New resource,** and then select **Namespace.**



3. Complete the New Resource – Namespace dialog box as follows:
   - In the **Name** field, type **PowerReports.**
   - In the **Type** field, type **Custom Java Provider.**

- Click **OK.**

The PowerReports - Namespace - Resource Properties window opens.



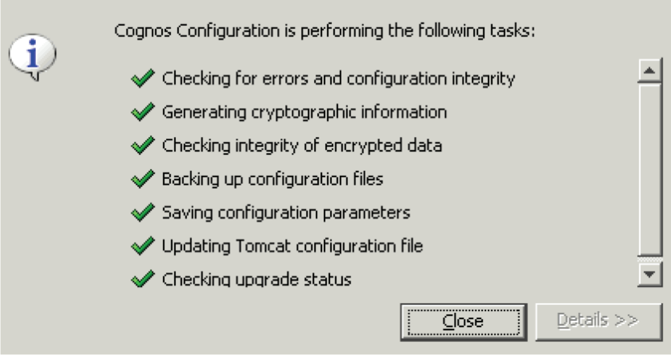
| Name | Value |
|---|---|
| Type | Custom Java Provider |
| * Namespace ID | PowerReports |
| Java class name | JDBCPowerReports |
| * Selectable for authentication? | True |

4. Set the **Namespace ID** property to **PowerReports.**
5. Set the **Java class name** property to **JDBCPowerReports.**

### 6.2.5.6 Saving Your Configuration and Starting the Cognos 8 Service

To save the configuration and start the Cognos 8 service:

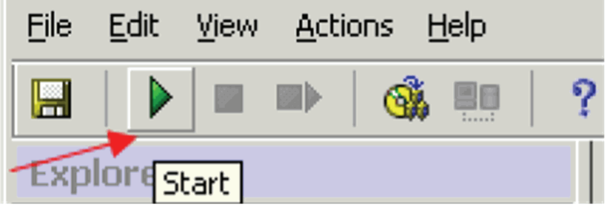
1. Open the File menu and select **Save** to save your changes to the configuration settings. The system displays the following dialog box and lists each task as it is performed:



Cognos Configuration is performing the following tasks:

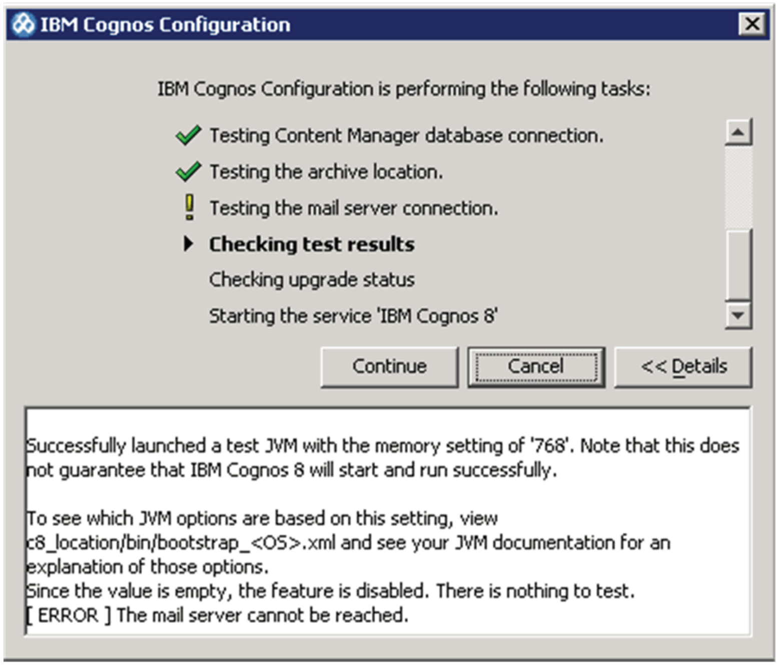
- ✓ Checking for errors and configuration integrity
- ✓ Generating cryptographic information
- ✓ Checking integrity of encrypted data
- ✓ Backing up configuration files
- ✓ Saving configuration parameters
- ✓ Updating Tomcat configuration file
- ✓ Checking upgrade status

2. Click **Close** when the system completes all the configuration tasks.
3. Click the **Start** icon in the IBM Cognos Configuration window to run the Cognos 8 service.



The system begins to run the IBM Cognos 8 service.

- If there are no problems with the configuration, the system completes the test phase and starts the IBM Cognos 8 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:

- ✓ Testing Content Manager database connection.
- ✓ Testing the archive location.
- ! Testing the mail server connection.
- ▶ **Checking test results**
- Checking upgrade status
- Starting the service 'IBM Cognos 8'

Successfully launched a test JVM with the memory setting of '768'. Note that this does not guarantee that IBM Cognos 8 will start and run successfully.

To see which JVM options are based on this setting, view c8_location/bin/bootstrap_<OS>.xml and see your JVM documentation for an explanation of those options.
Since the value is empty, the feature is disabled. There is nothing to test.
[ ERROR ] The mail server cannot be reached.

At this point, you can:

- Click **Details** for more information about the warnings and errors.
- Click **Cancel** to stop the process. If the warnings or errors are due to reasons other than mail server connection failure, cancel the process and check your configuration again.
- Click **Continue** to ignore the warnings and errors, and complete the process of starting the IBM Cognos 8 service. For example, you can 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 8 configuration.

### 6.2.6 Importing the Content Repository

---

**Note:** If your security settings on the server do not permit you to view the Cognos connection, add the site URL (http://*Cognos_8_Server*/cognos8) to the list of local intranet sites.

---

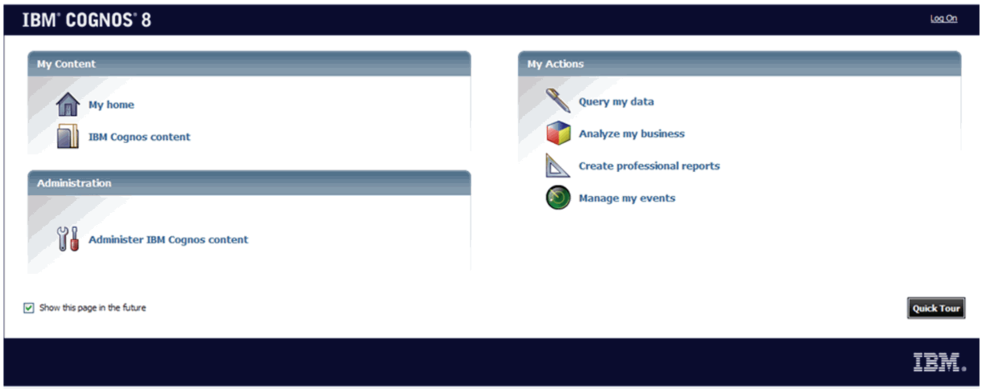
To import the content repository to the database:

1. Log in to the IBM Cognos 8 Server as a user with administrator privileges.
2. Start Internet Explorer.

3. Enter the URL in the following format:

   http://*Cognos_8_Server*/cognos8

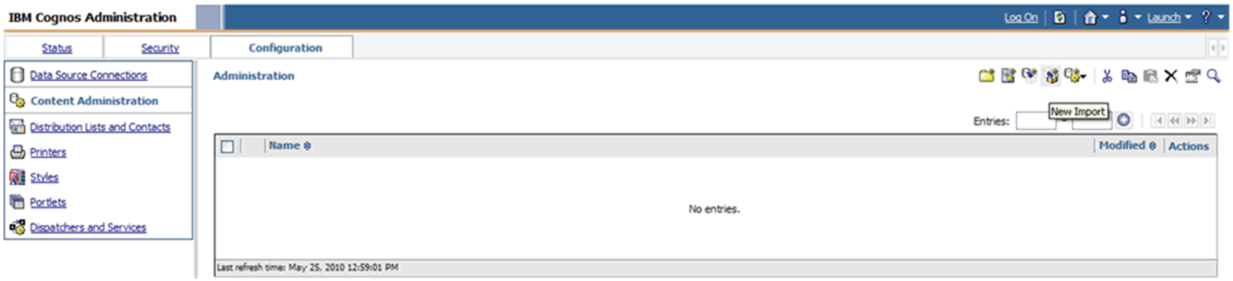
   The IBM Cognos 8 main window opens.



4. Click **Administer IBM Cognos content.** The IBM Cognos Administration window opens.

5. Click the **Configuration** tab.

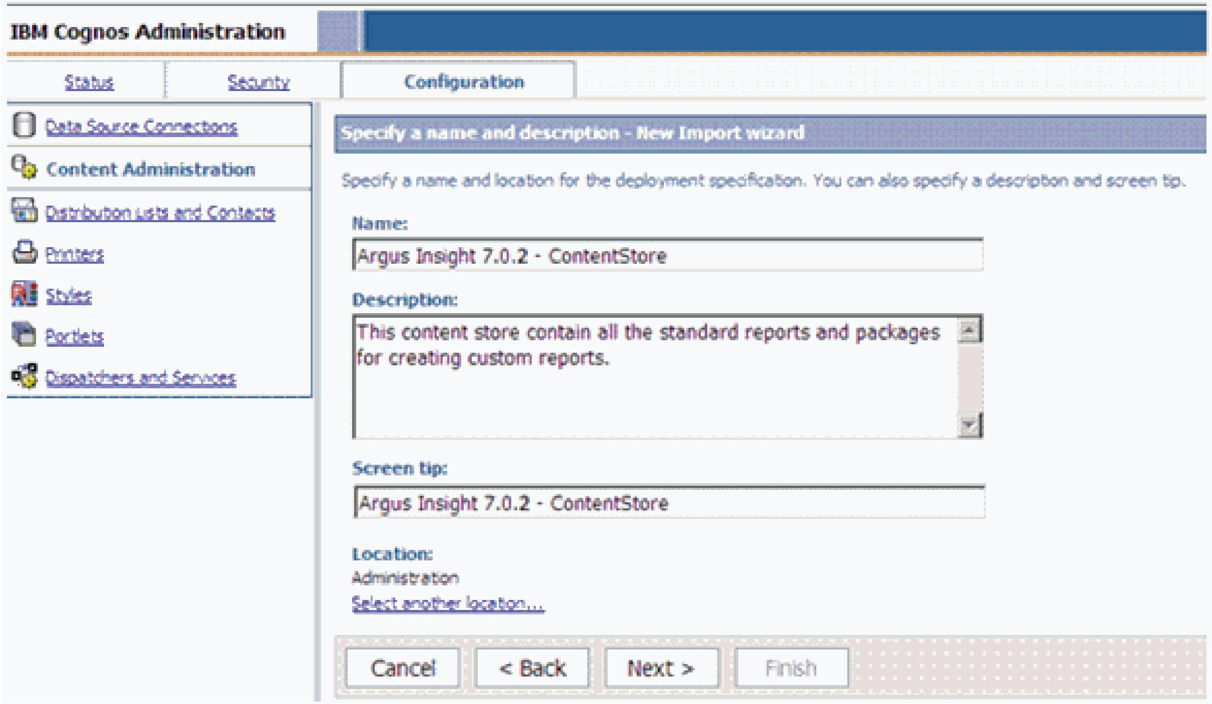
6. Click the **Content Administration** link. The Content Administration window opens.



7. Click the **New Import** icon. The system starts the New Import wizard.

8. Click **Next** to continue. The wizard prompts for the encryption password.

9. Type the password and click **OK.** The wizard prompts for the name, description, and location of the Argus Insight deployment.



Specify a name and description - New Import wizard

Specify a name and location for the deployment specification. You can also specify a description and screen tip.

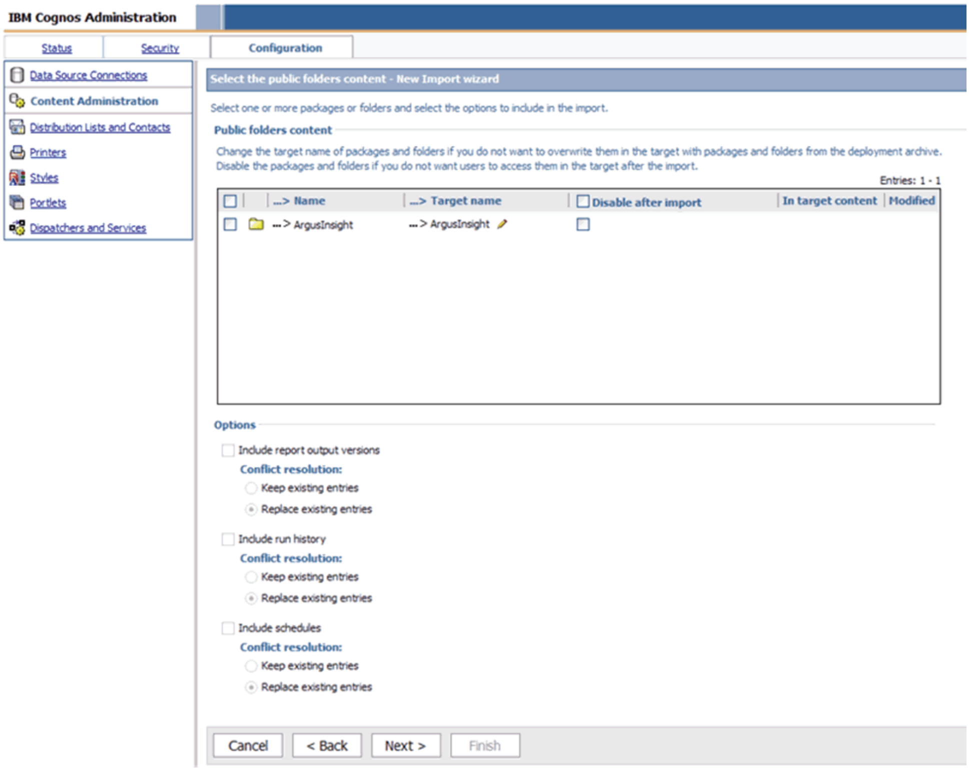
Name:
Argus Insight 7.0.2 - ContentStore

Description:
This content store contain all the standard reports and packages for creating custom reports.

Screen tip:
Argus Insight 7.0.2 - ContentStore

Location:
Administration
Select another location...

10. Leave the default values and click **Next** to continue. The wizard prompts you to select the public folders content.



Select the public folders content - New Import wizard

Select one or more packages or folders and select the options to include in the import.

Public folders content

Change the target name of packages and folders if you do not want to overwrite them in the target with packages and folders from the deployment archive. Disable the packages and folders if you do not want users to access them in the target after the import.

Entries: 1 - 1

| ☐ | | ...> Name | ...> Target name | ☐ Disable after import | In target content | Modified |
|---|---|---|---|---|---|---|
| ☐ | | ...> ArgusInsight | ...> ArgusInsight | ☐ | | |

Options

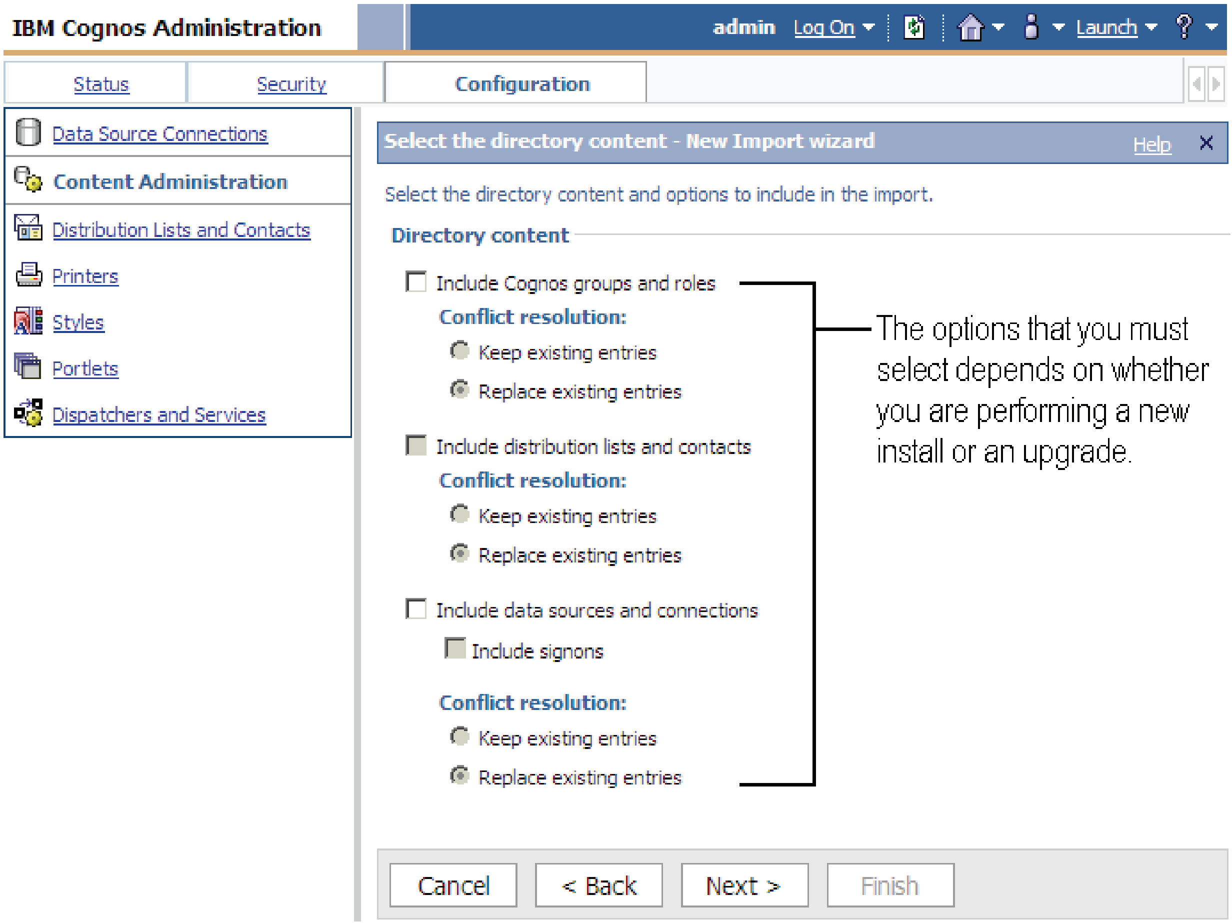
☐ Include report output versions
Conflict resolution:
○ Keep existing entries
● Replace existing entries

☐ Include run history
Conflict resolution:
○ Keep existing entries
● Replace existing entries

☐ Include schedules
Conflict resolution:
○ Keep existing entries
● Replace existing entries

11. Select the **Name** check box to choose all the check boxes in this category, and click **Next.**

    The wizard prompts you to select the directory content and options to include in the import.



**Select the directory content - New Import wizard**

Select the directory content and options to include in the import.

**Directory content**

☐ Include Cognos groups and roles

**Conflict resolution:**

○ Keep existing entries

● Replace existing entries

☐ Include distribution lists and contacts

**Conflict resolution:**

○ Keep existing entries

● Replace existing entries

☐ Include data sources and connections

☐ Include signons

**Conflict resolution:**

○ Keep existing entries

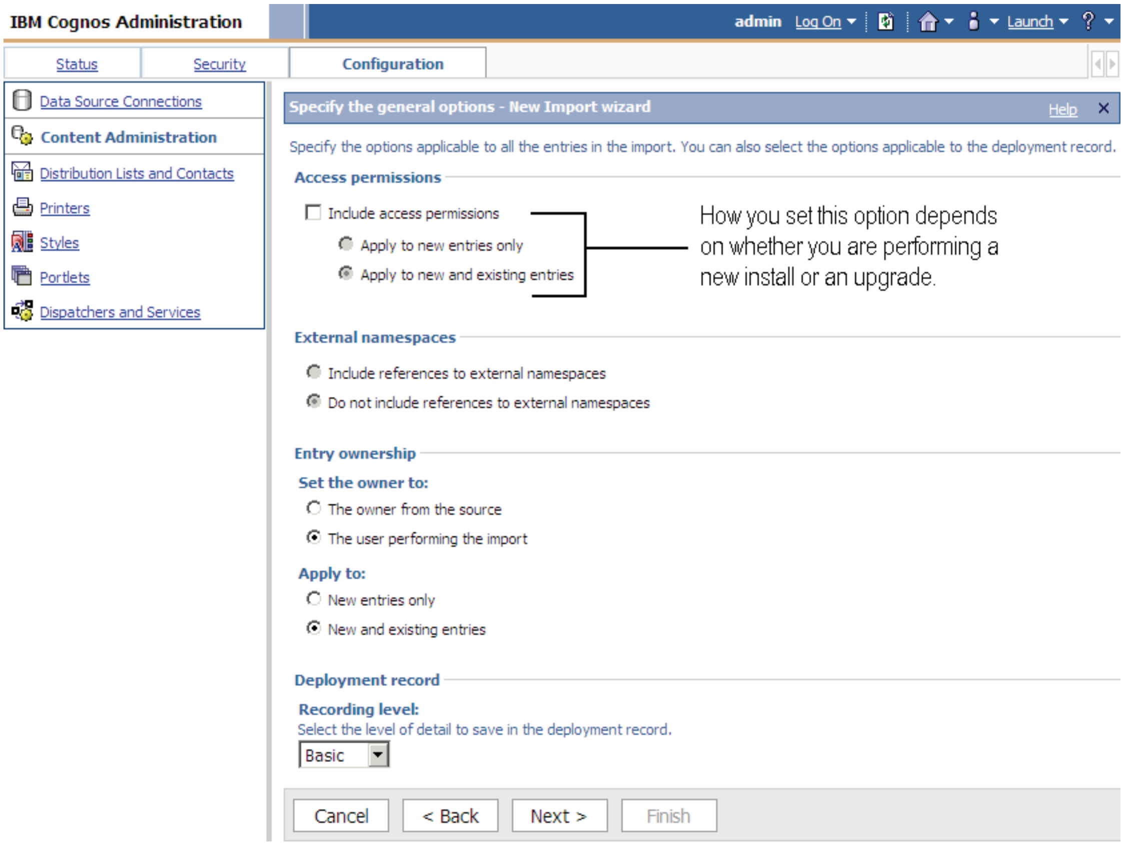
● Replace existing entries

The options that you must select depends on whether you are performing a new install or an upgrade.

12. Select the directory content and options to include in the import. The options that you select depends on whether you are performing a new install or an upgrade.

| Directory Content and Options | New Install | Upgrade |
|---|---|---|
| Include Cognos groups and roles | Selected | NOT selected |
| Include distribution lists and contacts | NOT selected | NOT selected |
| Include data sources and connections | Selected | NOT selected |
| Include signons | Selected | NOT selected |

13. Click **Next.** The wizard prompts you to specify the general options.



Specify the general options - New Import wizard

Specify the options applicable to all the entries in the import. You can also select the options applicable to the deployment record.

Access permissions

☐ Include access permissions
  ○ Apply to new entries only
  ● Apply to new and existing entries

How you set this option depends on whether you are performing a new install or an upgrade.

External namespaces

○ Include references to external namespaces
● Do not include references to external namespaces

Entry ownership

Set the owner to:
○ The owner from the source
● The user performing the import

Apply to:
○ New entries only
● New and existing entries

Deployment record

Recording level:
Select the level of detail to save in the deployment record.
Basic

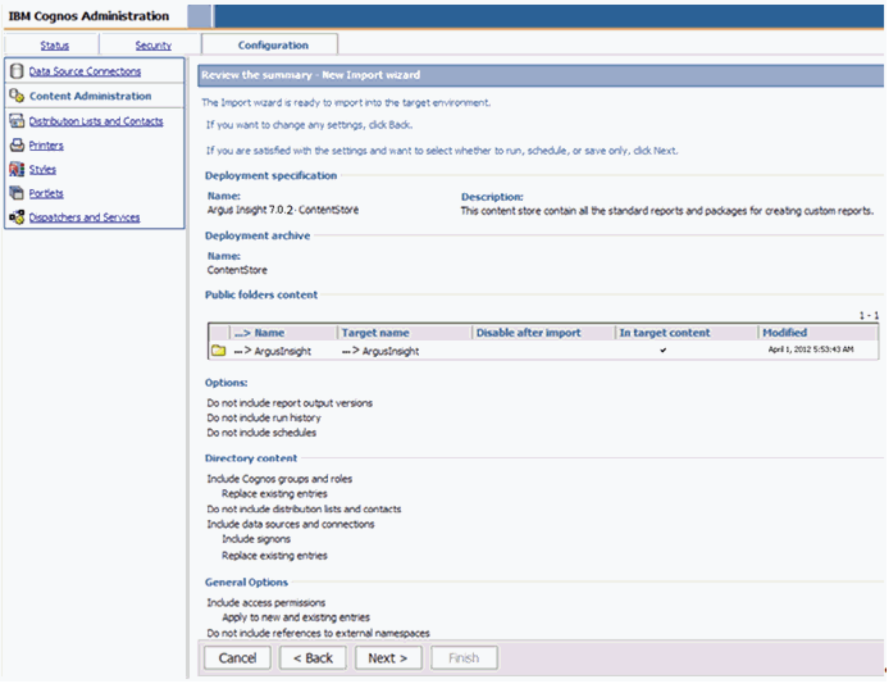
14. Set the **Access permissions** depending on whether you are performing a new install or an upgrade:

    - If you are performing a new install, you MUST select the **Include access permissions** check box.
    - If you are performing an upgrade, do NOT select the **Include access permissions** check box.

15. Verify that the remaining general options are set as follows:

    - For External namespaces, verify that **Do not include references to external namespaces** is selected, but dimmed.
    - For Entry ownership, set the owner to **The user performing the import** and apply to **New and existing entries**.
    - For the Deployment record, select **Basic** for the Recording level.

16. Click **Next.** The wizard displays the summary screen.



The Import wizard is ready to import into the target environment.

If you want to change any settings, click Back.

If you are satisfied with the settings and want to select whether to run, schedule, or save only, click Next.

**Deployment specification**

**Name:**
Argus Insight 7.0.2- ContentStore

**Description:**
This content store contain all the standard reports and packages for creating custom reports.

**Deployment archive**

**Name:**
ContentStore

**Public folders content**

1 - 1

| ...> Name | Target name | Disable after import | In target content | Modified |
|---|---|---|---|---|
| ---> ArgusInsight | ---> ArgusInsight | | ✓ | April 1, 2012 5:53:43 AM |

**Options:**

Do not include report output versions
Do not include run history
Do not include schedules

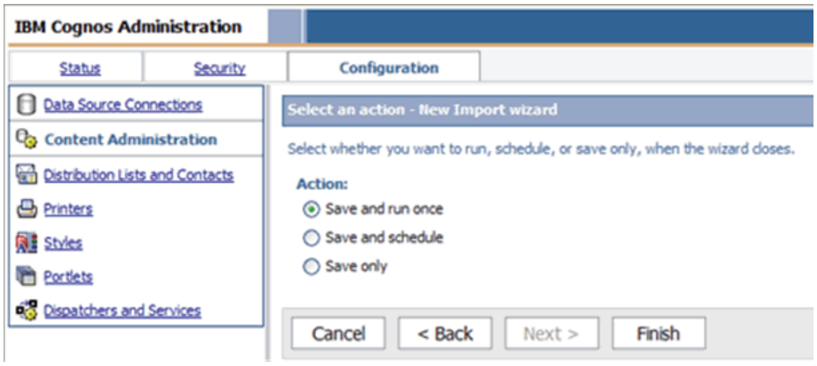
**Directory content**

Include Cognos groups and roles
  Replace existing entries
Do not include distribution lists and contacts
Include data sources and connections
  Include signons
  Replace existing entries

**General Options**

Include access permissions
  Apply to new and existing entries
Do not include references to external namespaces

17. Review the summary information, and click **Next.** The wizard prompts you to select the type of New Import action.



Select whether you want to run, schedule, or save only, when the wizard closes.

**Action:**

● Save and run once
○ Save and schedule
○ Save only

18. Select the **Save and run once** option, and click **Finish.** The wizard prompts you to selection the options for this import.

19. Select **Upgrade all report specifications to the latest version** and click **Run.** The wizard summarizes your selection for this import.

20. Click **OK** to run the import.

21. Verify the import as follows:

    a. Click **More** corresponding to the newly imported Content Store.

    b. Click **View run history** to view the deployment history.

    c. Verify that the **Status** column displays the status as Succeeded.

    d. Click **Close** to exit.

The repository import is complete.

---

**Note:** If the database changed from the 7.0 database, you must also update the source data information after importing the content repository. Skip to Section 6.2.7.2, "Editing Sign On" for instructions.

---

## 6.2.7 Configuring Cognos Security

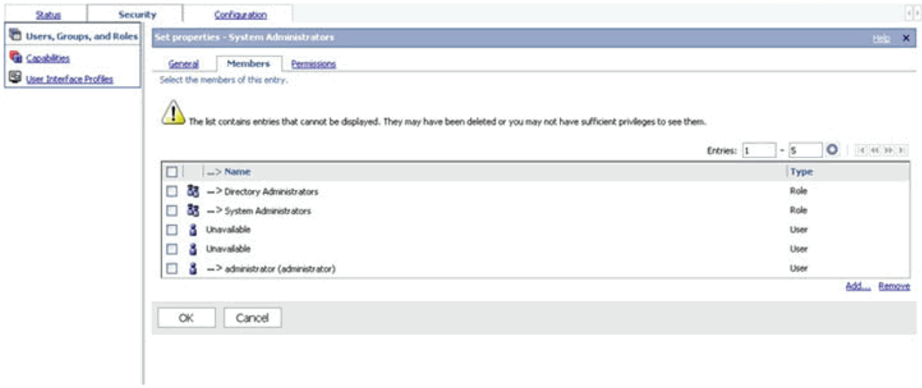
This section includes the following topics:

- Configuring Cognos Users and Roles
- Editing Sign On
- Activating the PowerReports Namespace

### 6.2.7.1 Configuring Cognos Users and Roles

To configure Cognos user and roles:

1. Set up an administrator user in the Cognos environment. An administrator user is an Argus Insight user who is part of the system administrator role.

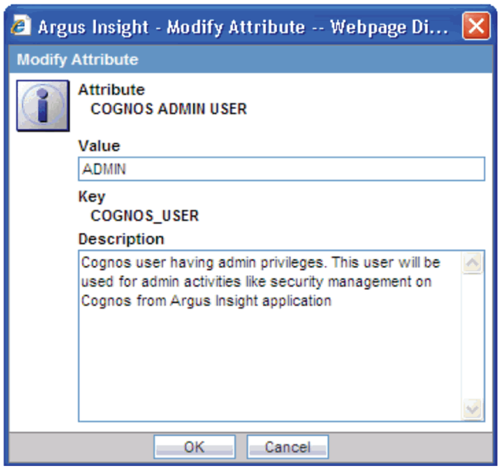


Select the members of this entry.

The list contains entries that cannot be displayed. They may have been deleted or you may not have sufficient privileges to see them.

| ☐ | --> Name | Type |
|---|---|---|
| ☐ | --> Directory Administrators | Role |
| ☐ | --> System Administrators | Role |
| ☐ | Unavailable | User |
| ☐ | Unavailable | User |
| ☐ | --> administrator (administrator) | User |

2. Log in to Argus Insight as a user with administrator privileges.
3. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page to open the ADMINISTRATION TOOLS page.
4. Click the **List Maintenance** tab.
5. Select **Profile Switches** from the List Maintenance Items group.
6. Define the COGNOS ADMIN USER attribute.
   a. Select **COGNOS ADMIN USER** from the Attributes group.
   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COGNOS ADMIN USER

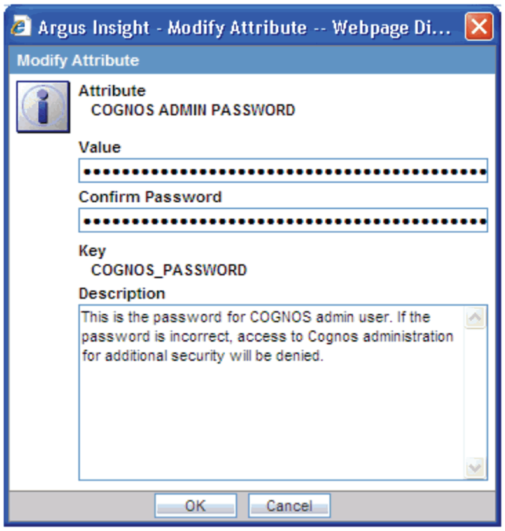
Value
ADMIN

Key
COGNOS_USER

Description
Cognos user having admin privileges. This user will be used for admin activities like security management on Cognos from Argus Insight application

   c. Enter the value for the Cognos administrator user.
   d. Click **OK** to save your changes and return to the List Maintenance tab.

7. Define the COGNOS ADMIN PASSWORD attribute.
   a. Select **COGNOS ADMIN PASSWORD** from the Attributes group.
   b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COGNOS ADMIN PASSWORD

Value
••••••••••••••••••••••••••••••••••••••••••••

Confirm Password
••••••••••••••••••••••••••••••••••••••••••••

Key
COGNOS_PASSWORD

Description
This is the password for COGNOS admin user. If the password is incorrect, access to Cognos administration for additional security will be denied.

   c. Click the **Value** field, and type the password for the Cognos administrator.
   d. Re-type the password in the **Confirm Password** field for verification.
   e. Click **OK** to save your changes and return to the List Maintenance tab.

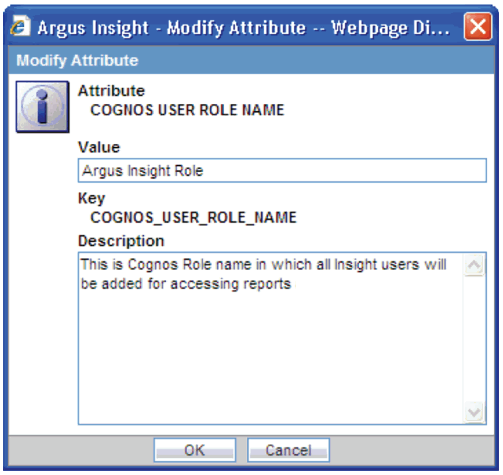
8. Verify that the following List Maintenance entries are configured.
   - COGNOS SERVER
   - COGNOS ADMIN USER
   - COGNOS ADMIN PASSWORD

   This role will have all rights required to run various parts of Argus Insight application. All Insight users will become part of this role during their first login.

9. Define the COGNOS USER ROLE NAME attribute.

a. Select **COGNOS USER ROLE NAME** from the Attributes group.

b. Click **Modify.** The following Modify Attribute dialog box opens:



Attribute
COGNOS USER ROLE NAME

Value
Argus Insight Role

Key
COGNOS_USER_ROLE_NAME

Description
This is Cognos Role name in which all Insight users will be added for accessing reports

c. Click the **Value** field, and type the Cognos User Role Name you want to create in Cognos environment.

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

The system adds the newly configured role to the following roles:

- Analysis Users
- Query User
- Author

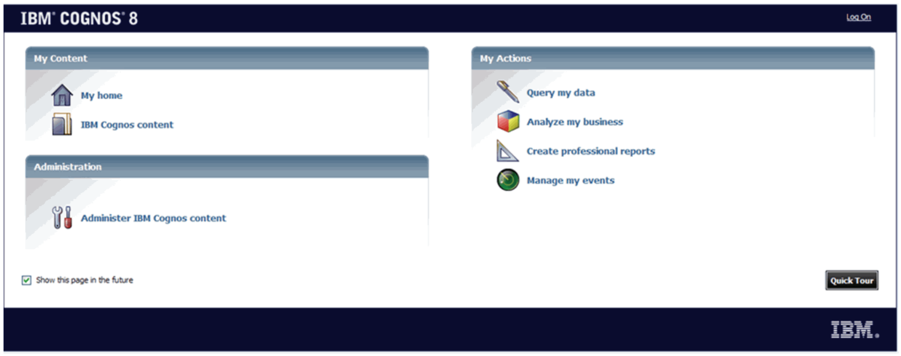
#### 6.2.7.2 Editing Sign On

To edit your sign-on information:

1. Log in to the Cognos 8 Server as an administrator user.
2. Start Internet Explorer.
3. Type the URL in the following format and press Enter:

   http://*Cognos_8_Server*/cognos8

   The IBM Cognos 8 home page opens.



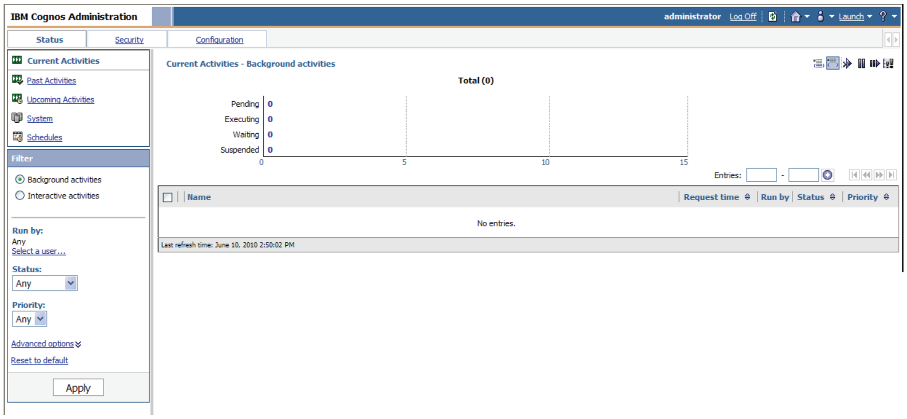
☑ Show this page in the future

---

**Note:** If your security settings on the server do not permit you to view the Cognos connection, add the site URL (http://*Cognos_8_Server*/cognos8) to the list of local intranet sites.

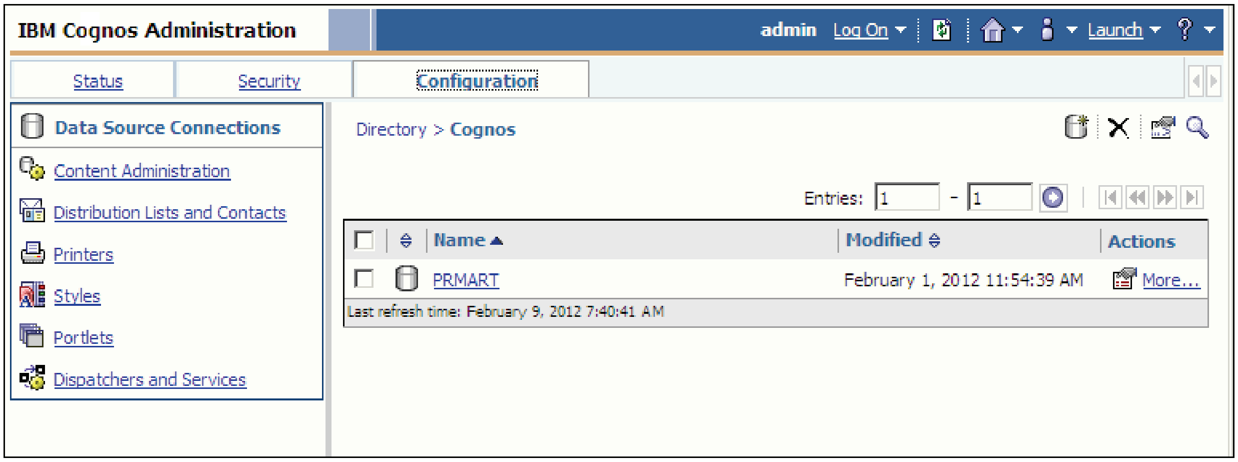
---

4. Click **Administer IBM Cognos content.** The IBM Cognos Administration window opens.



5. Click the **Configuration** tab.

6. Click **Data Source Connections** and click **PRMART.**

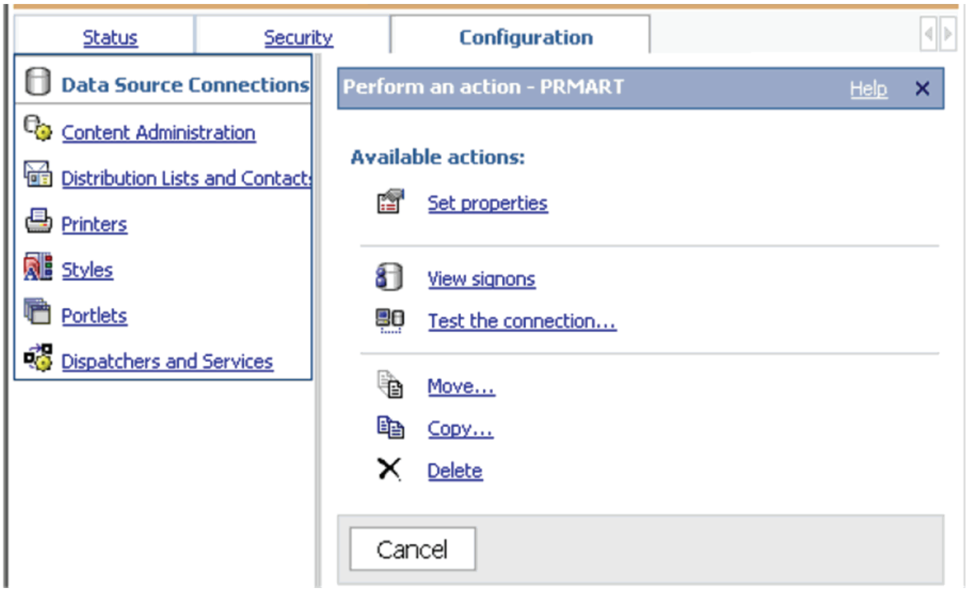


| ☐ | Name ▲ | Modified | Actions |
|---|---|---|---|
| ☐ | PRMART | February 1, 2012 11:54:39 AM | More... |

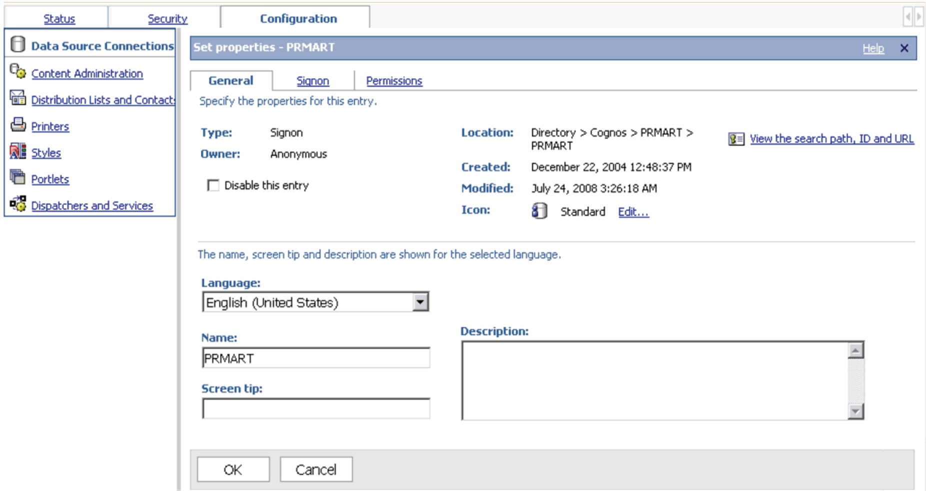
Last refresh time: February 9, 2012 7:40:41 AM

7. Click **PRMART.**

8. Click the **More** link to the right of the PRMART link. The Perform an action - PRMART pane opens.



9. Click **Set properties.** The Set properties page for PRMART opens.



Specify the properties for this entry.

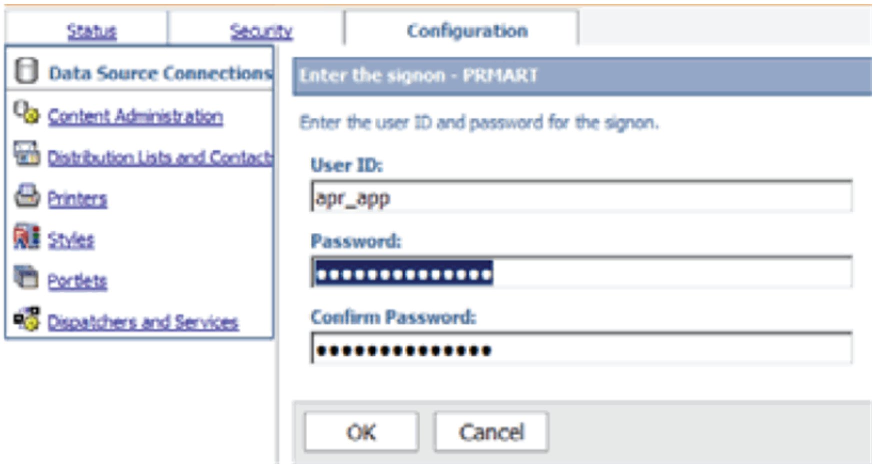
Type: Signon
Owner: Anonymous
☐ Disable this entry
Location: Directory > Cognos > PRMART > PRMART
Created: December 22, 2004 12:48:37 PM
Modified: July 24, 2008 3:26:18 AM
Icon: Standard

The name, screen tip and description are shown for the selected language.

Language: English (United States)
Name: PRMART
Screen tip:
Description:

10. Click the **Signon** tab.

11. Click the **Edit the signon** link. The system opens the following pane:

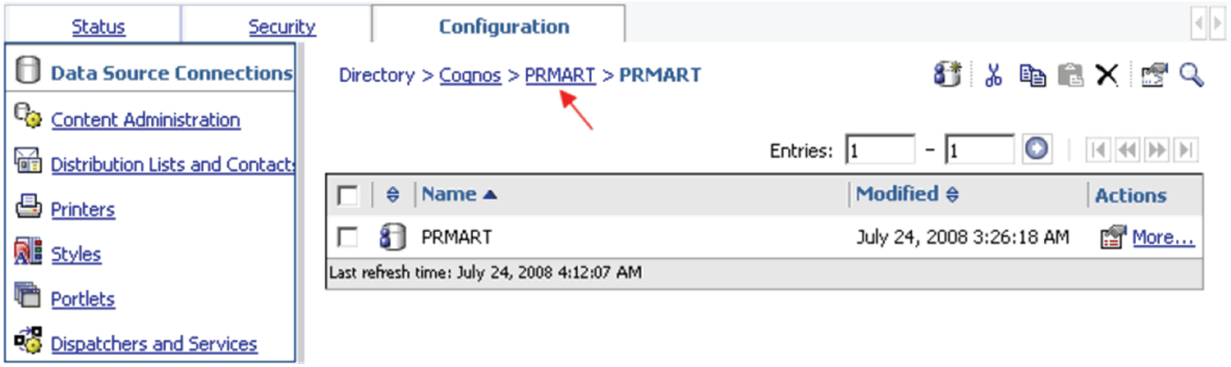


Enter the user ID and password for the signon.

User ID: apr_app
Password: •••••••••••••••
Confirm Password: •••••••••••••••

   a. In the **User ID** field, type the ID for the APR_APP user.
   b. In the **Password** field, type the password for the APR_APP user.
   c. In the **Confirm Password** field, re-type the password for verification.
   d. Click **OK** to set the password.

12. Click **OK** again to return to this screen:



Directory > Cognos > PRMART > PRMART

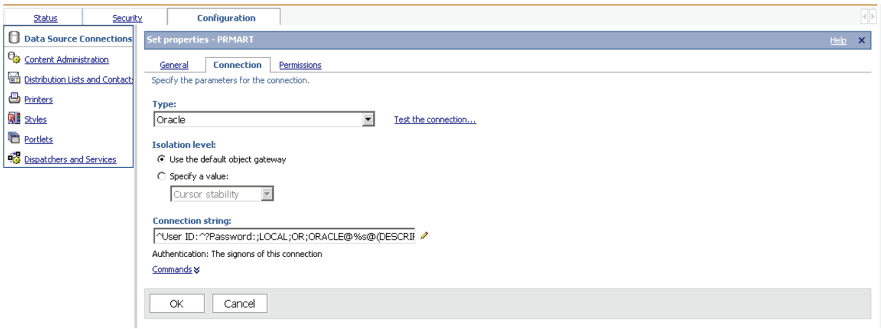
Entries: 1 - 1

| ☐ | Name ▲ | Modified | Actions |
|---|---|---|---|
| ☐ | PRMART | July 24, 2008 3:26:18 AM | More... |

Last refresh time: July 24, 2008 4:12:07 AM

13. Click the **PRMART** link, click the **More** link, and then click **Set properties.**

14. Click the **Connection** tab. The system displays the following information:



Set properties - PRMART

Specify the parameters for the connection.

Type: Oracle

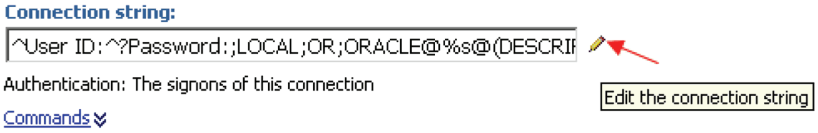
Isolation level:

● Use the default object gateway

○ Specify a value: Cursor stability

Connection string: ^User ID:^?Password:;LOCAL;OR;ORACLE@%s@(DESCRIF

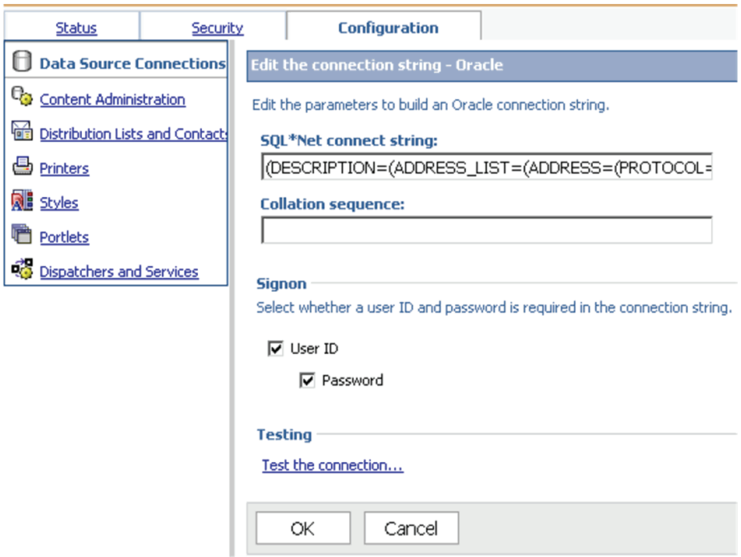
Authentication: The signons of this connection



Connection string: ^User ID:^?Password:;LOCAL;OR;ORACLE@%s@(DESCRIF

Authentication: The signons of this connection

15. Click the **pencil** icon to edit the connection string. The system displays the Edit the connection string - Oracle pane.



Edit the connection string - Oracle

Edit the parameters to build an Oracle connection string.

SQL*Net connect string: (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=

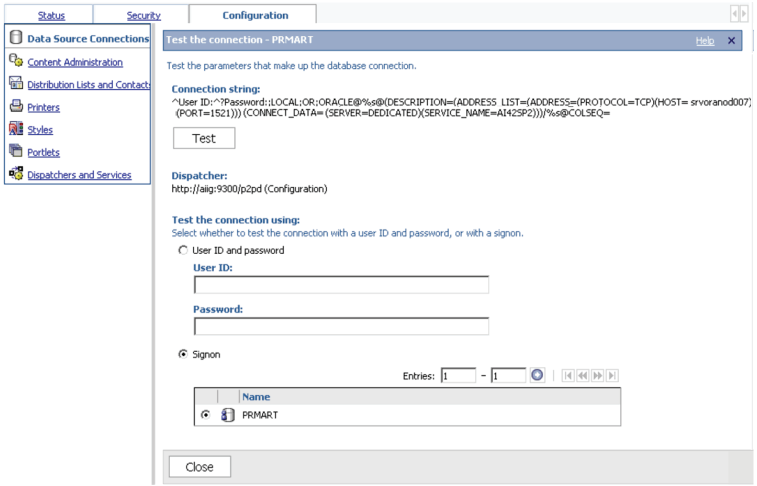
Collation sequence:

Select whether a user ID and password is required in the connection string.

☑ User ID

☑ Password

16. Set the following information in the **SQL*Net connect strings** field:
    - Set the HOST as the Argus Insight Database Server Name.
    - Set the PORT as the Argus Insight Database Port Number.
    - Set the SERVICE_NAME as the Argus Insight Database Instance Name.
17. Click the **Test the connection** link. Wait until the system opens the Test the connection - PRMART pane and then click **Test.**



Test the connection - PRMART

Test the parameters that make up the database connection.

Connection string:
^User ID:^?Password:;LOCAL;OR;ORACLE@%s@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST= srvoranod007)(PORT=1521))) (CONNECT_DATA= (SERVER=DEDICATED)(SERVICE_NAME=AI42SP2)))/%s@COLSEQ=

Dispatcher:
http://aiig:9300/p2pd (Configuration)

Test the connection using:
Select whether to test the connection with a user ID and password, or with a signon.

○ User ID and password

User ID:

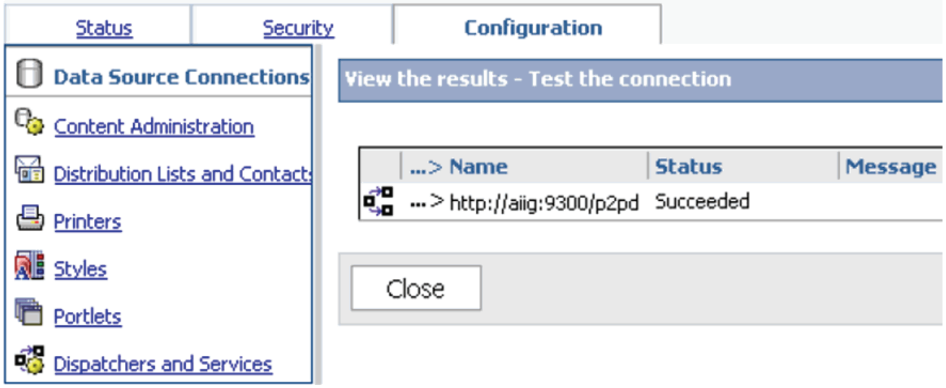
Password:

● Signon

Entries: 1 - 1

● PRMART

18. Wait for the testing results and verify that the connection succeeded.



| ...> Name | Status | Message |
|---|---|---|
| ...> http://aiig:9300/p2pd | Succeeded | |

19. Click **Close.**

20. Click **Close.**

21. Click **OK.**

22. Click **OK.**

### 6.2.7.3 Activating the PowerReports Namespace

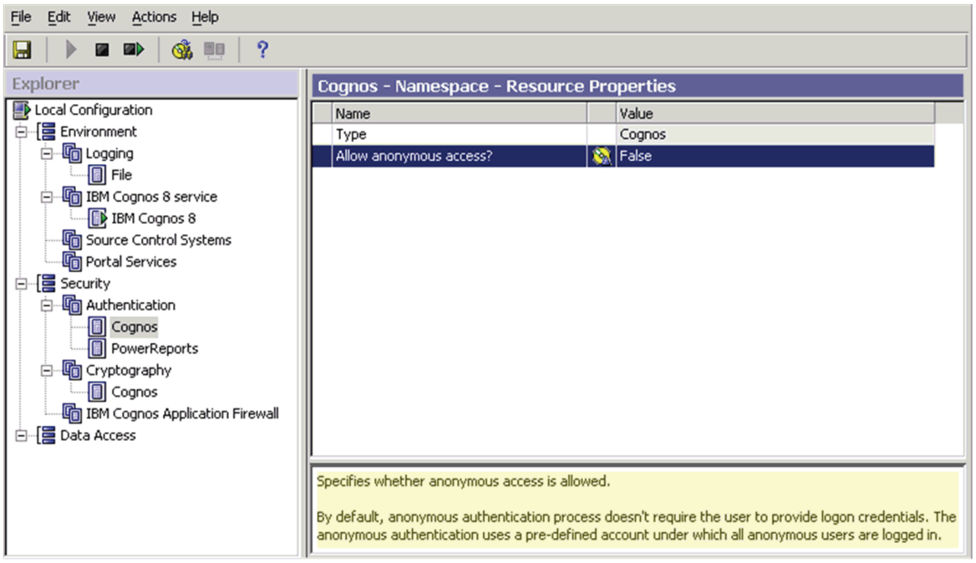
To activate the PowerReports namespace:

1. Open the Cognos 8 configuration.

2. Click **Start, All Programs, IBM Cognos 8,** and then select **IBM Cognos Configuration.** The IBM Cognos Configuration window opens.

3. Navigate to **Security, Authentication,** and then select **Cognos.** The system displays the Cognos - Namespace - Resource properties pane.

4. Set the **Allow Anonymous access?** property to **False.**



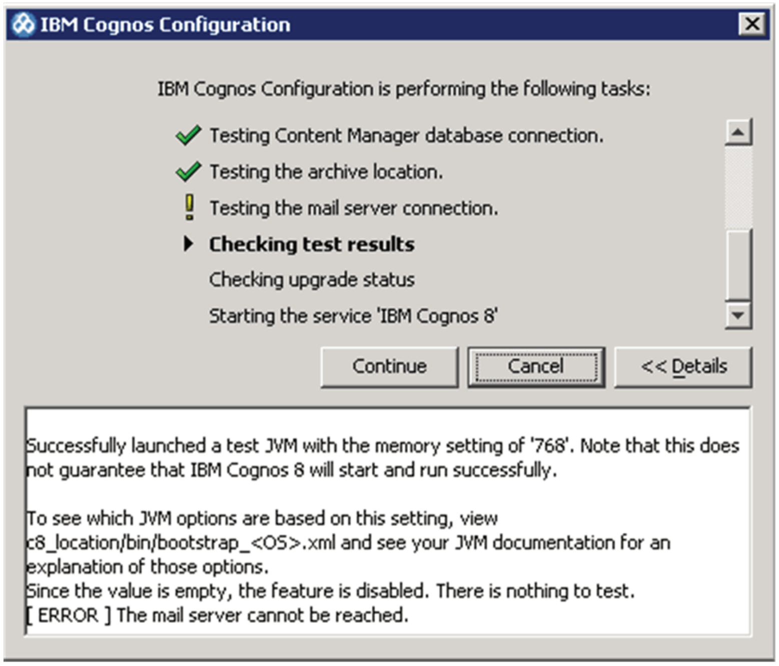
| Name | Value |
|---|---|
| Type | Cognos |
| Allow anonymous access? | False |

Specifies whether anonymous access is allowed.

By default, anonymous authentication process doesn't require the user to provide logon credentials. The anonymous authentication uses a pre-defined account under which all anonymous users are logged in.

5. Open the **File** menu and select **Save.**

6. Open the **Actions** menu and select **Restart** to restart the Cognos 8 service. The system displays status information about each task being performed during the restart.



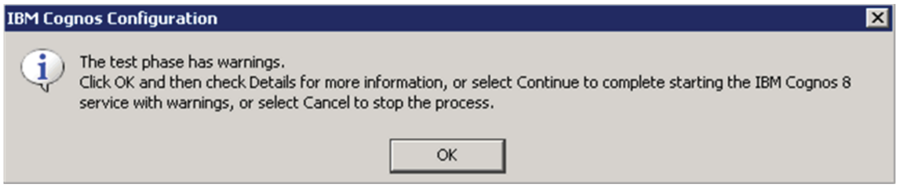
IBM Cognos Configuration is performing the following tasks:

- ✓ Testing Content Manager database connection.
- ! Testing the archive location.
- ! Testing the mail server connection.
- ▸ **Checking test results**
- Checking upgrade status
- Starting the service 'IBM Cognos 8'

Successfully launched a test JVM with the memory setting of '768'. Note that this does not guarantee that IBM Cognos 8 will start and run successfully.

To see which JVM options are based on this setting, view c8_location/bin/bootstrap_<OS>.xml and see your JVM documentation for an explanation of those options.
Since the value is empty, the feature is disabled. There is nothing to test.
[ ERROR ] The mail server cannot be reached.

During the Cognos service restart, the system may display the following message if there are any warnings:



The test phase has warnings.
Click OK and then check Details for more information, or select Continue to complete starting the IBM Cognos 8 service with warnings, or select Cancel to stop the process.

7. Process any warning message as follows:

   a. Click **OK.**

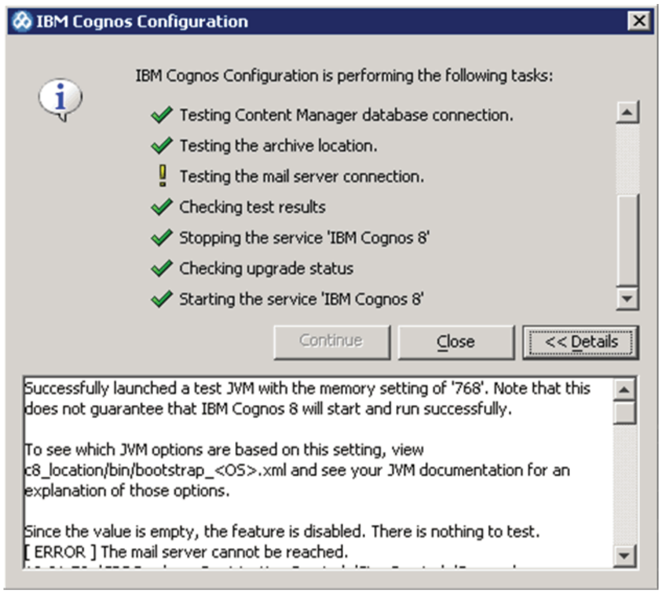
   b. Click **Details** to obtain more information about the warning.

      Depending on the type of warning, you can:

      — Click **Continue** to ignore the warning and continue with the process of restarting the IBM Cognos 8 service. For example, you may want to ignore a warning that the connection to the mail server failed.

      — Click **Cancel** to stop the restart process. 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 8 service.

8. Wait until the system performs all the configuration tasks and displays the status for each task.



IBM Cognos Configuration is performing the following tasks:

✓ Testing Content Manager database connection.
✓ Testing the archive location.
! Testing the mail server connection.
✓ Checking test results
✓ Stopping the service 'IBM Cognos 8'
✓ Checking upgrade status
✓ Starting the service 'IBM Cognos 8'

Successfully launched a test JVM with the memory setting of '768'. Note that this does not guarantee that IBM Cognos 8 will start and run successfully.

To see which JVM options are based on this setting, view c8_location/bin/bootstrap_<OS>.xml and see your JVM documentation for an explanation of those options.

Since the value is empty, the feature is disabled. There is nothing to test.
[ ERROR ] The mail server cannot be reached.

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_Installation_Path*\c8\configuration\schemas\content

3. Run the **AddSysAdminMember.sql** script.
4. Commit the changes.

---

## 6.2.8 Configuring the LDAP Settings

This section describes how to integrate the LDAP authentication with Argus Insight and Cognos. Be sure to follow all installation procedures in the specified order:

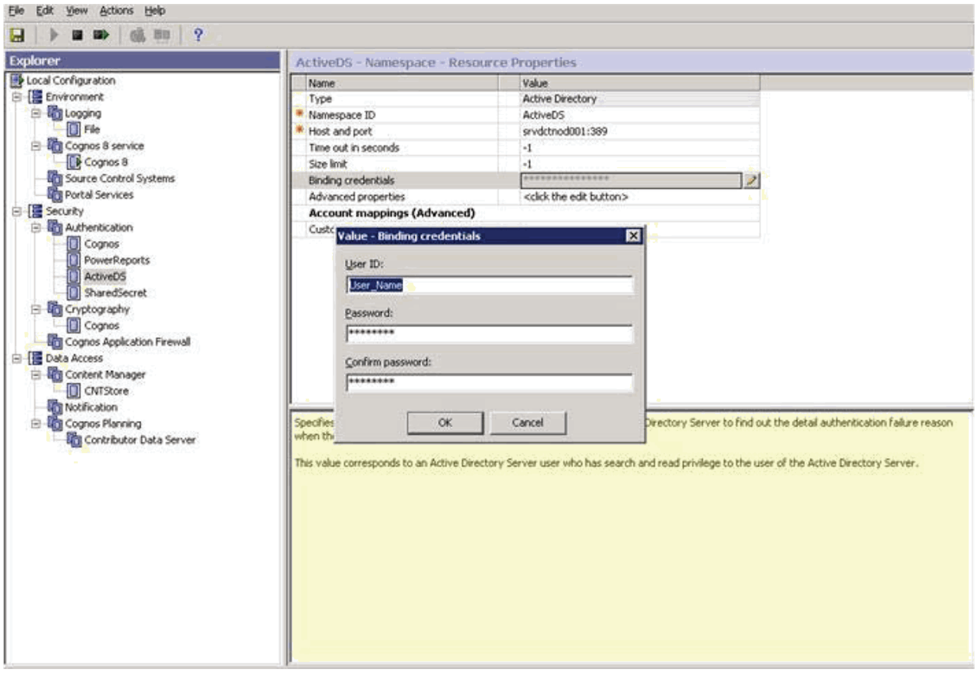
- Configuring the Active Directory
- Configuring LDAP in COGNOS for SunOne
- Setting Up the Cognos LDAP Configuration in Argus Insight
- Setting Up Report Packages for Cognos LDAP

### 6.2.8.1 Configuring the Active Directory

To configure the Active Directory on the Cognos Server:

1. Go to Cognos Server and open the Cognos configuration.

2. Navigate to Security, Authentication, and then add a namespace.
3. Select **Active Directory** as the Type.
4. Configure the Active Directory NameSpace.
5. Provide the Bind credentials, save the configuration, and restart the Cognos service.



ActiveDS - Namespace - Resource Properties

| Name | Value |
|---|---|
| Type | Active Directory |
| Namespace ID | ActiveDS |
| Host and port | srvdctnod001:389 |
| Time out in seconds | -1 |
| Size limit | -1 |
| Binding credentials | *************** |
| Advanced properties | <click the edit button> |
| **Account mappings (Advanced)** | |
| Custc | |

Value - Binding credentials

User ID: User_Name

Password: ********

Confirm password: ********

Specifies … Directory Server to find out the detail authentication failure reason when th…

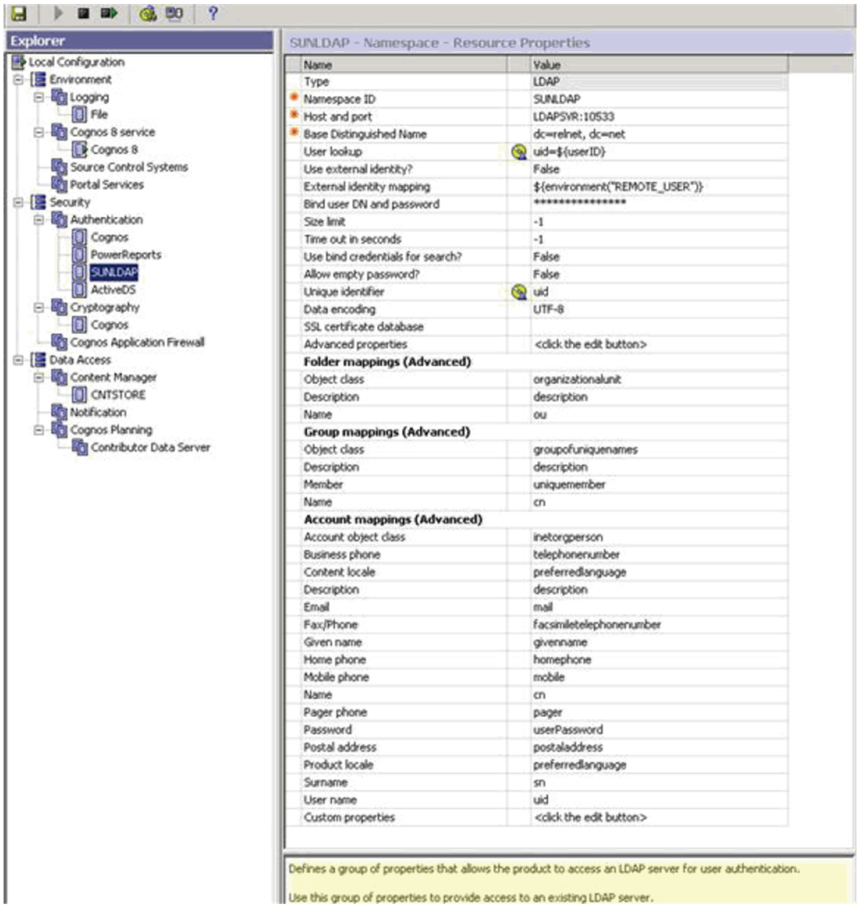
This value corresponds to an Active Directory Server user who has search and read privilege to the user of the Active Directory Server.

6. Click **Modify** and set the value to 1.

### 6.2.8.2 Configuring LDAP in COGNOS for SunOne

To configure LDAP for Active Directory:

1. Configure SunOne on Cognos 8 Server.
2. Go to Cognos Server and open the Cognos configuration.
3. Navigate to **Security, Authentication,** and then add a namespace.
4. Select **LDAP** as the Type.
5. Configure the SunOne NameSpace.
6. Enter NameSpaceID, Host and Port, Base Distinguish Name, user lookup as "uid=$(user ID)" and unique identifier as "uid." No need to enter any bind credentials.



SUNLDAP - Namespace - Resource Properties

| Name | Value |
|---|---|
| Type | LDAP |
| Namespace ID | SUNLDAP |
| Host and port | LDAPSVR:10533 |
| Base Distinguished Name | dc=relnet, dc=net |
| User lookup | uid=${userID} |
| Use external identity? | False |
| External identity mapping | ${environment("REMOTE_USER")} |
| Bind user DN and password | *************** |
| Size limit | -1 |
| Time out in seconds | -1 |
| Use bind credentials for search? | False |
| Allow empty password? | False |
| Unique identifier | uid |
| Data encoding | UTF-8 |
| SSL certificate database | |
| Advanced properties | <click the edit button> |
| **Folder mappings (Advanced)** | |
| Object class | organizationalunit |
| Description | description |
| Name | ou |
| **Group mappings (Advanced)** | |
| Object class | groupofuniquenames |
| Description | description |
| Member | uniquemember |
| Name | cn |
| **Account mappings (Advanced)** | |
| Account object class | inetorgperson |
| Business phone | telephonenumber |
| Content locale | preferredlanguage |
| Description | description |
| Email | mail |
| Fax/Phone | facsimiletelephonenumber |
| Given name | givenname |
| Home phone | homephone |
| Mobile phone | mobile |
| Name | cn |
| Pager phone | pager |
| Password | userPassword |
| Postal address | postaladdress |
| Product locale | preferredlanguage |
| Surname | sn |
| User name | uid |
| Custom properties | <click the edit button> |

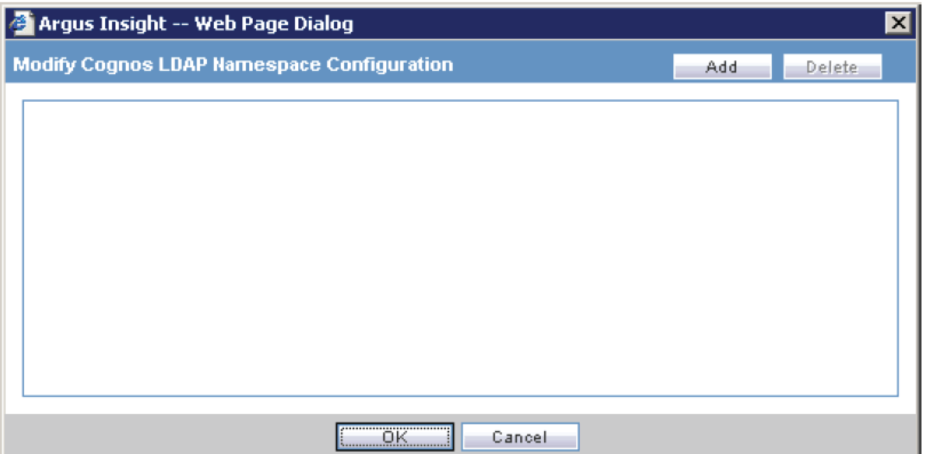
Defines a group of properties that allows the product to access an LDAP server for user authentication.

Use this group of properties to provide access to an existing LDAP server.

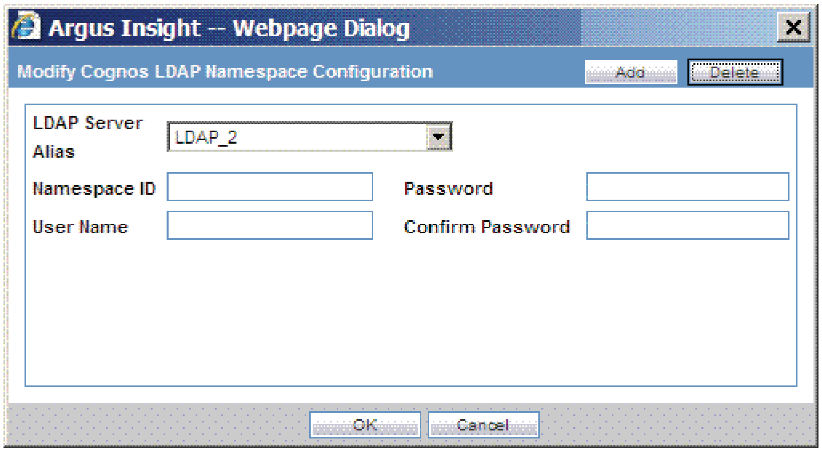
7. Save the Cognos configuration and restart the Cognos service.

### 6.2.8.3 Setting Up the Cognos LDAP Configuration in Argus Insight

1. Log in to the Argus Insight application.
2. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page to open the ADMINISTRATION TOOLS page.
3. Click the **List Maintenance** tab.
4. Select **LDAP** from the List Maintenance Items group. The system updates the right panel with the list of attributes that you can configure.
5. Select the **Cognos LDAP Name Space Configuration** attribute and click **Modify.** The Modify Cognos LDAP Namespace Configuration window opens.


Argus Insight -- Web Page Dialog
Modify Cognos LDAP Namespace Configuration
Add
Delete
OK
Cancel

6. Click **Add.** The Modify Cognos LDAP Namespace Configuration dialog box opens.



7. Complete the Modify Cognos LDAP Namespace Configuration dialog box as follows:
    a. In the **LDAP Server Alias** field, select the LDAP server from the list. This field lists the LDAP servers configured in Argus Safety.
    b. In the **Namespace ID** field, type the namespace identifier for either Active Directory or SunOne (whichever you have configured in Cognos).
    c. In the **User Name** field, type the name of the Cognos and Insight user who is part of a configured LDAP namespace in Cognos and is a Cognos administrator.
    d. In the **Password** field, type the password for the configured Cognos administrator user.
    e. In the **Confirm Password** field, re-type the password for verification.
    f. Click **OK** to save the Cognos LDAP Namespace configuration.

#### 6.2.8.4 Setting Up Report Packages for Cognos LDAP

When Cognos is configured for LDAP authentication, Argus Insight requires a different set of packages and models for Release 7.0.2.

To publish the report packages required for running reports on Cognos with LDAP:

1. Go to Cognos Server.
2. Open the Framework Manager:
   a. Click **Start.**
   b. Navigate to **All Programs, IBM Cognos8,** and select **Framework Manager.**
3. Open the **File** menu and select **Open.**
4. Navigate to the following location:

   `Argus_Insight_Installation_Directory\Oracle\ArgusInsight\Cognos8\Models\LDAP Models`
5. Open the **Compliance** folder.
6. Select the **Compliance.cpf** file, and then click **Open.**
7. Select the configured LDAP namespace to authenticate user.
8. Enter the user credentials to log in.
9. Open the **View** menu and select **Project Viewer.**
   a. In the Project Viewer pane, click **Packages.**
   b. In the project tree, select **Packages,** right-click **Compliance,** and then select **Publish Packages.** The Publish wizard opens.
10. Click **Next** to continue through each of the Publish wizard screens until you have the option to publish the package.
11. Click **Publish.**

    The system displays a message that a package with that name already exists and prompts if you want to overwrite the package.
12. Complete the publish process as follows:
    a. Click **Yes** to overwrite the package.
    b. Click **Finish.**
    c. Click **Close** to exit from the Publish wizard.
13. Open the **File** menu and click **Close.** When the system prompts if you want to save the changes you made to the project, click **No.**
14. Navigate back to the LDAP Models folder (see Step 4), and repeat the process for each package in the LDAP Models folder:
    - Configuration
    - Custom Compliance
    - General
    - Management
    - Pharmacovigilance
    - Report Writer

# 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
- Importing the Repository
- Configuring the BusinessObjects Server
- Configuring the Argus Insight Web Server
- Configuring LDAP Authentication Settings

If you are using Cognos 8 instead of BusinessObjects XI, see Chapter 6 for information about configuring the Cognos 8 environment for Argus Insight.

## 7.1 Checking Requirements

Before attempting to configure 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.

## 7.2 Importing the Repository

Before importing the repository, you must delete all the objects in the Argus Insight folder and its corresponding universe and groups. To access the Argus Insight folder, log on to the Central Management Console on the BusinessObjects Server and click **Folders/All Folders**.

To import the repository:

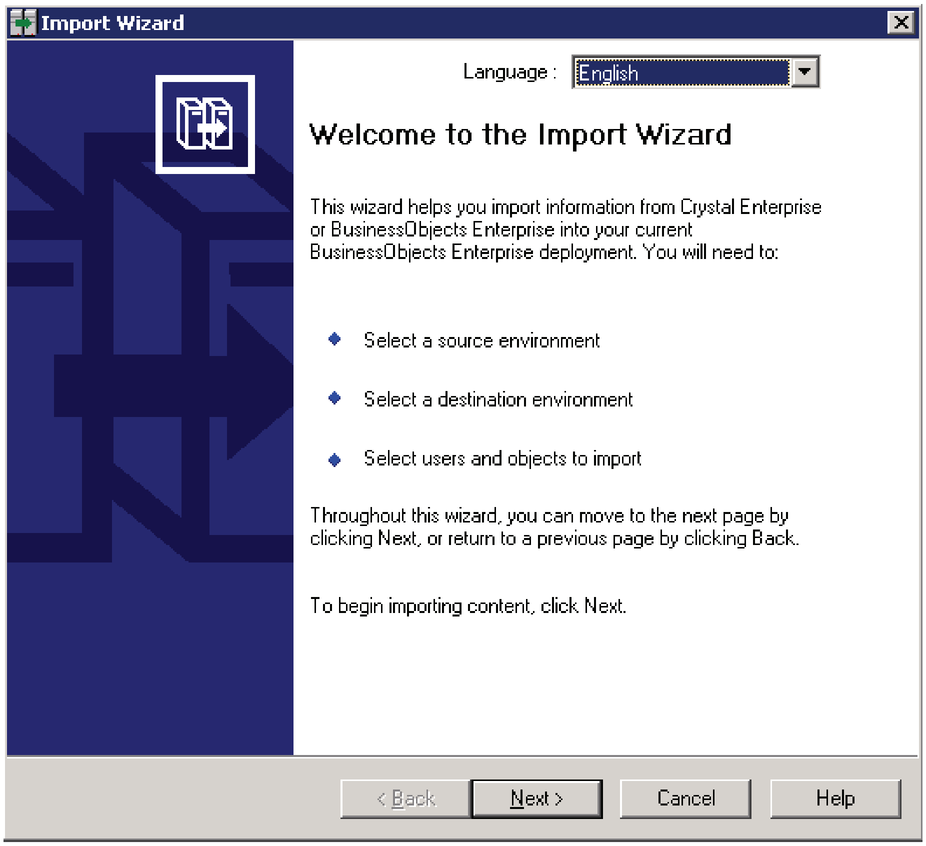
1. Determine if you need to copy the Repository.biar file:

- If BusinessObjects and Argus Insight use the same server, you do not need to copy the Repository.biar file. You can skip this step.
- If BusinessObjects and Argus Insight use different servers, copy the Repository.biar file from this location:

  *Argus_Insight_Web_Server_Location*\\*OracleArgusInsight*\BOXI Repository\

  Paste the file on the BusinessObjects Server.

2. Click **Start.**
3. Navigate to **All Programs, BusinessObjects XI Release 3.1, BusinessObjects Enterprise,** and then select **Import Wizard.** The Welcome screen for the Import Wizard opens.



Welcome to the Import Wizard

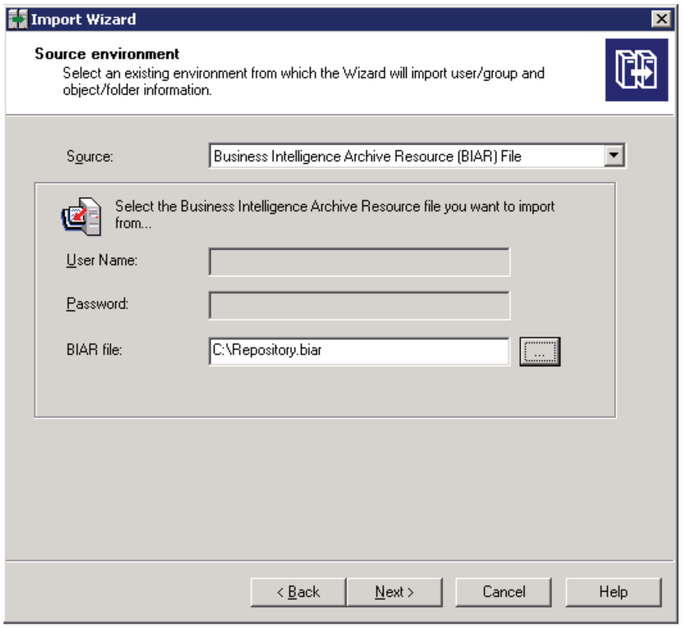
This wizard helps you import information from Crystal Enterprise or BusinessObjects Enterprise into your current BusinessObjects Enterprise deployment. You will need to:

- Select a source environment
- Select a destination environment
- Select users and objects to import

Throughout this wizard, you can move to the next page by clicking Next, or return to a previous page by clicking Back.

To begin importing content, click Next.

4. Click **Next** to begin importing content. The Source environment dialog box opens.



Select an existing environment from which the Wizard will import user/group and object/folder information.

Source: Business Intelligence Archive Resource (BIAR) File

Select the Business Intelligence Archive Resource file you want to import from...

User Name:

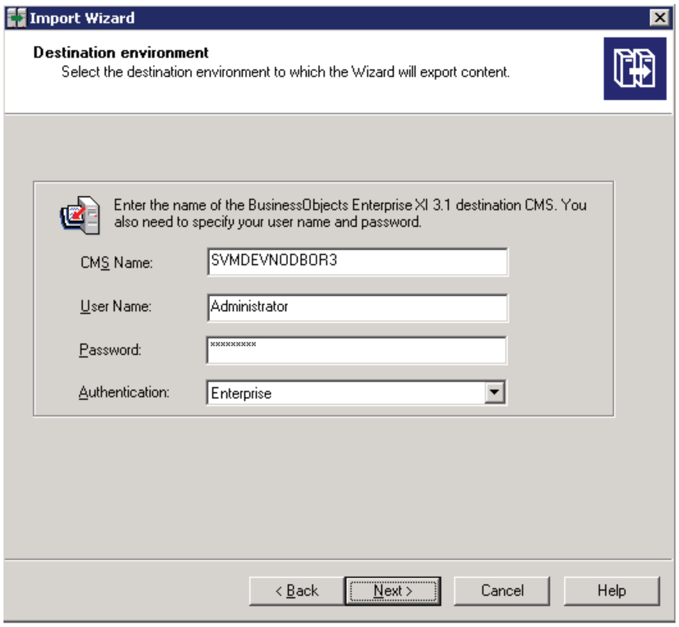
Password:

BIAR file: C:\Repository.biar

a. In the **Source** field, select **Business Intelligence Archive Resource (BIAR) File.**

b. In the **BIAR file** field, browse to the location of the Business Intelligence Archive Resource file that you are using as the source.

5. Click **Next.** The Destination environment dialog box opens.



Select the destination environment to which the Wizard will export content.

Enter the name of the BusinessObjects Enterprise XI 3.1 destination CMS. You also need to specify your user name and password.

CMS Name: SVMDEVNODBOR3

User Name: Administrator

Password: *********

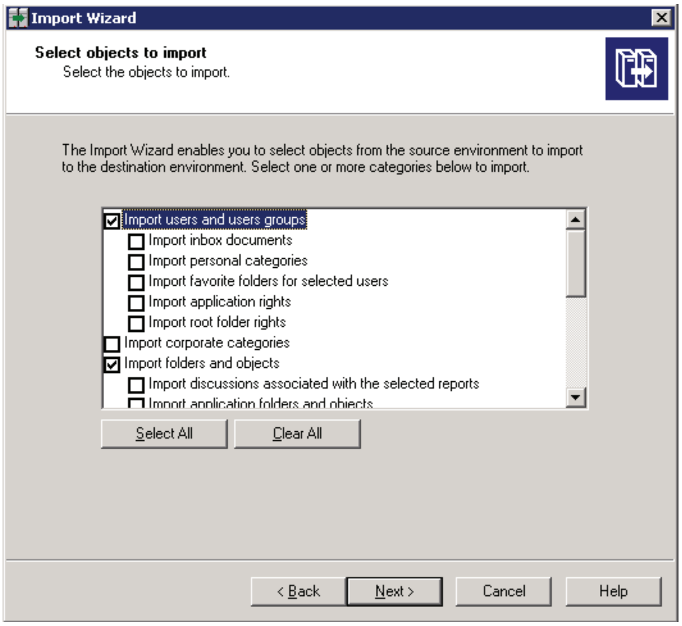
Authentication: Enterprise

a. In the **CMS Name** field, enter the name of the BusinessObjects Server.

b. In the **User Name** field, enter **Administrator.**

c. In the **Password** field, enter the corresponding password for the specified user.

6. Click **Next.** The Import Wizard begins the load process and displays a progress status bar. When done with this process, the wizard opens the Select objects to import dialog box.



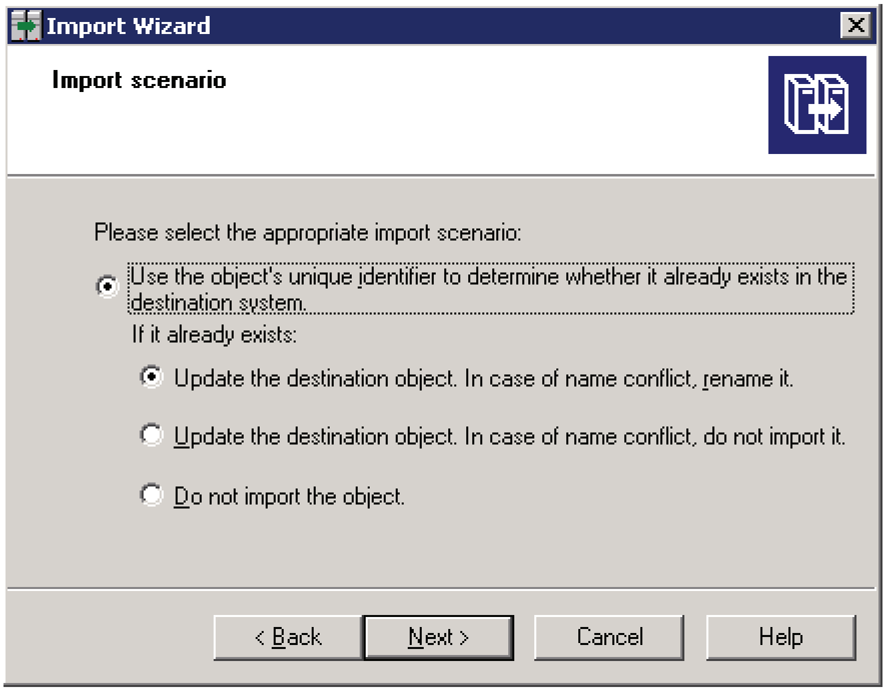
**Select objects to import**

Select the objects to import.

The Import Wizard enables you to select objects from the source environment to import to the destination environment. Select one or more categories below to import.

- ☑ Import users and users groups
  - ☐ Import inbox documents
  - ☐ Import personal categories
  - ☐ Import favorite folders for selected users
  - ☐ Import application rights
  - ☐ Import root folder rights
- ☐ Import corporate categories
- ☑ Import folders and objects
  - ☐ Import discussions associated with the selected reports
  - ☐ Import application folders and objects

7. Scroll through the list and select the following check boxes:
   - **Import users and users groups**
   - **Import folders and objects**
   - **Import universes**
8. Click **Next.** The Import scenario dialog box opens.



**Import scenario**

Please select the appropriate import scenario:

● Use the object's unique identifier to determine whether it already exists in the destination system.

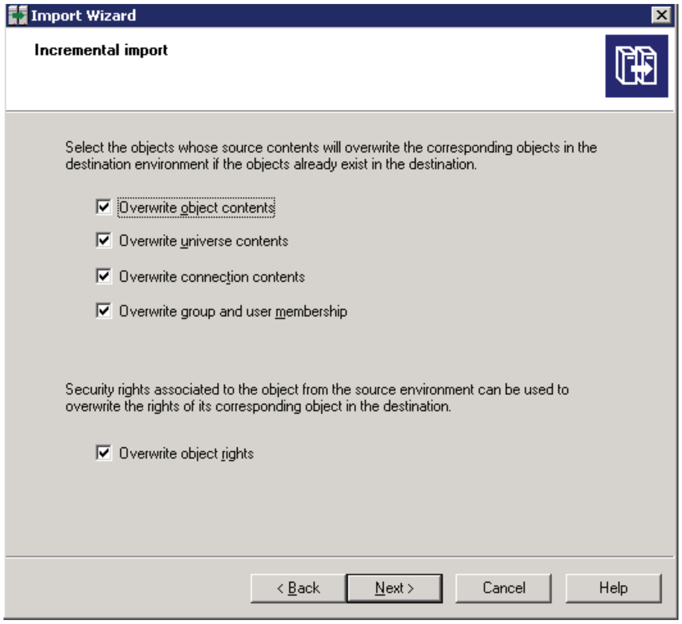
If it already exists:

● Update the destination object. In case of name conflict, rename it.

○ Update the destination object. In case of name conflict, do not import it.

○ Do not import the object.

9. Select how you want the system to process objects that already exist in the destination system.
10. Click **Next.** The Incremental import dialog box opens.



**Incremental import**

Select the objects whose source contents will overwrite the corresponding objects in the destination environment if the objects already exist in the destination.

☑ Overwrite object contents

☑ Overwrite universe contents

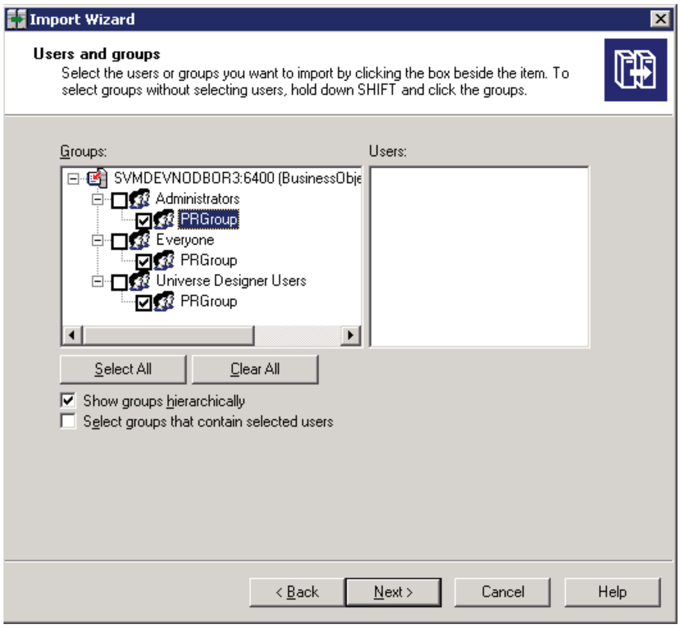
☑ Overwrite connection contents

☑ Overwrite group and user membership

Security rights associated to the object from the source environment can be used to overwrite the rights of its corresponding object in the destination.

☑ Overwrite object rights

11. Select all check boxes.
12. Click **Next.** The Users and groups dialog box opens.



**Users and groups**

Select the users or groups you want to import by clicking the box beside the item. To select groups without selecting users, hold down SHIFT and click the groups.

SVMDEVNODBOR3:6400 (BusinessObje
- ☐ Administrators
  - ☑ PRGroup
- ☐ Everyone
  - ☑ PRGroup
- ☐ Universe Designer Users
  - ☑ PRGroup

☑ Show groups hierarchically

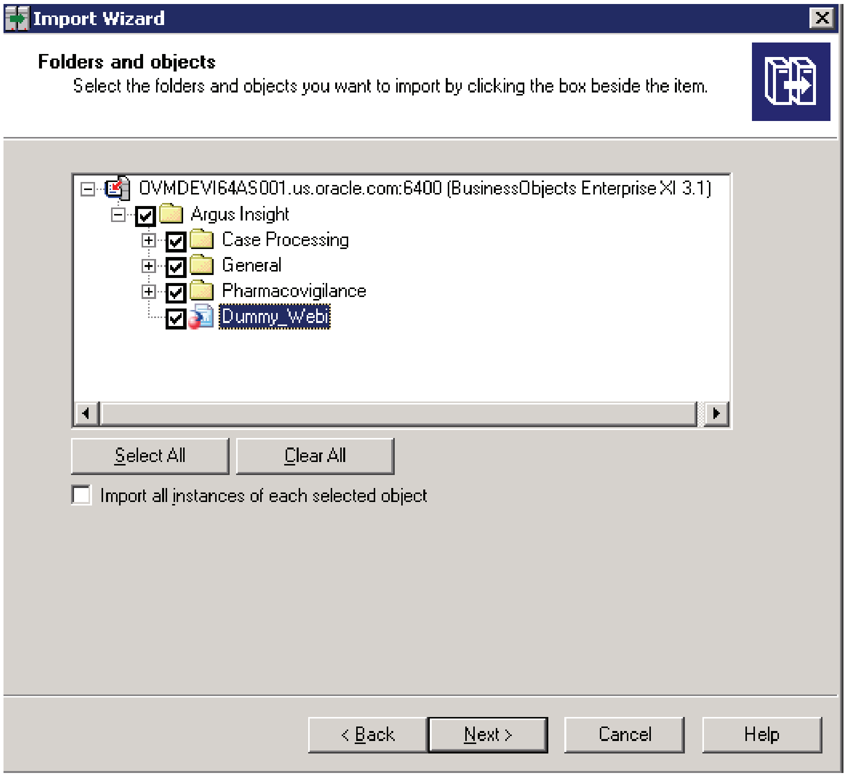
☐ Select groups that contain selected users

---

**Note:** The appearance of the preceding dialog box depends on the environment and on the BusinessObjects Server configuration for your system.

---

13. Select the users and groups you want to import.
14. Click **Next.**
15. Set the custom access levels.
16. Click **Next.** The Folders and objects dialog box opens.



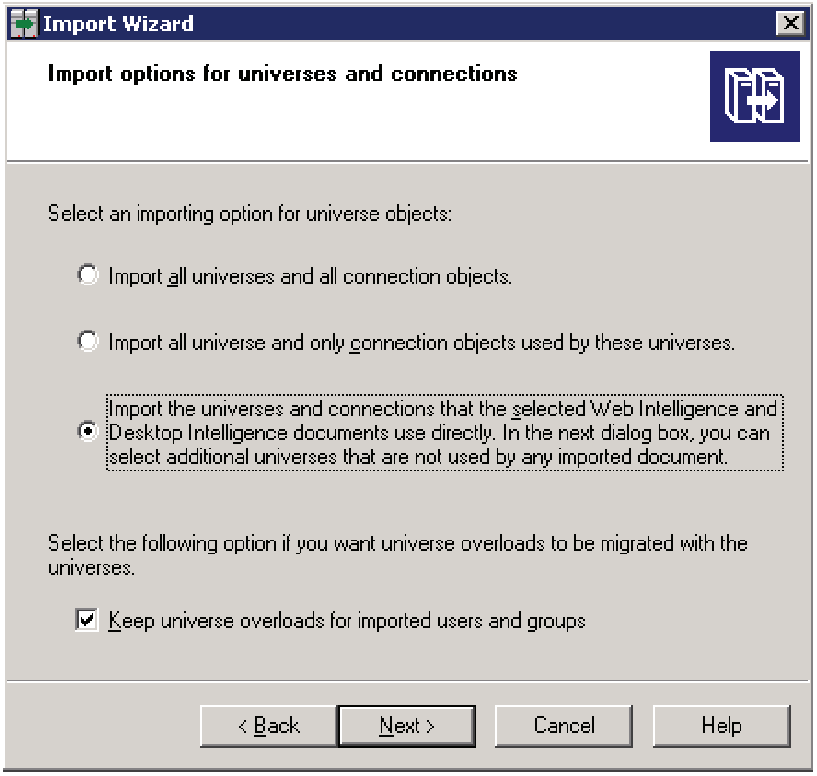
**Folders and objects**

Select the folders and objects you want to import by clicking the box beside the item.

- OVMDEVI64AS001.us.oracle.com:6400 (BusinessObjects Enterprise XI 3.1)
  - ☑ Argus Insight
    - ☑ Case Processing
    - ☑ General
    - ☑ Pharmacovigilance
    - ☑ Dummy_Webi

☐ Import all instances of each selected object

17. Select the folders and objects you want to import.
18. Click **Next.** The Import options for universes and connections dialog box opens.



**Import options for universes and connections**

Select an importing option for universe objects:

○ Import all universes and all connection objects.

○ Import all universe and only connection objects used by these universes.

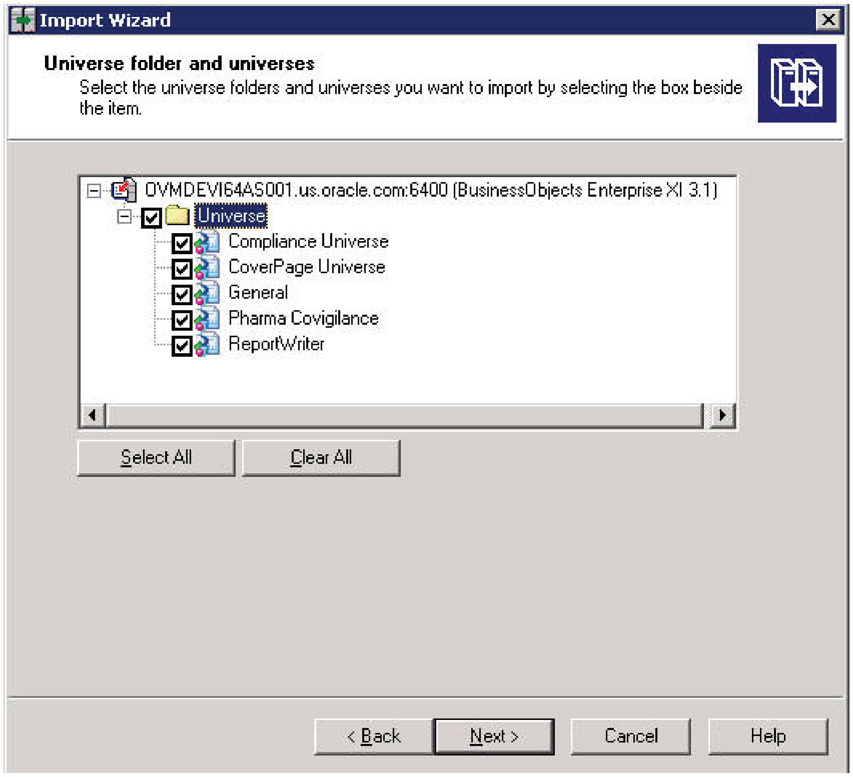
● Import the universes and connections that the selected Web Intelligence and Desktop Intelligence documents use directly. In the next dialog box, you can select additional universes that are not used by any imported document.

Select the following option if you want universe overloads to be migrated with the universes.

☑ Keep universe overloads for imported users and groups

19. Select the appropriate options as shown in the previous illustration.

**20.** Click **Next.** The Universe folder and universes dialog box opens.



**Universe folder and universes**

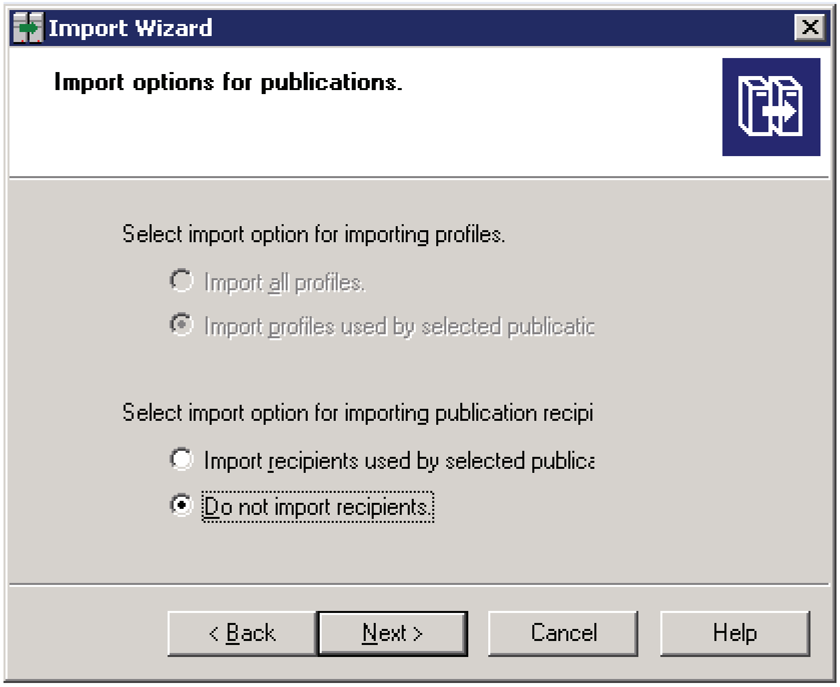
Select the universe folders and universes you want to import by selecting the box beside the item.

- OVMDEVI64AS001.us.oracle.com:6400 (BusinessObjects Enterprise XI 3.1)
  - ☑ Universe
    - ☑ Compliance Universe
    - ☑ CoverPage Universe
    - ☑ General
    - ☑ Pharma Covigilance
    - ☑ ReportWriter

a. Click **Clear All.**

b. Select the check box for the root Universe folder.

**21.** Click **Next.** The Import options for publications dialog box opens.



**Import options for publications.**

Select import option for importing profiles.

○ Import all profiles.

● Import profiles used by selected publicatic

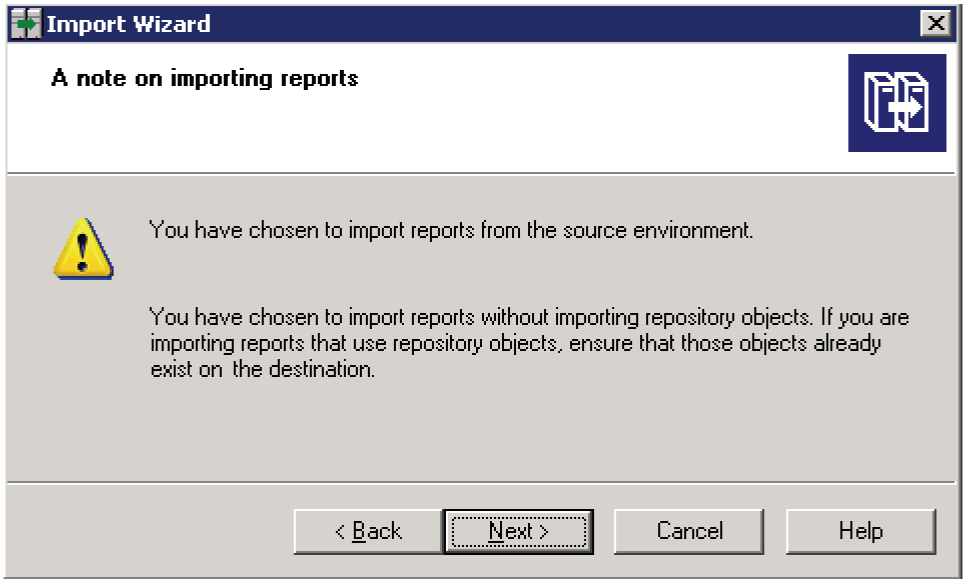
Select import option for importing publication recipi

○ Import recipients used by selected publica

● Do not import recipients.

**22.** Select **Do not import recipients.**

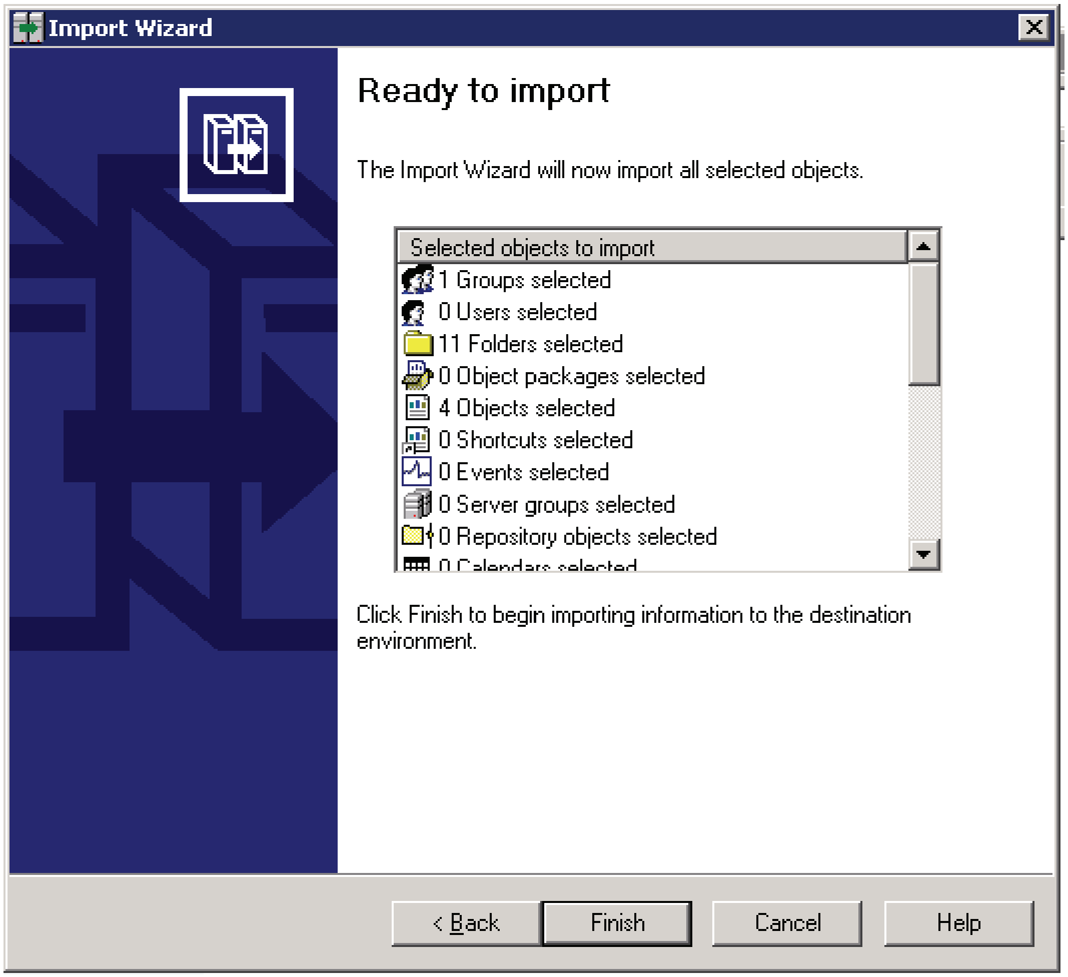
**23.** Click **Next.** The system displays a message that you have chosen to import reports from the source environment without importing the repository objects. If you are importing reports that use repository objects, you must ensure that those objects already exist on the destination.



You have chosen to import reports from the source environment.

You have chosen to import reports without importing repository objects. If you are importing reports that use repository objects, ensure that those objects already exist on the destination.

**24.** Click **Next.** The Ready to import dialog box opens.



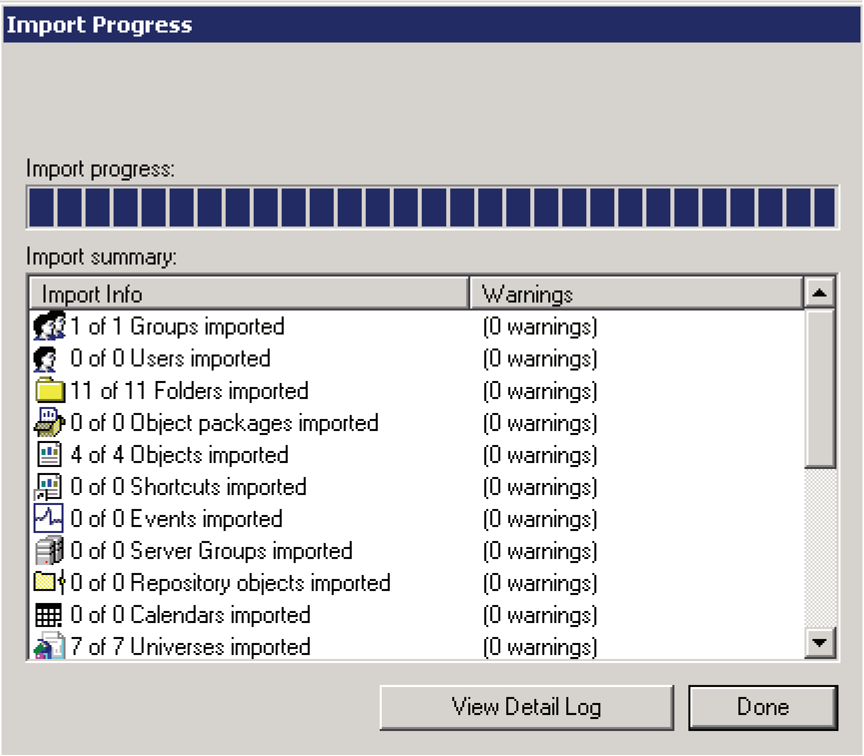
Ready to import

The Import Wizard will now import all selected objects.

Selected objects to import
1 Groups selected
0 Users selected
11 Folders selected
0 Object packages selected
4 Objects selected
0 Shortcuts selected
0 Events selected
0 Server groups selected
0 Repository objects selected
0 Calendars selected

Click Finish to begin importing information to the destination environment.

**25.** Click **Finish** to begin importing information to the destination environment. The system opens the Import Progress dialog box and updates the screen with status information during the import process.



| Import Info | Warnings |
|---|---|
| 1 of 1 Groups imported | (0 warnings) |
| 0 of 0 Users imported | (0 warnings) |
| 11 of 11 Folders imported | (0 warnings) |
| 0 of 0 Object packages imported | (0 warnings) |
| 4 of 4 Objects imported | (0 warnings) |
| 0 of 0 Shortcuts imported | (0 warnings) |
| 0 of 0 Events imported | (0 warnings) |
| 0 of 0 Server Groups imported | (0 warnings) |
| 0 of 0 Repository objects imported | (0 warnings) |
| 0 of 0 Calendars imported | (0 warnings) |
| 7 of 7 Universes imported | (0 warnings) |

When the import is complete, you can:

- Click **View Detail Log** for more information about the import.
- Click **Done** to close the dialog box.

## 7.3 Configuring the BusinessObjects Server

The sections describes the following tasks that you must complete to configure the BusinessObjects Server:

- Copying the PRMART TNS Entry
- Logging On to the Central Management Console
- Configuring Trusted Authentication for BusinessObjects
- Changing the Connection String for Universe
- Configuring PRGroup Settings
- Configuring Argus Insight Folder Rights
- Configuring BusinessObjects Applications Rights

### 7.3.1 Copying the PRMART TNS Entry

If the BusinessObjects application uses a different server from the Argus Insight application, you must update the TNSNAMES.ora file as follows:

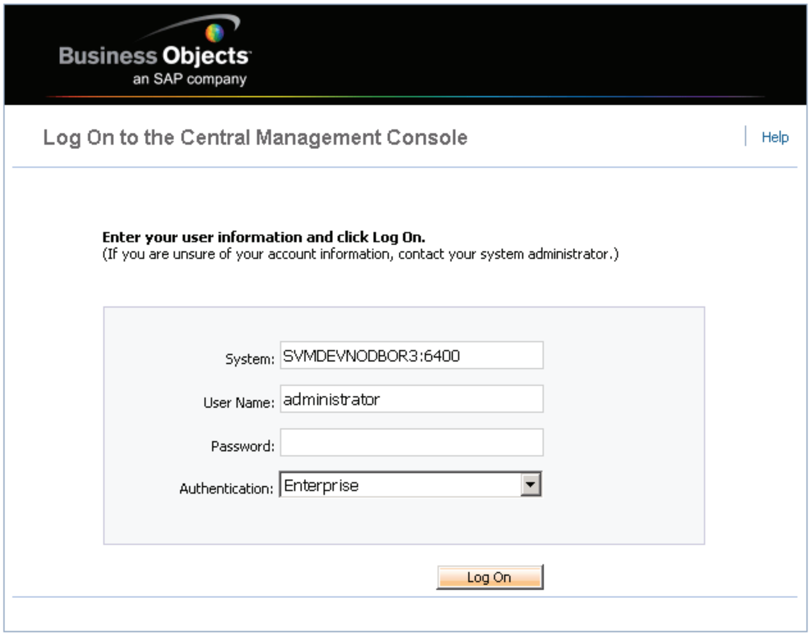
1. Copy the PRMART TNS entry from the Argus Insight Web Server.
2. Paste the entry into the TNSNAMES.ora file on the BusinessObjects Server.

If both applications use the same server and Oracle client, no modifications to the TNSNAMES.ora file are required.

### 7.3.2 Logging On to the Central Management Console

To log on to the Central Management Console on the BusinessObjects Server:

1. Click **Start.**
2. Navigate to **All Programs, BusinessObjects XI Release 3.1, BusinessObjects Enterprise,** and then select **BusinessObjects Enterprise Central Management Console.** The Logon page for the Central Management Console opens.



Enter your user information and click Log On.
(If you are unsure of your account information, contact your system administrator.)

System: SVMDEVNODBOR3:6400
User Name: administrator
Password:
Authentication: Enterprise

3. Enter your user name and password.
4. Click **Log On.**

### 7.3.3 Configuring Trusted Authentication for BusinessObjects

Trusted Authentication provides a transparent, single sign-on solution to the problem of how to integrate your BusinessObjects Enterprise authentication solution with third-party authentication solutions.

Once users log on to the system, they do not want to have to provide their password more than once in a session. In this scenario, Trusted Authentication allows applications that have established trust with the Central Management Server to log on users without their password.

To enable Trusted Authentication, you must configure both the BusinessObjects Server and the Argus Insight Web Server.

To configure the server to use Trusted Authentication:

1. Log on to the Central Management Console as a user with administrator privileges.
2. Click **Authentication** from the Home page.
3. Double-click **Enterprise.**
4. Select the **Trusted Authentication is enabled** check box.
5. Create a shared secret for your users.

---

**Note:** The Argus Insight Web Server and the Central Management Console use the shared secret to create a trusted authentication password. In other words, the systems use this secret password to establish trust.

---

6. Enter a timeout value for your trusted authentication requests.

---

**Note:** The timeout value determines how long the Central Management Console waits for the SessionMgr.Logon call from Argus Insight. The recommended timeout value is **0** (zero).

---

7. Click **Update.**

#### 7.3.3.1 Configuring the Argus Insight Web Server to Use Trusted Authentication

When creating a valid configuration file on the Argus Insight Web Server, the following conditions apply to the configuration file:

- The name of the file must be TrustedPrincipal.conf.
- The file must be placed at this location:

  businessobjects_root/win32_x86
- The file must contain the line:

  `SharedSecret=secret_password`

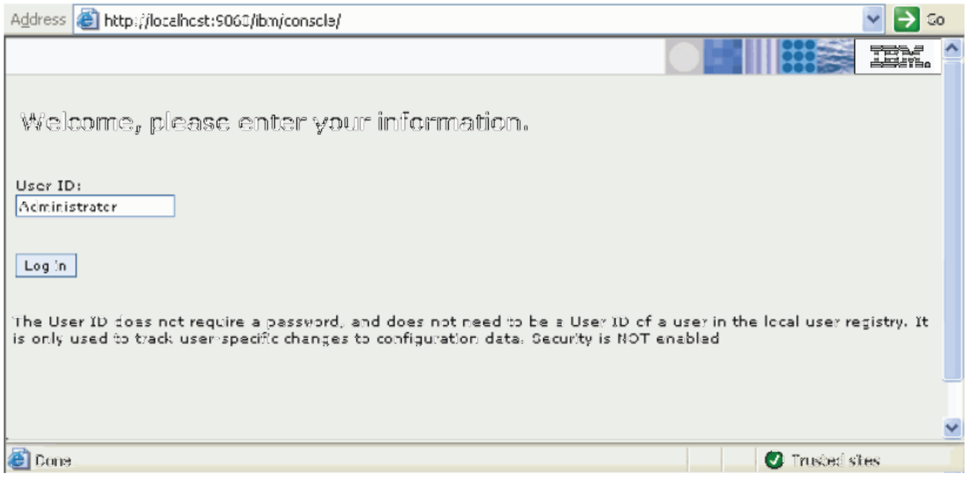
  where *secret_password* is the trusted authentication password.
- The file must be saved with UTF-8 encoding if it contains non-ASCII characters.
- Either Tomcat or WebSphere must be installed on the BusinessObjects Server.

#### 7.3.3.2 Configuring WebSphere

If Tomcat is not installed on the BusinessObjects Server, configure WebSphere as follows:

1. Verify that WebSphere 6.0 is installed and working correctly. To do so, launch either its default page or administrative console in a web browser. Generally, the default path to WebSphere is as follows:

   `http://localhost:9060/ibm/console/`



Welcome, please enter your information.

User ID: Administrator

The User ID does not require a password, and does not need to be a User ID of a user in the local user registry. It is only used to track user-specific changes to configuration data. Security is NOT enabled

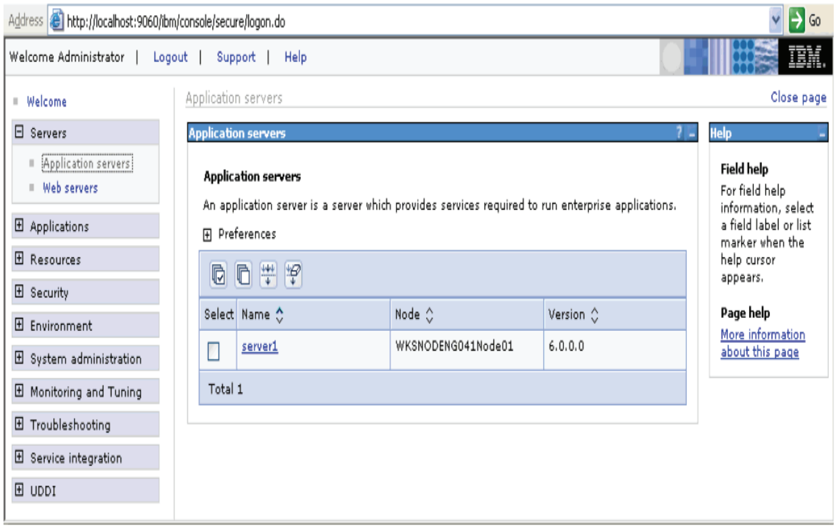
2. Verify and install the latest Java Virtual Machine (JVM) on the WebSphere computer.

3. Install BusinessObjects. During the installation setup, ensure that you deselect the Tomcat Server installation option.

4. Configure the WebSphere Server. First, change the class path as follows:

   a. Restart the WebSphere Administrative console.

   b. Expand the Servers group in the navigation pane of the Administrative console.



**Application servers**

An application server is a server which provides services required to run enterprise applications.

| Select | Name | Node | Version |
|---|---|---|---|
| ☐ | server1 | WKSNODENG041Node01 | 6.0.0.0 |
| Total 1 | | | |

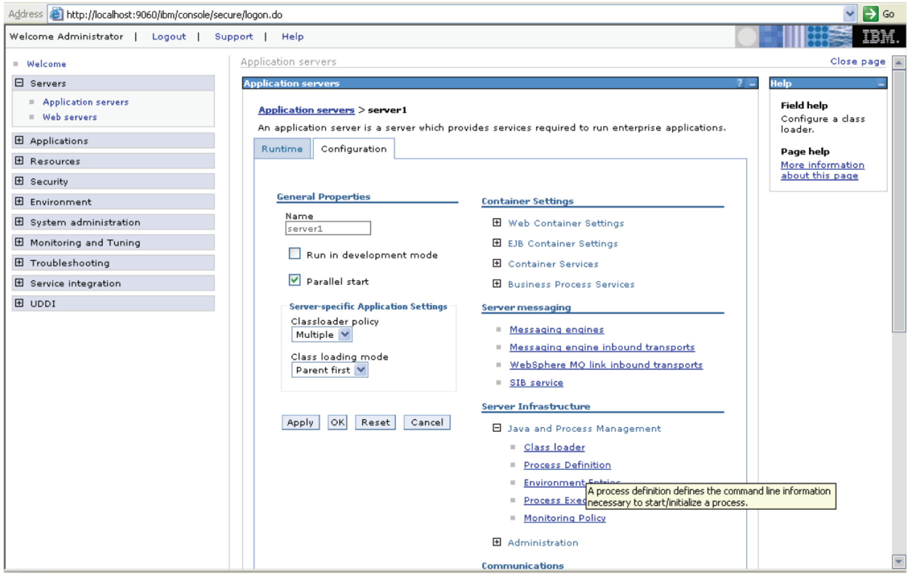
**Field help**

For field help information, select a field label or list marker when the help cursor appears.

**Page help**

More information about this page

   c. Click **Application Servers,** and then click the **server1** link. The system opens the settings page for the server.



An application server is a server which provides services required to run enterprise applications.

Name: server1

☐ Run in development mode

☑ Parallel start

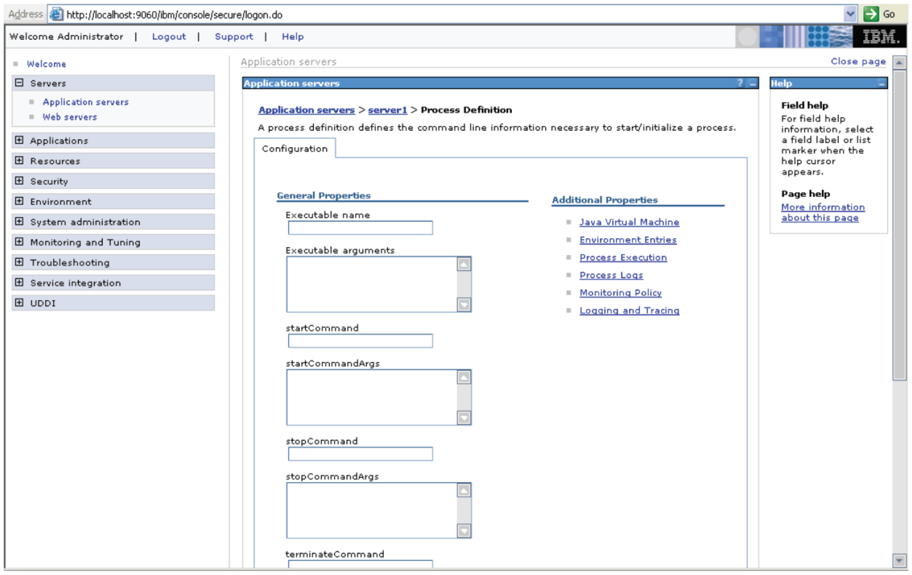
Classloader policy: Multiple

Class loading mode: Parent first

Configure a class loader.

A process definition defines the command line information necessary to start/initialize a process.

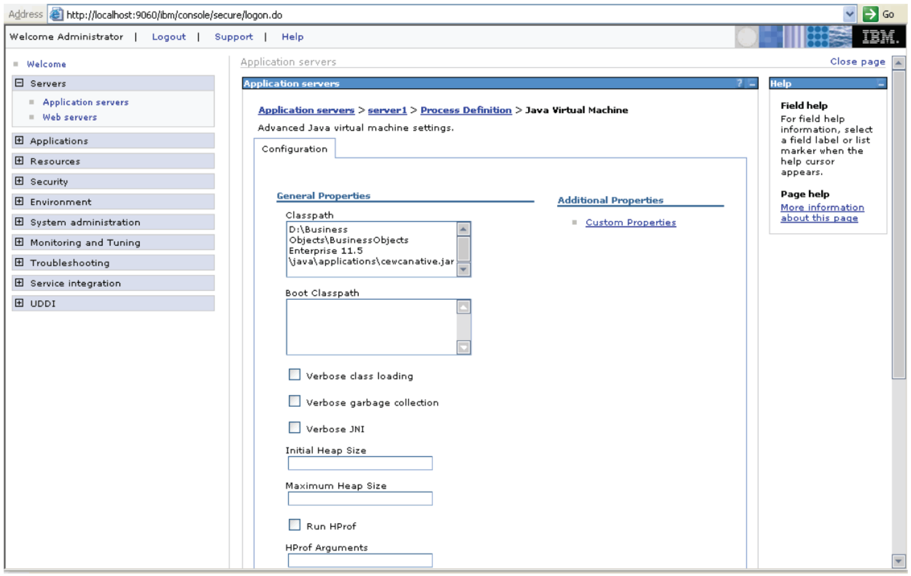
**d.** Click the **Configuration** tab, and then click the **Process Definition** link in the Server Infrastructure group. The Process Definition page opens.



A process definition defines the command line information necessary to start/initialize a process.

For field help information, select a field label or list marker when the help cursor appears.

**e.** Click the **Java Virtual Machine** link in the Additional Properties group. The Java Virtual Machine settings page opens.



Address: http://localhost:9060/ibm/console/secure/logon.do

Application servers > server1 > Process Definition > Java Virtual Machine

Advanced Java virtual machine settings.

Classpath: D:\Business Objects\BusinessObjects Enterprise 11.5 \java\applications\cewcanative.jar

☐ Verbose class loading

☐ Verbose garbage collection

☐ Verbose JNI

☐ Run HProf

For field help information, select a field label or list marker when the help cursor appears.

- **f.** Click the **Classpath** field in the General Properties section, and enter the complete path to the cewcanative.jar file. The default location is:

  *drive*:\Business Objects\BusinessObjects Enterprise 11.5\java\applications

- **g.** Save your changes to the master configuration.

**5.** Change the Path environmental variable as follows:

- **a.** Note the location of the win32_X86 folder in the BusinessObjects Enterprise software installation. The default location is:

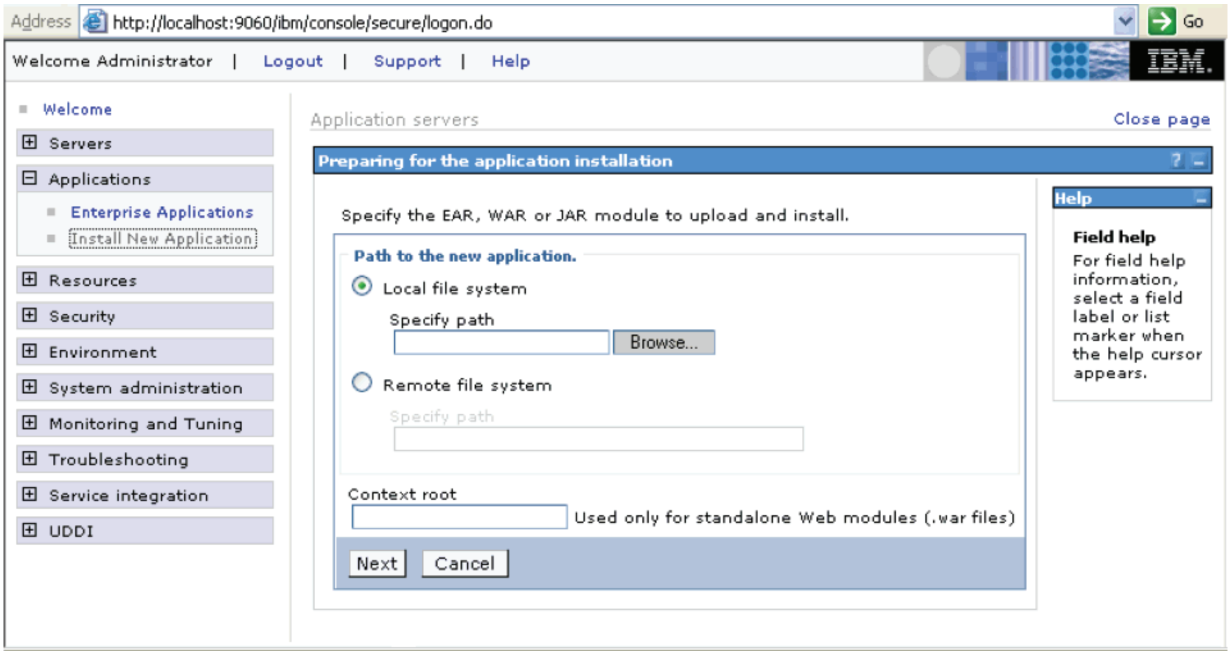
  *drive:*\Program Files\Business Objects\BusinessObjects Enterprise 11.5\win32_X86

- **b.** Right-click the **My Computer** icon on your desktop, and select **Properties.**
- **c.** Click the **Advanced** tab.
- **d.** Click **Environment Variables.**
- **e.** Scroll through the list of system variables until you find the Path variable.
- **f.** Select the **Path** variable and then click **Edit.**
- **g.** Position the cursor at the end of the information in the **Variable value** field.
- **h.** Add a semicolon (;) and then enter the complete path to the location of the win32_X86 folder.
- **i.** Click **OK** to save your changes and close the Edit System Variable dialog box.
- **j.** Click **OK** to close the Environment Variables dialog box.
- **k.** Click **OK** to close the System Properties dialog box.

#### 7.3.3.3 Deploying the WebSphere Server

To deploy the WebSphere Server:

1. Open the Administrative console.
2. Expand **Applications,** and then click **Install New Application.**



Specify the EAR, WAR or JAR module to upload and install.

Path to the new application.

● Local file system

Specify path

○ Remote file system

Specify path

Context root

Used only for standalone Web modules (.war files)

Field help

For field help information, select a field label or list marker when the help cursor appears.

a. Click **Browse** to enter the complete path to the location of the styles.war file. The default location is:

   *drive*:\Program Files\business objects\businessobjects enterprise 11.5\java\applications

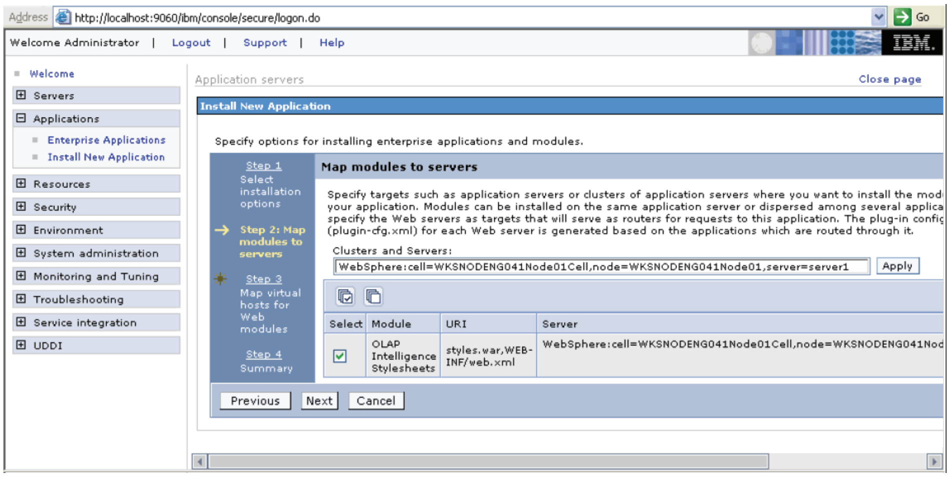
b. Type the context root for the WAR file in the **Context Root** field. See Table 7–1 for the order and the context root of various files to be deployed.

c. Click **Next.**

*Table 7–1 WAR Files to Be Deployed*

| WAR File | Context Root |
|---|---|
| Desktop.war | /businessobjects/enterprise115/desktoplaunch/businessobjects |
| Webcompadapter.war | /businessobjects |
| Jsfadmin.war | /jsfadmin |
| Admin.war | /businessobjects/enterprise115/adminlaunch |
| Adhoc.war | /businessobjects/enterprise115/Adhoc |

3. Accept the default values on the subsequent pages and continue to click **Next** until you get to Step 2: Map modules to servers.



Specify options for installing enterprise applications and modules.

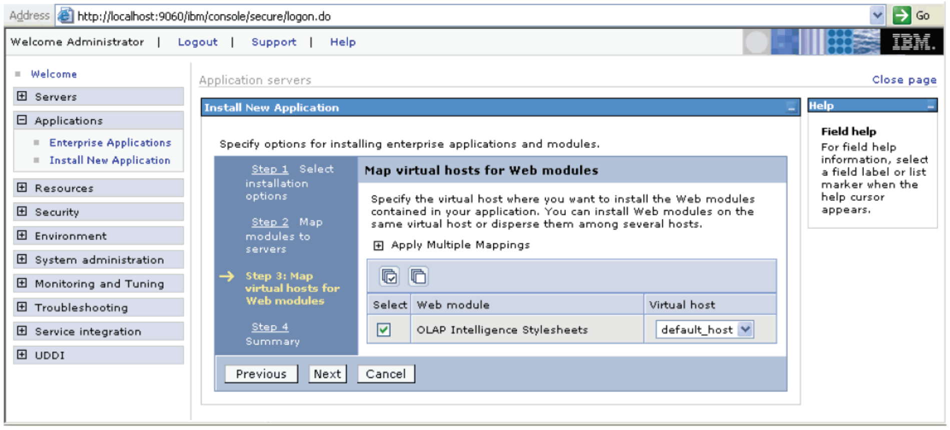
**Map modules to servers**

Specify targets such as application servers or clusters of application servers where you want to install the mod your application. Modules can be installed on the same application server or dispersed among several applica specify the Web servers as targets that will serve as routers for requests to this application. The plug-in confic (plugin-cfg.xml) for each Web server is generated based on the applications which are routed through it.

Clusters and Servers: WebSphere:cell=WKSNODENG041Node01Cell,node=WKSNODENG041Node01,server=server1

| Select | Module | URI | Server |
|---|---|---|---|
| ☑ | OLAP Intelligence Stylesheets | styles.war,WEB-INF/web.xml | WebSphere:cell=WKSNODENG041Node01Cell,node=WKSNODENG041Nod |

4. Select the Application Server (that is, server1) and click **Next.** The system continues to Step 3.



Specify options for installing enterprise applications and modules.

**Map virtual hosts for Web modules**

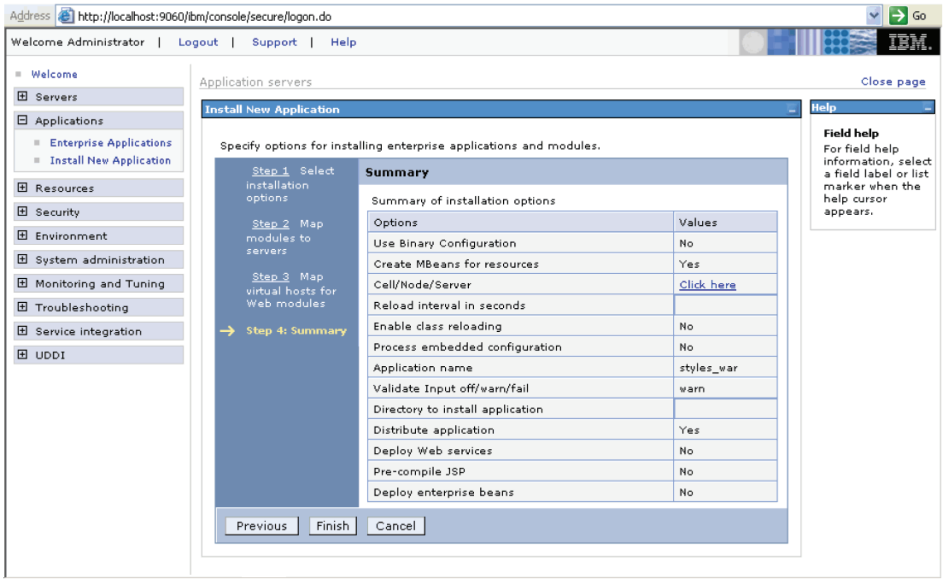
Specify the virtual host where you want to install the Web modules contained in your application. You can install Web modules on the same virtual host or disperse them among several hosts.

| Select | Web module | Virtual host |
|---|---|---|
| ☑ | OLAP Intelligence Stylesheets | default_host |

**Field help**

For field help information, select a field label or list marker when the help cursor appears.

5. Select the web module in the list and click **Next.** The system continues to Step 4 and displays the summary of installation options.



Specify options for installing enterprise applications and modules.

**Summary**

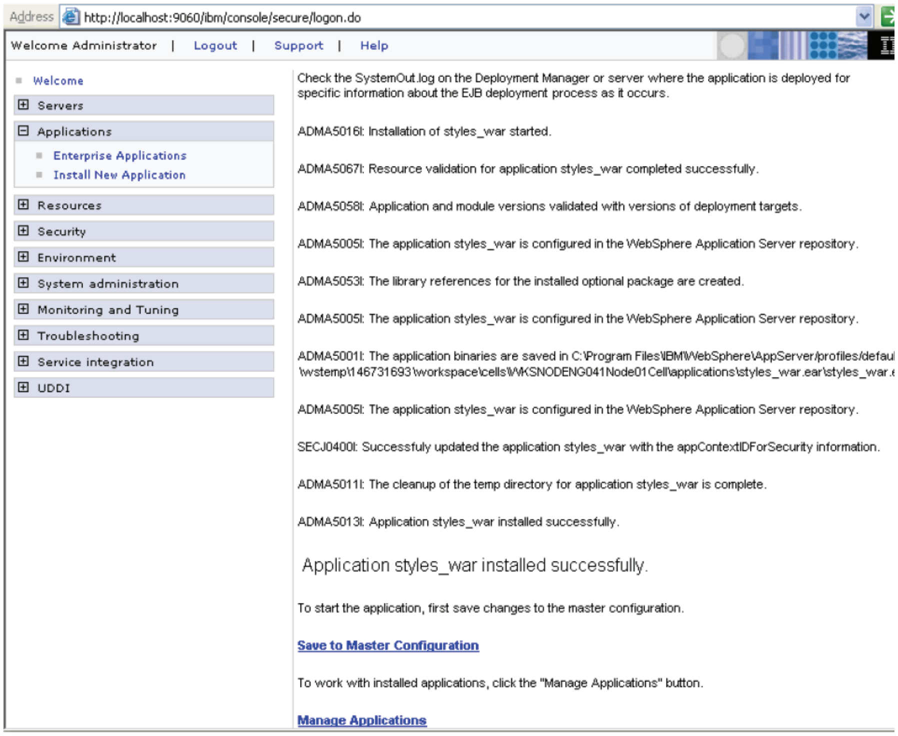
Summary of installation options

| Options | Values |
|---|---|
| Use Binary Configuration | No |
| Create MBeans for resources | Yes |
| Cell/Node/Server | Click here |
| Reload interval in seconds | |
| Enable class reloading | No |
| Process embedded configuration | No |
| Application name | styles_war |
| Validate Input off/warn/fail | warn |
| Directory to install application | |
| Distribute application | Yes |
| Deploy Web services | No |
| Pre-compile JSP | No |
| Deploy enterprise beans | No |

**Field help**

For field help information, select a field label or list marker when the help cursor appears.

6. Click **Finish.** The system displays progress messages and reports when the installation of the application file has been installed successfully.



```
Check the SystemOut.log on the Deployment Manager or server where the application is deployed for
specific information about the EJB deployment process as it occurs.

ADMA5016I: Installation of styles_war started.

ADMA5067I: Resource validation for application styles_war completed successfully.

ADMA5058I: Application and module versions validated with versions of deployment targets.

ADMA5005I: The application styles_war is configured in the WebSphere Application Server repository.

ADMA5053I: The library references for the installed optional package are created.

ADMA5005I: The application styles_war is configured in the WebSphere Application Server repository.

ADMA5001I: The application binaries are saved in C:\Program Files\IBM\WebSphere\AppServer/profiles/defau
\wstemp\146731693\workspace\cells\WKSNODENG041Node01Cell\applications\styles_war.ear\styles_war.

ADMA5005I: The application styles_war is configured in the WebSphere Application Server repository.

SECJ0400I: Successfuly updated the application styles_war with the appContextIDForSecurity information.

ADMA5011I: The cleanup of the temp directory for application styles_war is complete.

ADMA5013I: Application styles_war installed successfully.
```

Application styles_war installed successfully.

To start the application, first save changes to the master configuration.

Save to Master Configuration

To work with installed applications, click the "Manage Applications" button.

Manage Applications

7. Click **Save to Master Configuration** to save the installation changes.
8. Repeat the process for each file listed in Table 7–1, " WAR Files to Be Deployed". Remember to deploy the files in the order listed in Table 7–1, otherwise, the integration will fail because these files have dependencies on each other.
9. Verify that BusinessObjects has been integrated successfully with WebSphere:
   a. Open a browser window.
   b. Use the following format to enter the URL for the desktop launchpad:

      http://*host_name*:*port_number*/businessobjects/enterprise115/desktoplaunch

      For example:

      http://localhost:9080/businessobjects/enterprise115/desktoplaunch

---

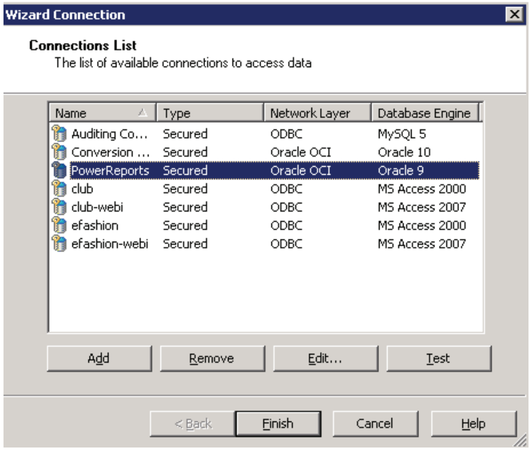
**Note:** You **cannot** use the shortcuts in the BusinessObjects Enterprise program group to access the BusinessObjects Enterprise launchpads deployed on your WebSphere Server. To access them, you must include the port number of the WebSphere Server in your URL.

---

### 7.3.4 Changing the Connection String for Universe

To change the connection string:

1. Start the BusinessObjects Universe Designer application.
2. Open the **Tools** menu and select **Connections.** The Wizard Connection dialog box opens.



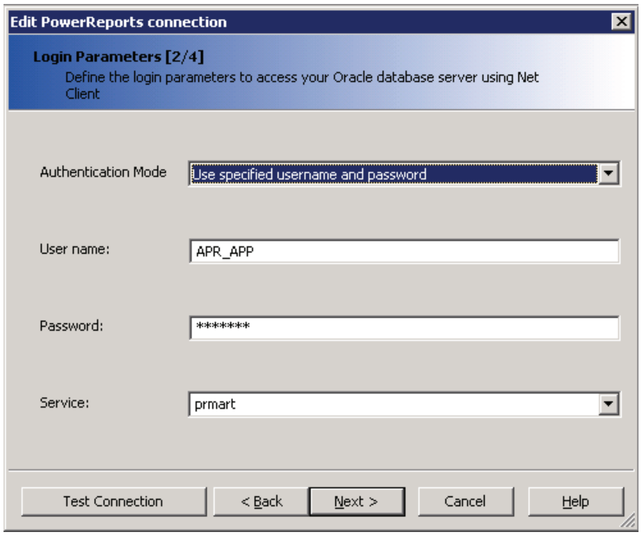
Wizard Connection

**Connections List**

The list of available connections to access data

| Name | Type | Network Layer | Database Engine |
|---|---|---|---|
| Auditing Co... | Secured | ODBC | MySQL 5 |
| Conversion ... | Secured | Oracle OCI | Oracle 10 |
| PowerReports | Secured | Oracle OCI | Oracle 9 |
| club | Secured | ODBC | MS Access 2000 |
| club-webi | Secured | ODBC | MS Access 2007 |
| efashion | Secured | ODBC | MS Access 2000 |
| efashion-webi | Secured | ODBC | MS Access 2007 |

3. Select **PowerReports** and click **Edit** to modify the connection.
   - If the current PowerReports connection was edited with a previous version, the system prompts for confirmation that you want to edit the connection. Click **Yes** to continue. The Edit PowerReports connection dialog box opens.
   - If the current PowerReports connection was not edited with a previous version, the Edit PowerReports connection dialog box opens.



Edit PowerReports connection

**Login Parameters [2/4]**

Define the login parameters to access your Oracle database server using Net Client

Authentication Mode: Use specified username and password

User name: APR_APP

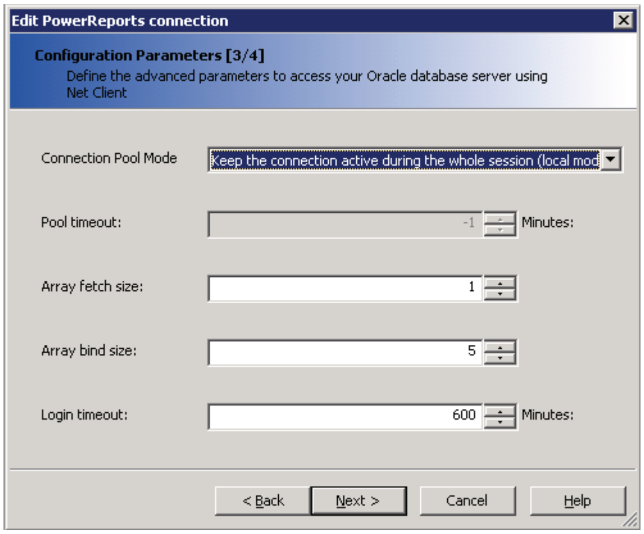
Password: *******

Service: prmart

4. Enter the user name and password for Argus Insight database read-only user / APR_APP user. The read-only user is created during schema creation. For example, APR_MART_DB_LINK_USER.

> **Note:** APR_APP user has rights to update many of the MART tables. If user wants to use read-only account for BusinessObjects connection they can use APR_MART_DB_LINK_USER account, but Case Series Freezing will not be supported in Reports and Report Writer with the use of read-only account.

5. Click **Next.** The Configuration Parameters dialog box opens.



**Configuration Parameters [3/4]**

Define the advanced parameters to access your Oracle database server using Net Client

Connection Pool Mode: Keep the connection active during the whole session (local mod

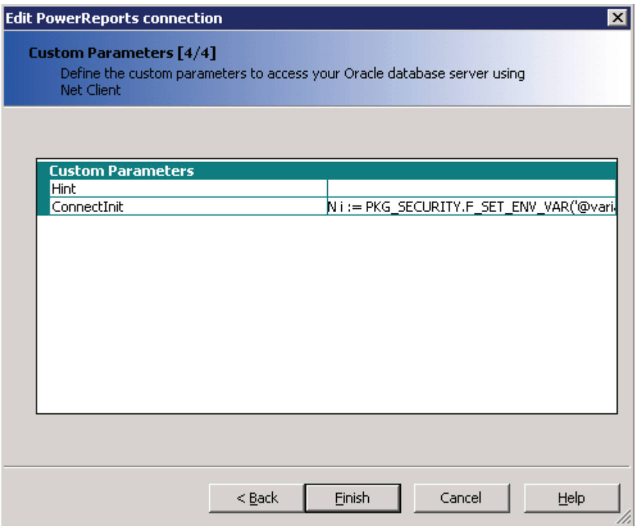
Pool timeout: -1 Minutes:

Array fetch size: 1

Array bind size: 5

Login timeout: 600 Minutes:

6. Click **Next.** The Custom Parameters dialog box opens.

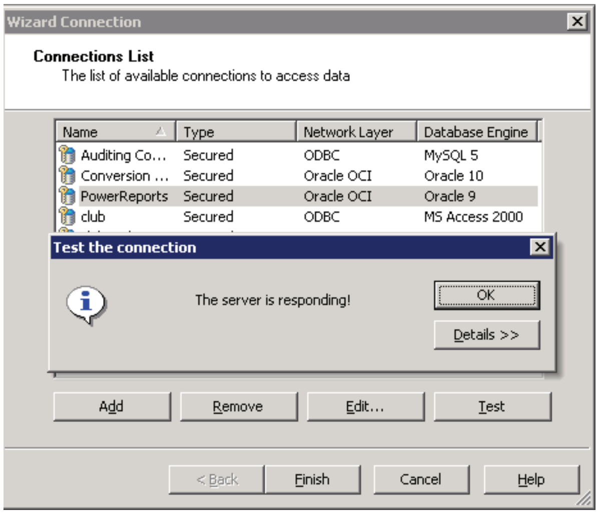


**Custom Parameters [4/4]**

Define the custom parameters to access your Oracle database server using Net Client

| Custom Parameters | |
|---|---|
| Hint | |
| ConnectInit | N i := PKG_SECURITY.F_SET_ENV_VAR('@vari |

7. Click **Finish.** The system returns to the Connections List dialog box.
8. Select **PowerReports** and then click **Test** to verify the connection. If you configured the connection correctly, the system confirms that the server is responding.



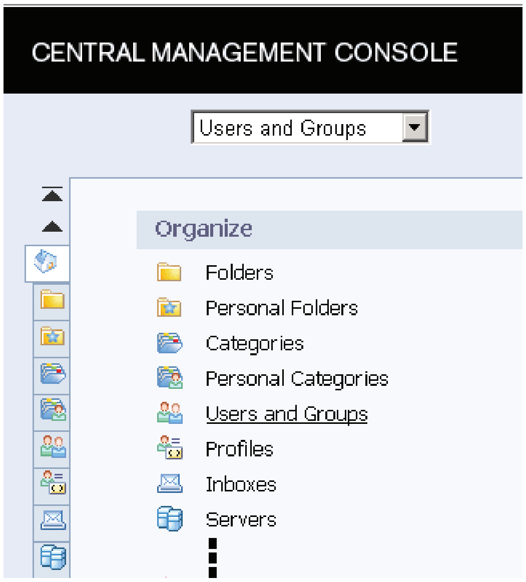
| Name | Type | Network Layer | Database Engine |
|---|---|---|---|
| Auditing Co... | Secured | ODBC | MySQL 5 |
| Conversion ... | Secured | Oracle OCI | Oracle 10 |
| PowerReports | Secured | Oracle OCI | Oracle 9 |
| club | Secured | ODBC | MS Access 2000 |

The server is responding!

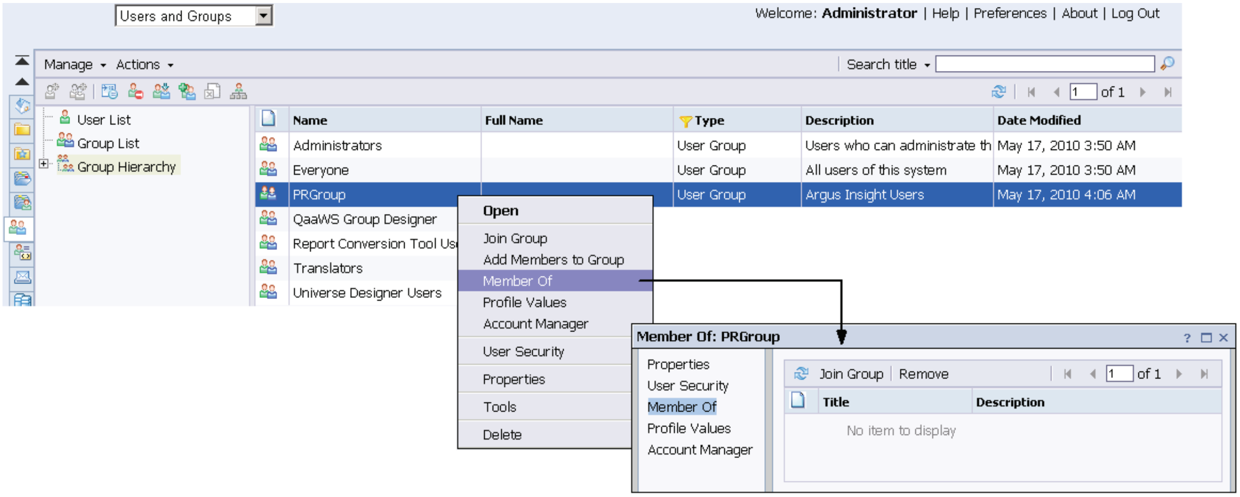
9. Click **OK** to close the message box.
10. Click **Finish** to exit from the BusinessObjects Designer.

### 7.3.5 Configuring PRGroup Settings

1. Log on to the Central Management Console on the BusinessObjects Server.
2. Click the **Users and Groups** link.



3. Navigate to **Group Hierarchy,** and then right-click **PRGroup** and select **Member Of.** The Member Of dialog box opens.

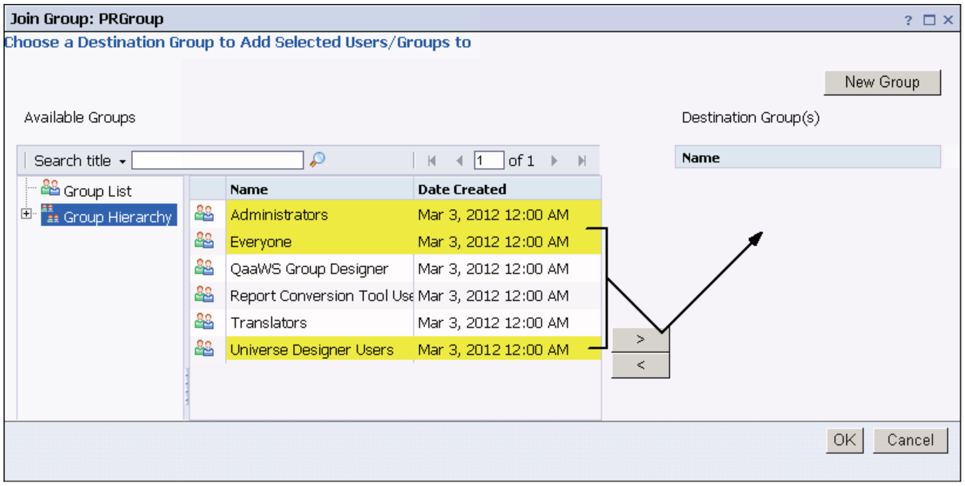


| Name | Full Name | Type | Description | Date Modified |
|---|---|---|---|---|
| Administrators | | User Group | Users who can administrate th | May 17, 2010 3:50 AM |
| Everyone | | User Group | All users of this system | May 17, 2010 3:50 AM |
| PRGroup | | User Group | Argus Insight Users | May 17, 2010 4:06 AM |
| QaaWS Group Designer | | | | |
| Report Conversion Tool Us | | | | |
| Translators | | | | |
| Universe Designer Users | | | | |

| Title | Description |
|---|---|
| No item to display | |

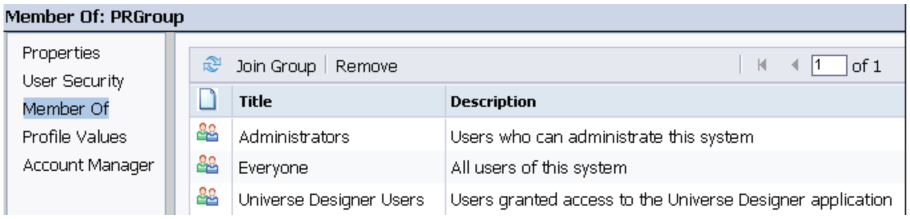
4. Click **Join Group.**

5. Navigate to **Group Hierarchy,** and move **Administrators, Everyone,** and **Universe Designer Users** from Available Groups to Destination Group(s).



| Name | Date Created |
|---|---|
| Administrators | Mar 3, 2012 12:00 AM |
| Everyone | Mar 3, 2012 12:00 AM |
| QaaWS Group Designer | Mar 3, 2012 12:00 AM |
| Report Conversion Tool Use | Mar 3, 2012 12:00 AM |
| Translators | Mar 3, 2012 12:00 AM |
| Universe Designer Users | Mar 3, 2012 12:00 AM |

6. Click **OK.** Note that the system adds PRGroup to your selections.



| Title | Description |
|---|---|
| Administrators | Users who can administrate this system |
| Everyone | All users of this system |
| Universe Designer Users | Users granted access to the Universe Designer application |

7. Click **Close.**

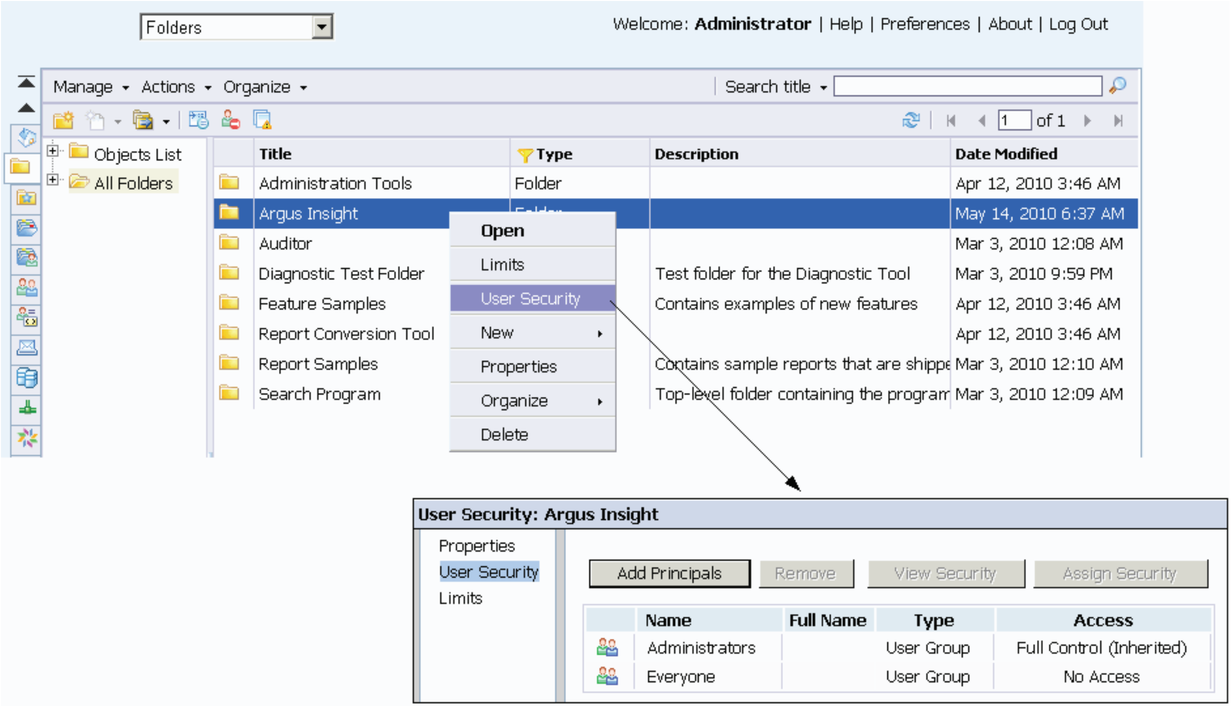
### 7.3.6 Configuring Argus Insight Folder Rights

To configure the rights for the Argus Insight folder:

1. Log on to the Central Management Console on the BusinessObjects Server.

2. Click **Folders.**

3. Right-click **Argus Insight** and select **User Security.**



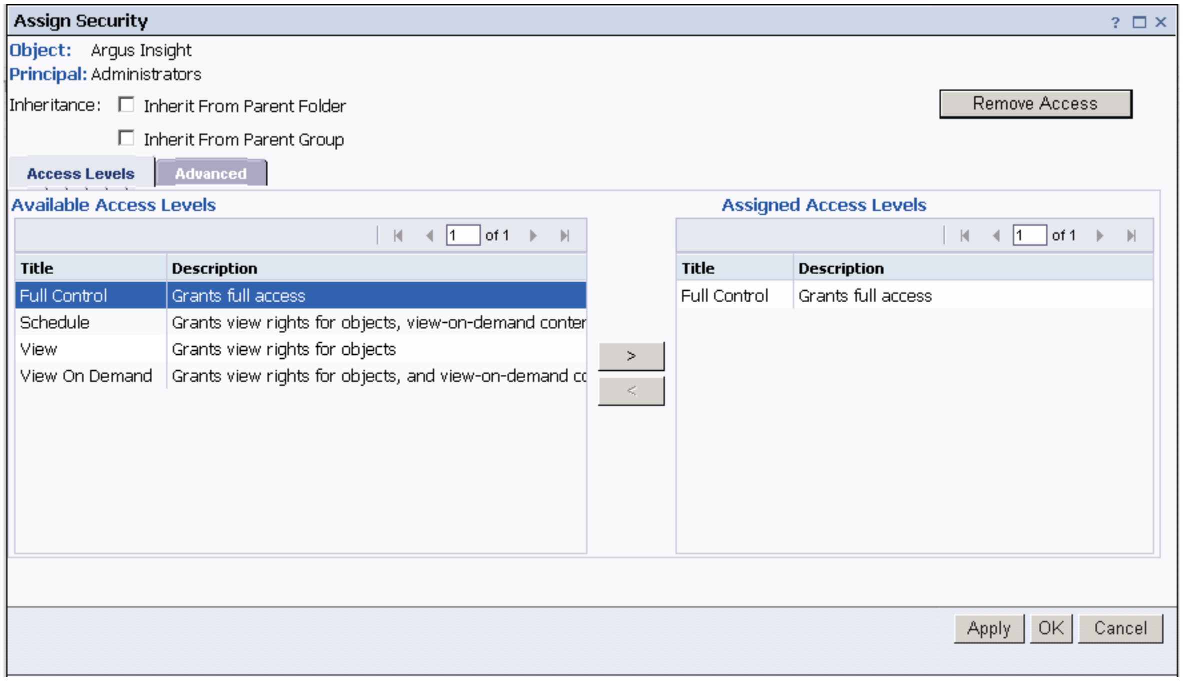
| Title | Type | Description | Date Modified |
|---|---|---|---|
| Administration Tools | Folder | | Apr 12, 2010 3:46 AM |
| Argus Insight | Folder | | May 14, 2010 6:37 AM |
| Auditor | | | Mar 3, 2010 12:08 AM |
| Diagnostic Test Folder | | Test folder for the Diagnostic Tool | Mar 3, 2010 9:59 PM |
| Feature Samples | | Contains examples of new features | Apr 12, 2010 3:46 AM |
| Report Conversion Tool | | | Apr 12, 2010 3:46 AM |
| Report Samples | | Contains sample reports that are shippe | Mar 3, 2010 12:10 AM |
| Search Program | | Top-level folder containing the program | Mar 3, 2010 12:09 AM |

| Name | Full Name | Type | Access |
|---|---|---|---|
| Administrators | | User Group | Full Control (Inherited) |
| Everyone | | User Group | No Access |

4. Select **Administrators** and click **Assign Security**. The Assign Security dialog box opens.

5. Uncheck the **Inherit From Parent Folder** and **Inherit From Parent Group** check boxes.

6. Select **Full Control** from the Available Access Levels section and click the right arrow (>) to assign the Full Control access level.



**Object:** Argus Insight
**Principal:** Administrators
Inheritance: ☐ Inherit From Parent Folder
☐ Inherit From Parent Group

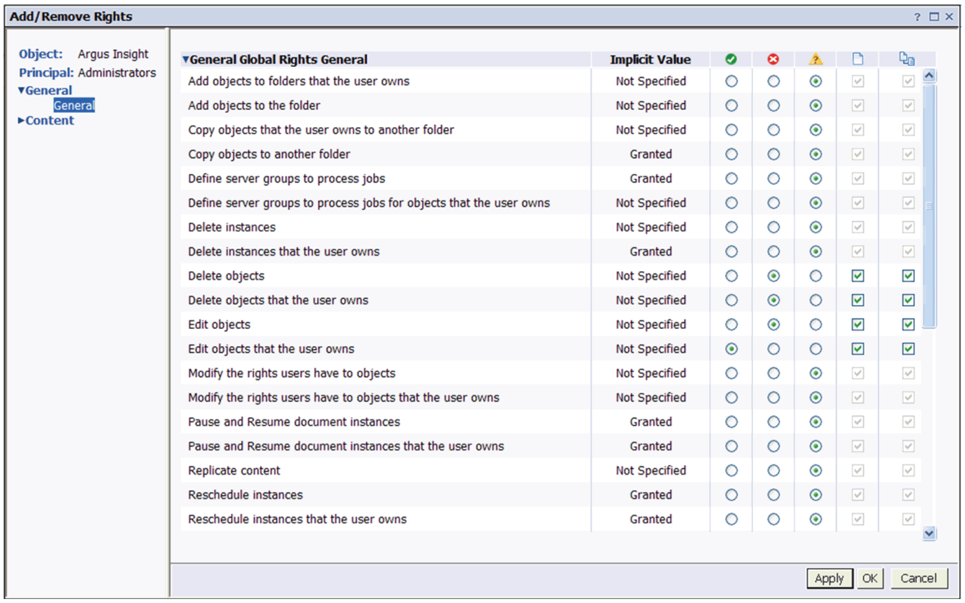
Available Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |
| Schedule | Grants view rights for objects, view-on-demand conter |
| View | Grants view rights for objects |
| View On Demand | Grants view rights for objects, and view-on-demand co |

Assigned Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |

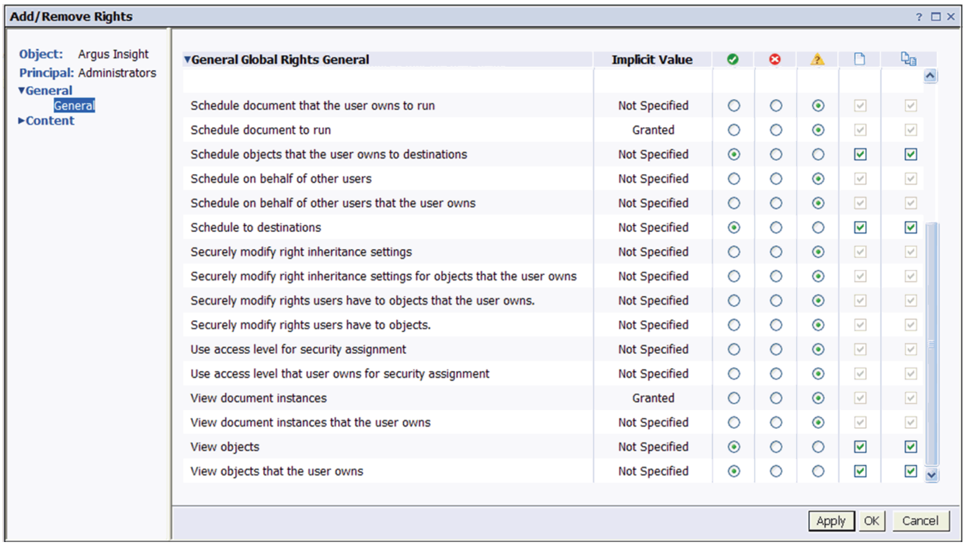
7. Click the **Advanced** tab, and then click **Add/Remove Rights.** Change the access rights to match the settings shown in the following two illustrations:



**Add/Remove Rights**

**Object:** Argus Insight
**Principal:** Administrators
▾General
General
▸Content

| ▾General Global Rights General | Implicit Value | ✓ | ✗ | ⚠ | 🗋 | ⧉ |
|---|---|---|---|---|---|---|
| Add objects to folders that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Add objects to the folder | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Copy objects that the user owns to another folder | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Copy objects to another folder | Granted | ○ | ○ | ● | ☑ | ☑ |
| Define server groups to process jobs | Granted | ○ | ○ | ● | ☑ | ☑ |
| Define server groups to process jobs for objects that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Delete instances | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Delete instances that the user owns | Granted | ○ | ○ | ● | ☑ | ☑ |
| Delete objects | Not Specified | ○ | ● | ○ | ☑ | ☑ |
| Delete objects that the user owns | Not Specified | ○ | ● | ○ | ☑ | ☑ |
| Edit objects | Not Specified | ○ | ● | ○ | ☑ | ☑ |
| Edit objects that the user owns | Not Specified | ● | ○ | ○ | ☑ | ☑ |
| Modify the rights users have to objects | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Modify the rights users have to objects that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Pause and Resume document instances | Granted | ○ | ○ | ● | ☑ | ☑ |
| Pause and Resume document instances that the user owns | Granted | ○ | ○ | ● | ☑ | ☑ |
| Replicate content | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Reschedule instances | Granted | ○ | ○ | ● | ☑ | ☑ |
| Reschedule instances that the user owns | Granted | ○ | ○ | ● | ☑ | ☑ |

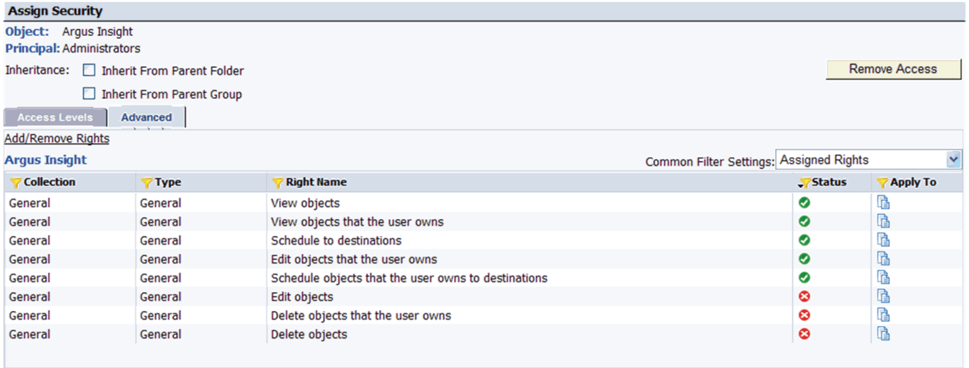


**Add/Remove Rights**

**Object:** Argus Insight
**Principal:** Administrators
▾General
General
▸Content

| ▾General Global Rights General | Implicit Value | ✓ | ✗ | ⚠ | 🗋 | ⧉ |
|---|---|---|---|---|---|---|
| Schedule document that the user owns to run | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Schedule document to run | Granted | ○ | ○ | ● | ☑ | ☑ |
| Schedule objects that the user owns to destinations | Not Specified | ● | ○ | ○ | ☑ | ☑ |
| Schedule on behalf of other users | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Schedule on behalf of other users that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Schedule to destinations | Not Specified | ● | ○ | ○ | ☑ | ☑ |
| Securely modify right inheritance settings | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Securely modify right inheritance settings for objects that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Securely modify rights users have to objects that the user owns. | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Securely modify rights users have to objects. | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Use access level for security assignment | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| Use access level that user owns for security assignment | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| View document instances | Granted | ○ | ○ | ● | ☑ | ☑ |
| View document instances that the user owns | Not Specified | ○ | ○ | ● | ☑ | ☑ |
| View objects | Not Specified | ● | ○ | ○ | ☑ | ☑ |
| View objects that the user owns | Not Specified | ● | ○ | ○ | ☑ | ☑ |

8. Click **OK.** The Assign Security page opens.



**Assign Security**

**Object:** Argus Insight
**Principal:** Administrators

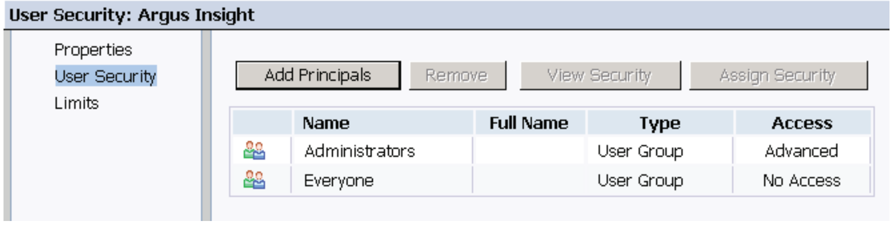
Inheritance: ☐ Inherit From Parent Folder
☐ Inherit From Parent Group

**Argus Insight**

Common Filter Settings: Assigned Rights

| Collection | Type | Right Name | Status | Apply To |
|---|---|---|---|---|
| General | General | View objects | ✓ | ⧉ |
| General | General | View objects that the user owns | ✓ | ⧉ |
| General | General | Schedule to destinations | ✓ | ⧉ |
| General | General | Edit objects that the user owns | ✓ | ⧉ |
| General | General | Schedule objects that the user owns to destinations | ✓ | ⧉ |
| General | General | Edit objects | ✗ | ⧉ |
| General | General | Delete objects that the user owns | ✗ | ⧉ |
| General | General | Delete objects | ✗ | ⧉ |

9. Click **OK.** The User Security: Argus Insight Page opens.

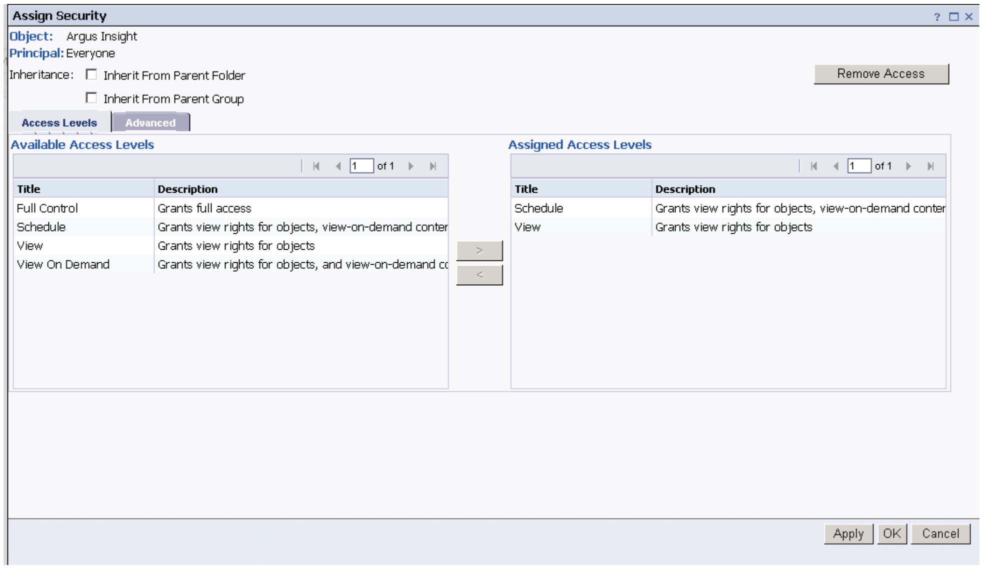


| | Name | Full Name | Type | Access |
|---|---|---|---|---|
| | Administrators | | User Group | Advanced |
| | Everyone | | User Group | No Access |

10. Select **Everyone** and click **Assign Security.** The Assign Security dialog box opens.

11. Uncheck the **Inherit From Parent Folder** and **Inherit From Parent Group** check boxes.

12. Select **Schedule** and **View** from the Available Access Levels section and click the right arrow (>) to assign those access levels.



Object: Argus Insight

Principal: Everyone

Inheritance: ☐ Inherit From Parent Folder

☐ Inherit From Parent Group

Available Access Levels

1 of 1

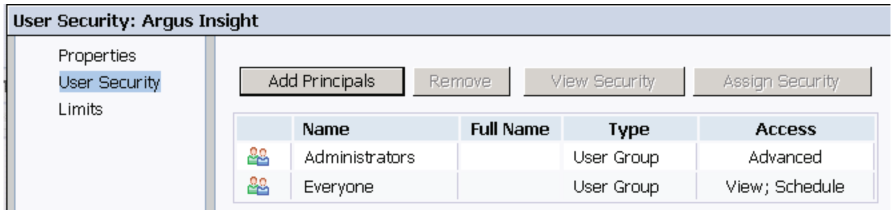
| Title | Description |
|---|---|
| Full Control | Grants full access |
| Schedule | Grants view rights for objects, view-on-demand conte |
| View | Grants view rights for objects |
| View On Demand | Grants view rights for objects, and view-on-demand c |

Assigned Access Levels

1 of 1

| Title | Description |
|---|---|
| Schedule | Grants view rights for objects, view-on-demand conte |
| View | Grants view rights for objects |

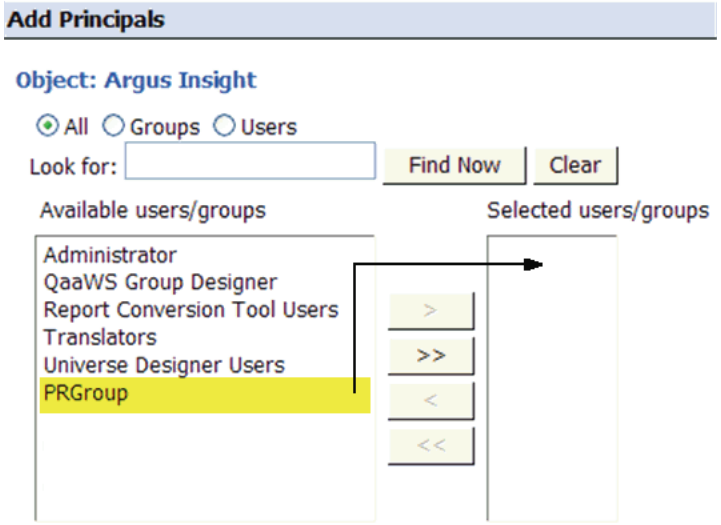
13. Click **OK.** The system returns to the User Security: Argus Insight page. Note that the access level for the Everyone user group is set to View and Schedule.



| | Name | Full Name | Type | Access |
|---|---|---|---|---|
| | Administrators | | User Group | Advanced |
| | Everyone | | User Group | View; Schedule |

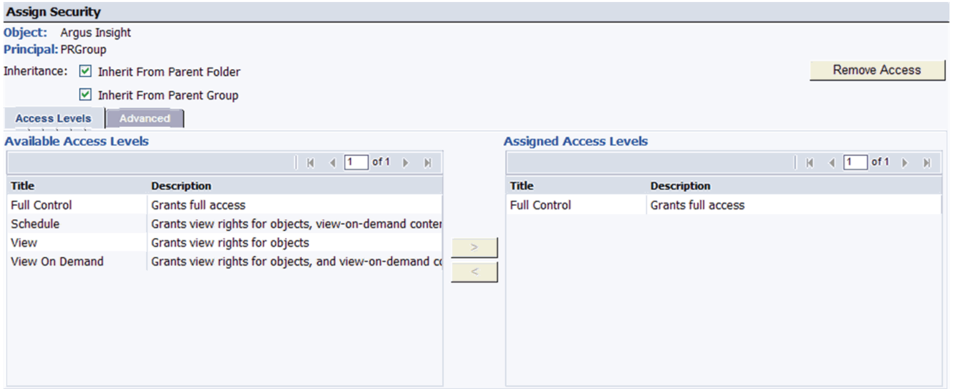
14. Click **Add Principals.**

15. Select **PRGroup** and click the right arrow (>) to move PRGroup to the Selected users/groups column.



16. Click **Add and Assign Security.**

17. Select **Full Control** from the Available Access Levels section and click the right arrow (>) to assign the access level.



Object: Argus Insight
Principal: PRGroup
Inheritance: ☑ Inherit From Parent Folder
☑ Inherit From Parent Group

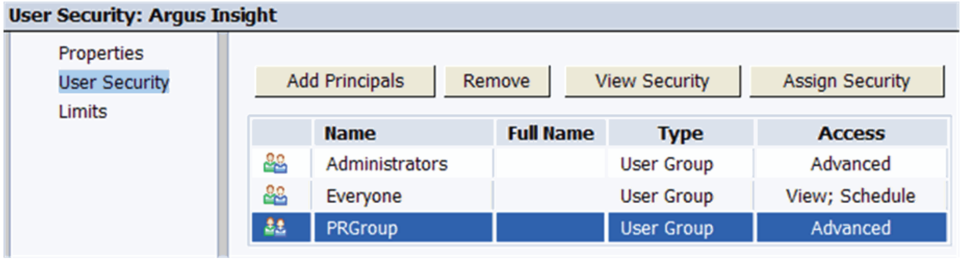
Available Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |
| Schedule | Grants view rights for objects, view-on-demand conter |
| View | Grants view rights for objects |
| View On Demand | Grants view rights for objects, and view-on-demand cc |

Assigned Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |

18. Click **OK.** The system returns to the User Security: Argus Insight page. Note that the access level for the PRGroup user group is set to Advanced.



| Name | Full Name | Type | Access |
|---|---|---|---|
| Administrators | | User Group | Advanced |
| Everyone | | User Group | View; Schedule |
| PRGroup | | User Group | Advanced |

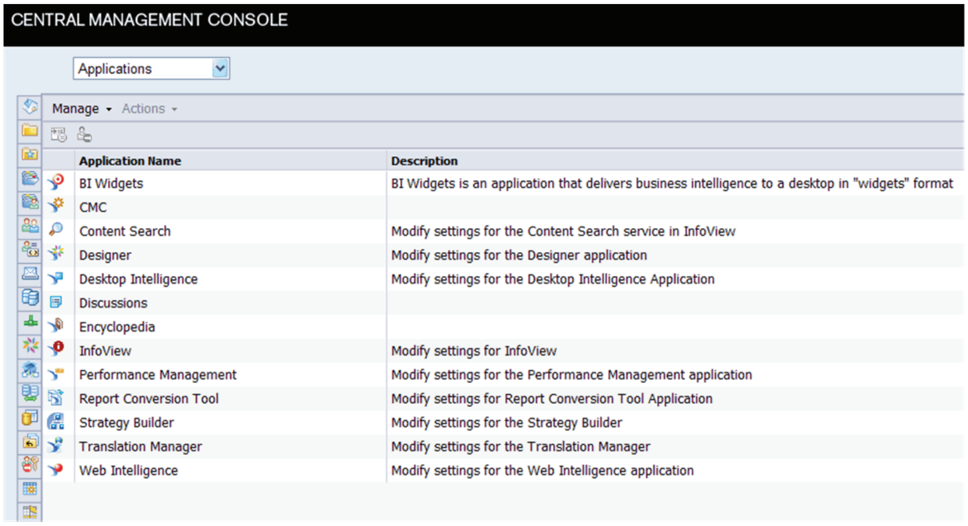
19. Click **Close.**

## 7.3.7 Configuring BusinessObjects Applications Rights

To configure rights for the BusinessObjects Applications:

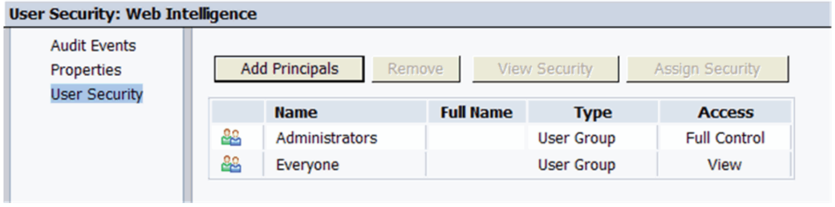
1. Log on to Central Management Console on the BusinessObjects Server.

2. Click **Applications.** The Applications page opens.



| Application Name | Description |
|---|---|
| BI Widgets | BI Widgets is an application that delivers business intelligence to a desktop in "widgets" format |
| CMC | |
| Content Search | Modify settings for the Content Search service in InfoView |
| Designer | Modify settings for the Designer application |
| Desktop Intelligence | Modify settings for the Desktop Intelligence Application |
| Discussions | |
| Encyclopedia | |
| InfoView | Modify settings for InfoView |
| Performance Management | Modify settings for the Performance Management application |
| Report Conversion Tool | Modify settings for Report Conversion Tool Application |
| Strategy Builder | Modify settings for the Strategy Builder |
| Translation Manager | Modify settings for the Translation Manager |
| Web Intelligence | Modify settings for the Web Intelligence application |

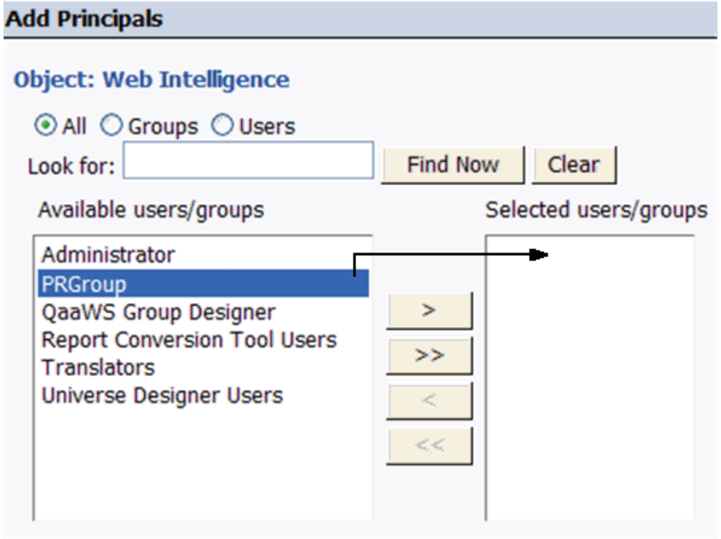
3. Right-click **Web Intelligence** and select **User Security.** The User Security: Web Intelligence page opens.



| Name | Full Name | Type | Access |
|---|---|---|---|
| Administrators | | User Group | Full Control |
| Everyone | | User Group | View |

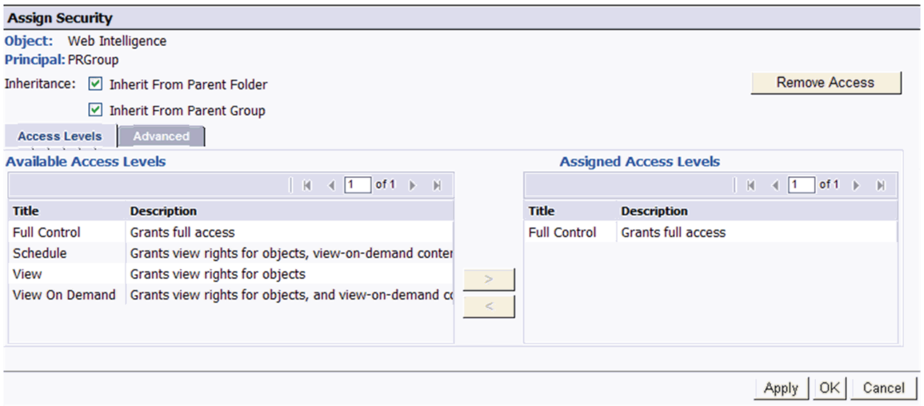
4. Click **Add Principals.**

5. Select **PRGroup** and click the right arrow (>) to move PRGroup to the Selected users/groups column.



6. Click **Add and Assign Security.**

7. Select **Full Control** from the Available Access Levels section and click the right arrow (>) to assign the access level.



**Object:** Web Intelligence
**Principal:** PRGroup
Inheritance: ☑ Inherit From Parent Folder
☑ Inherit From Parent Group

Available Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |
| Schedule | Grants view rights for objects, view-on-demand conter |
| View | Grants view rights for objects |
| View On Demand | Grants view rights for objects, and view-on-demand cc |

Assigned Access Levels

| Title | Description |
|---|---|
| Full Control | Grants full access |

8. Click **OK.**
9. Repeat this procedure to configure rights for the Designer and Desktop Intelligence applications for BusinessObjects.

## 7.4 Configuring the Argus Insight Web Server

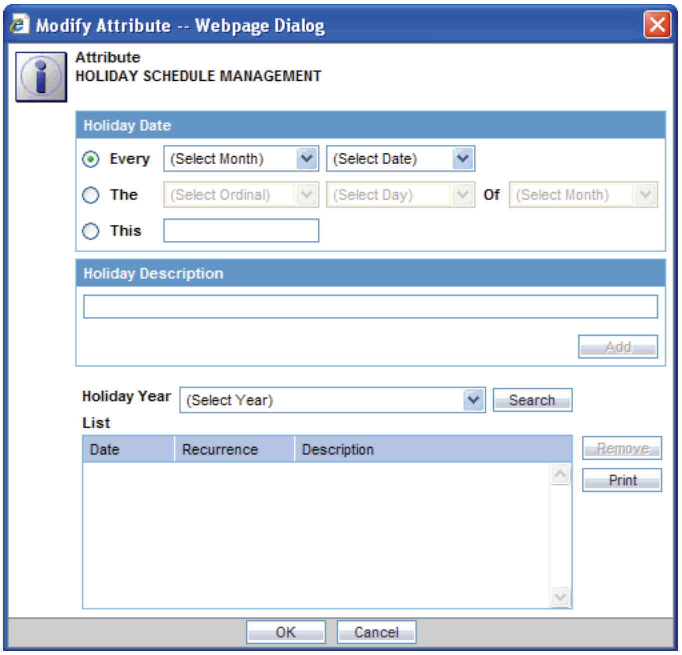
This section describes the steps to complete the following tasks:

- Configuring Holiday Schedule Management
- Configuring Product Designated Medical Events
- Configuring Measurable Suppliers
- Configuring Sites
- Configuring Acceptable Delay Justification

### 7.4.1 Configuring Holiday Schedule Management

To configure the holiday schedule:

1. Log in to the Argus Insight application.
2. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
3. Click the **List Maintenance** tab.
4. Select **Holiday Schedule Management** from the List Maintenance Items group.
5. Select **Company** or **US Federal** from the Attributes group, and click **Modify.** The Holiday Schedule Management dialog box opens.

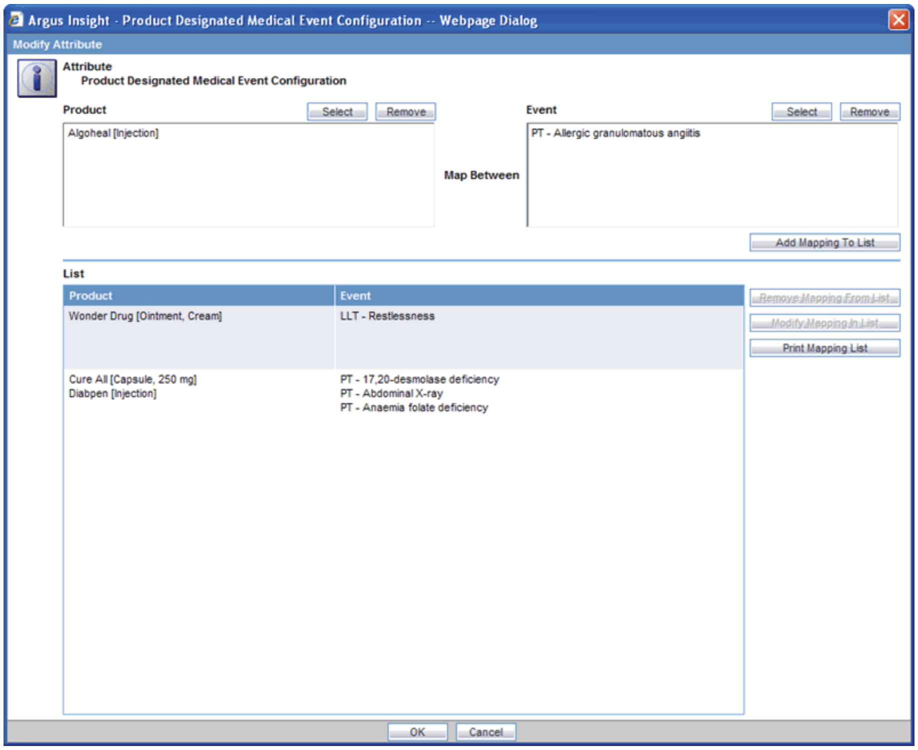

Modify Attribute -- Webpage Dialog
Attribute
HOLIDAY SCHEDULE MANAGEMENT
Holiday Date
● Every (Select Month) (Select Date)
○ The (Select Ordinal) (Select Day) Of (Select Month)
○ This
Holiday Description
Add
Holiday Year (Select Year)
Search
List
Date
Recurrence
Description
Remove
Print
OK
Cancel

6. Define the holidays.
7. Click **OK.** The system saves your changes and returns to the **List Maintenance** tab.

## 7.4.2 Configuring Product Designated Medical Events

To configure product designated medical events:

1. Select **Product Designated Medical Event Configuration** from the List Maintenance Items group.
2. Select **All Configurations** from the Attributes group, and click **Modify.** The Product Designated Medical Event Configuration dialog box opens.



Attribute
Product Designated Medical Event Configuration

Product: Algoheal [Injection]

Event: PT - Allergic granulomatous angiitis

List

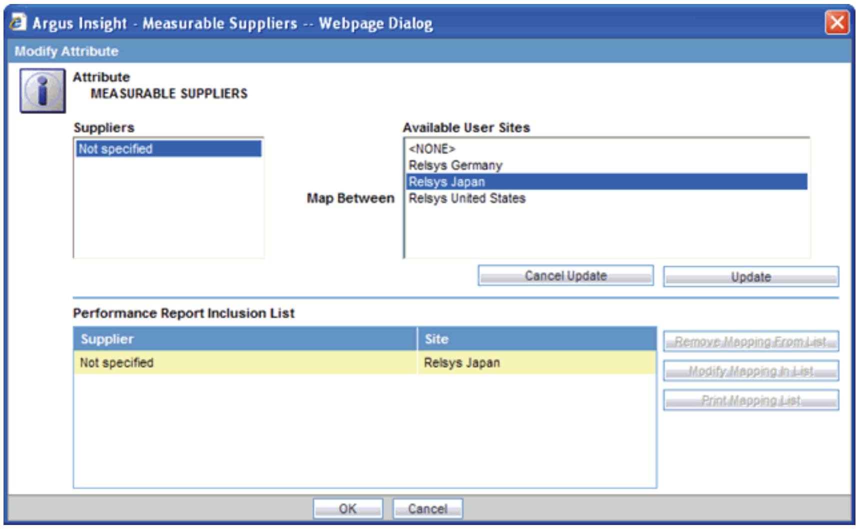
| Product | Event |
|---|---|
| Wonder Drug [Ointment, Cream] | LLT - Restlessness |
| Cure All [Capsule, 250 mg]<br>Diabpen [Injection] | PT - 17,20-desmolase deficiency<br>PT - Abdominal X-ray<br>PT - Anaemia folate deficiency |

3. Make the required selections.
4. Click **OK.** The system saves your changes and returns to the **List Maintenance** tab.

## 7.4.3 Configuring Measurable Suppliers

To configure measurable suppliers:

1. Select **Measurable Suppliers** from the List Maintenance Items group.
2. Select **All Configurations** from the Attributes group, and click **Modify.** The Measurable Suppliers dialog box opens.



Attribute
MEASURABLE SUPPLIERS

Suppliers: Not specified

Available User Sites:
<NONE>
Relsys Germany
Relsys Japan
Relsys United States

Performance Report Inclusion List

| Supplier | Site |
|---|---|
| Not specified | Relsys Japan |

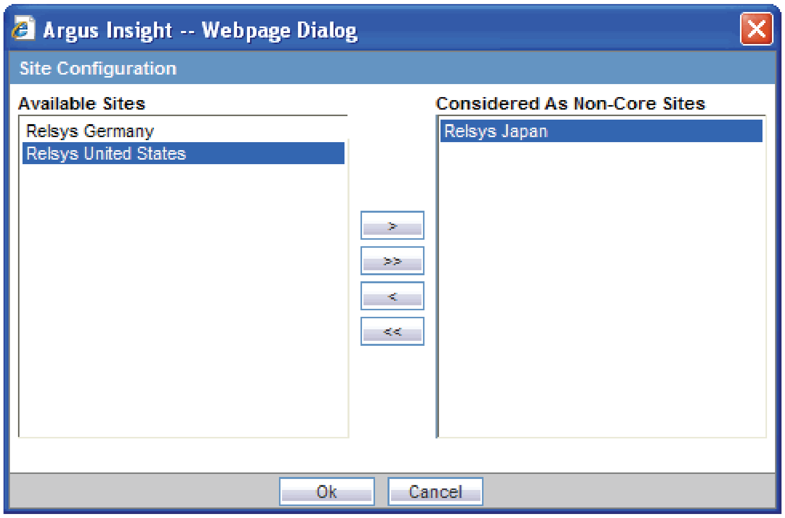
3. Make the required selections.

4. Click **OK.** The system saves your changes and returns to the **List Maintenance** tab.

### 7.4.4 Configuring Sites

To configure sites:

1. Select **Site Configuration** from the List Maintenance Items group.
2. Select **Non-Core Site Configuration** from the Attributes group, and click **Modify.** The Site Configuration dialog box opens.



3. Define your core and non-core sites by using the right and left arrows to move the entries between the Available Sites column (core) and the Considered As Non-Core Sites column.

   The system uses this configuration in the DCA-TME Notification Report in Case Processing.
4. Click **OK.** The system saves your changes and returns to the **List Maintenance** tab.

### 7.4.5 Configuring Acceptable Delay Justification

To configure an acceptable delay justification:

1. Select **Acceptable Delay Justification** from the List Maintenance Items group.
2. Select the delay justification that you want to modify. You can select:
   - **Acceptable Routing Delay Justification**
   - **Acceptable Submission Delay Justification**
3. Click **Modify.**
4. Enter the appropriate justification.

   The system uses this configuration in the Regulatory Submission and Distribution Compliance report.
5. Click **OK.** The system saves your changes and returns to the **List Maintenance** tab.

## 7.5 Configuring LDAP Authentication Settings

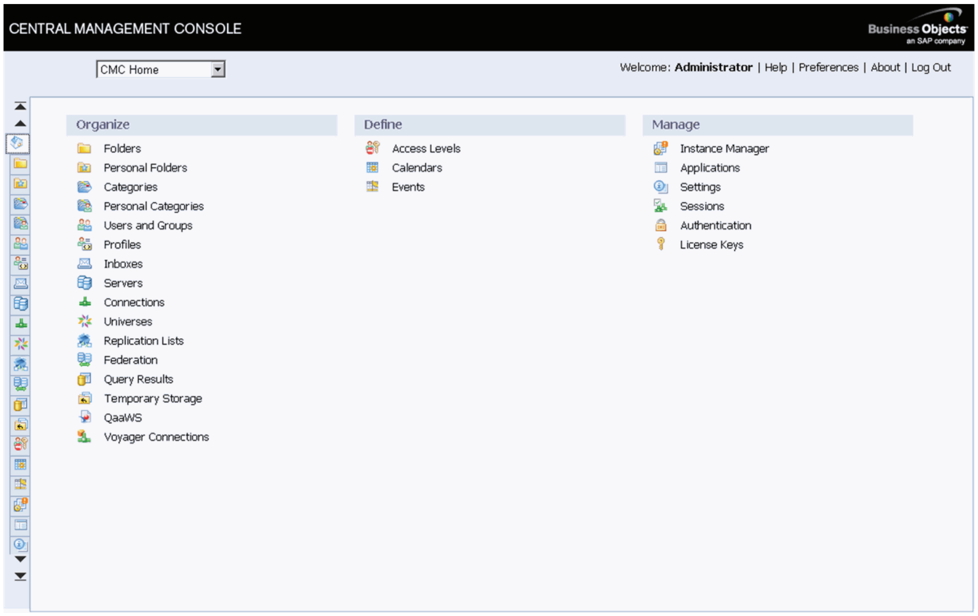
This topic describes how to integrate the LDAP authentication with Argus Insight and BusinessObjects. Follow the installation procedures in the order documented.

> **Note:** Create a group in the LDAP Server and assign LDAP users to this group. This group should not exist in BusinessObjects.

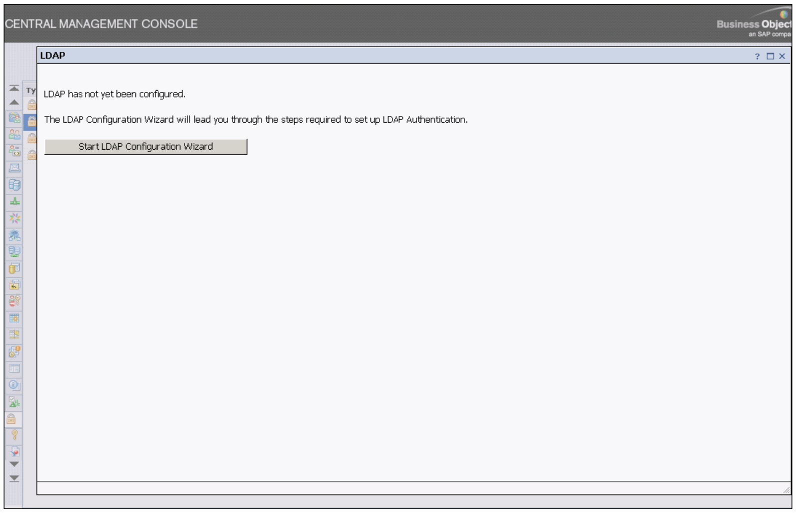
### 7.5.1 Setting Up LDAP Authentication in BusinessObjects

To configure the LDAP Server settings in BusinessObjects:

1. Log on to BusinessObjects Central Management Console using the administrator name and password.



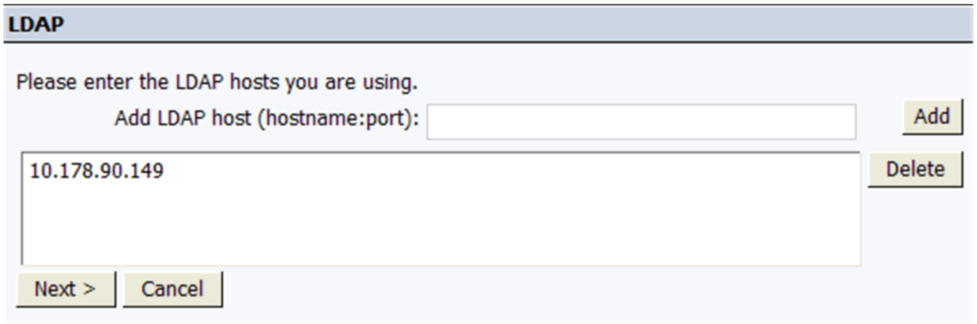
2. Click **Authentication** to access the authentication options in BusinessObjects.
3. Double-click **LDAP.**



LDAP has not yet been configured.

The LDAP Configuration Wizard will lead you through the steps required to set up LDAP Authentication.

4. Click **Start LDAP Configuration Wizard.** The system displays the following screen:



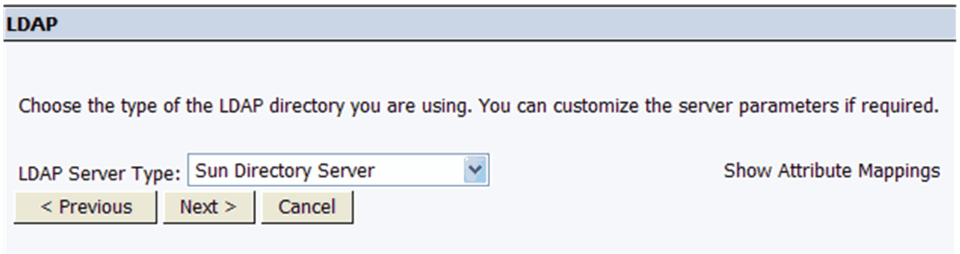
**LDAP**

Please enter the LDAP hosts you are using.

Add LDAP host (hostname:port):

10.178.90.149

5. Add the IP address and port number for the LDAP server. Click **Next.** The system displays the following screen:

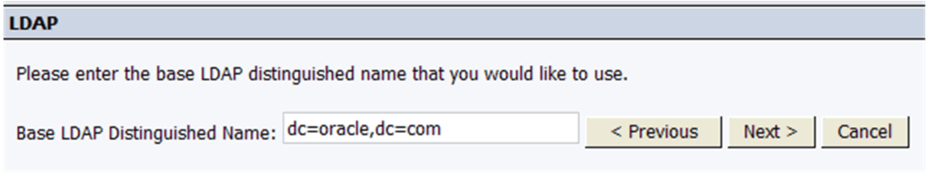


**LDAP**

Choose the type of the LDAP directory you are using. You can customize the server parameters if required.

LDAP Server Type: Sun Directory Server

6. Click **Next.** The system displays the following screen:

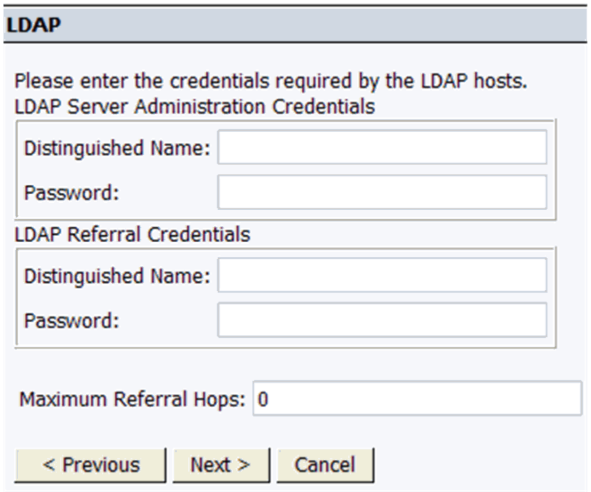


**LDAP**

Please enter the base LDAP distinguished name that you would like to use.

Base LDAP Distinguished Name: dc=oracle,dc=com

7. Enter a name for the base LDAP and click **Next.** The system displays the following screen:



**LDAP**

Please enter the credentials required by the LDAP hosts.

LDAP Server Administration Credentials

Distinguished Name:

Password:

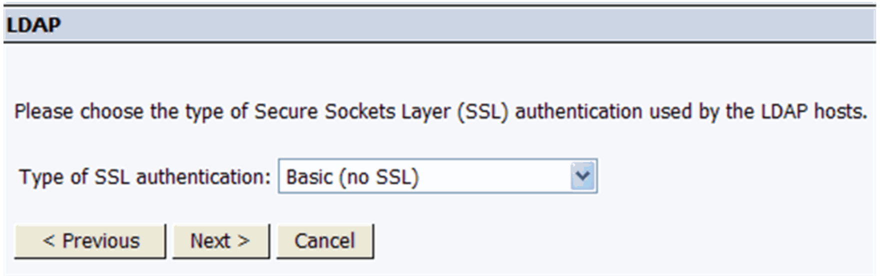
LDAP Referral Credentials

Distinguished Name:

Password:

Maximum Referral Hops: 0

8. Click **Next.** The system displays the following screen:

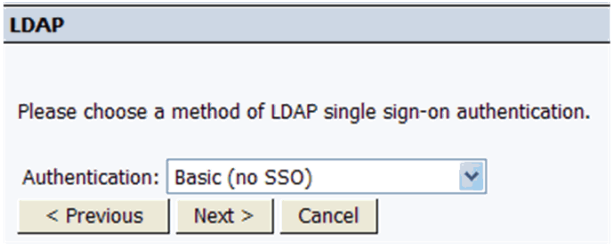


LDAP

Please choose the type of Secure Sockets Layer (SSL) authentication used by the LDAP hosts.

Type of SSL authentication: Basic (no SSL)

9. Click **Next.** The system displays the following screen:

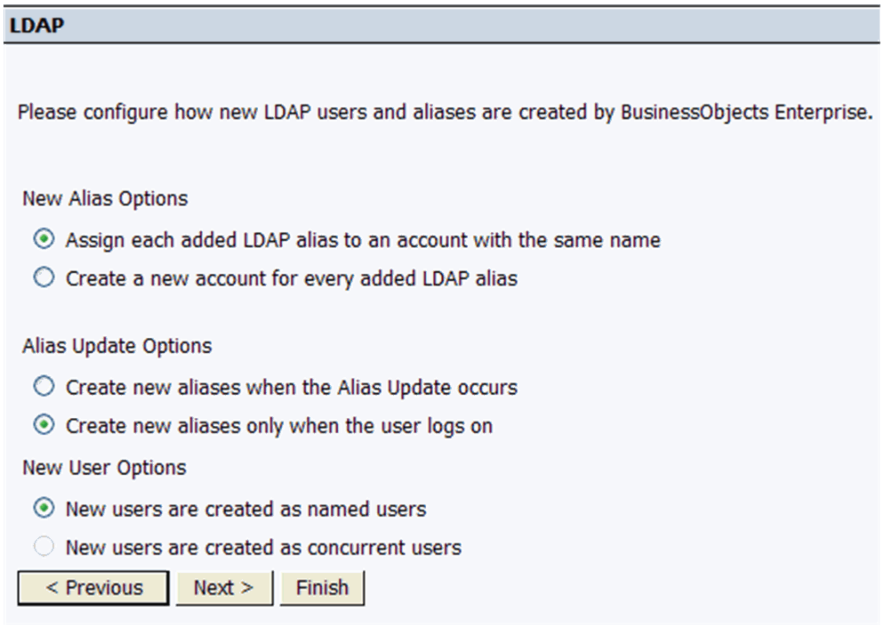


LDAP

Please choose a method of LDAP single sign-on authentication.

Authentication: Basic (no SSO)

10. Click **Next.** The system displays the following screen:



LDAP

Please configure how new LDAP users and aliases are created by BusinessObjects Enterprise.

New Alias Options

● Assign each added LDAP alias to an account with the same name
○ Create a new account for every added LDAP alias

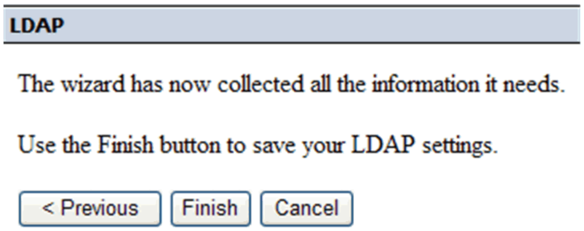
Alias Update Options

○ Create new aliases when the Alias Update occurs
● Create new aliases only when the user logs on

New User Options

● New users are created as named users
○ New users are created as concurrent users

11. Select one of the New User Options, whichever one is required:
    - **New users are created as named users**
    - **New users are created as concurrent users**
12. Click **Next.** The wizard reports when it has collected all the required information.

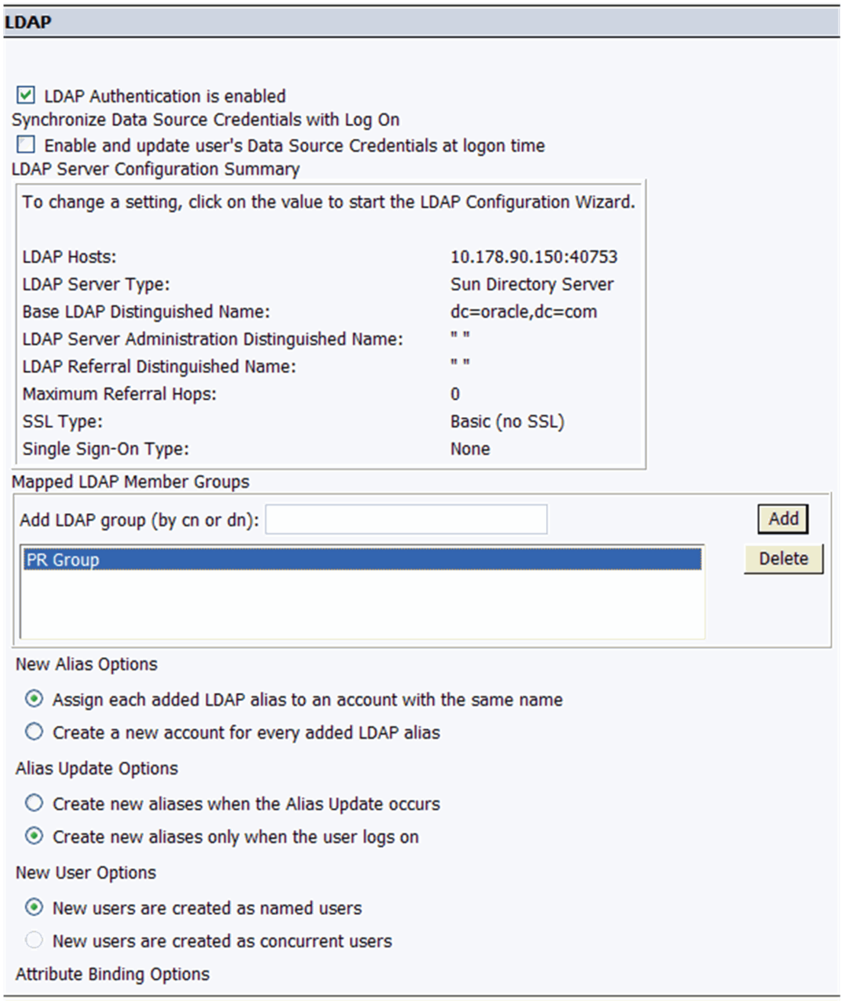


**LDAP**

The wizard has now collected all the information it needs.

Use the Finish button to save your LDAP settings.

13. Click **Finish.**
14. Wait until the system displays the LDAP screen.
15. Locate the **Add LDAP group (by cn or dn)** field in the LDAP screen. Type the Group Name configured in LDAP Server, and click **Add.**



**LDAP**

☑ LDAP Authentication is enabled

Synchronize Data Source Credentials with Log On

☐ Enable and update user's Data Source Credentials at logon time

LDAP Server Configuration Summary

To change a setting, click on the value to start the LDAP Configuration Wizard.

| | |
|---|---|
| LDAP Hosts: | 10.178.90.150:40753 |
| LDAP Server Type: | Sun Directory Server |
| Base LDAP Distinguished Name: | dc=oracle,dc=com |
| LDAP Server Administration Distinguished Name: | " " |
| LDAP Referral Distinguished Name: | " " |
| Maximum Referral Hops: | 0 |
| SSL Type: | Basic (no SSL) |
| Single Sign-On Type: | None |

Mapped LDAP Member Groups

Add LDAP group (by cn or dn):

PR Group

New Alias Options

● Assign each added LDAP alias to an account with the same name

○ Create a new account for every added LDAP alias

Alias Update Options

○ Create new aliases when the Alias Update occurs

● Create new aliases only when the user logs on

New User Options

● New users are created as named users

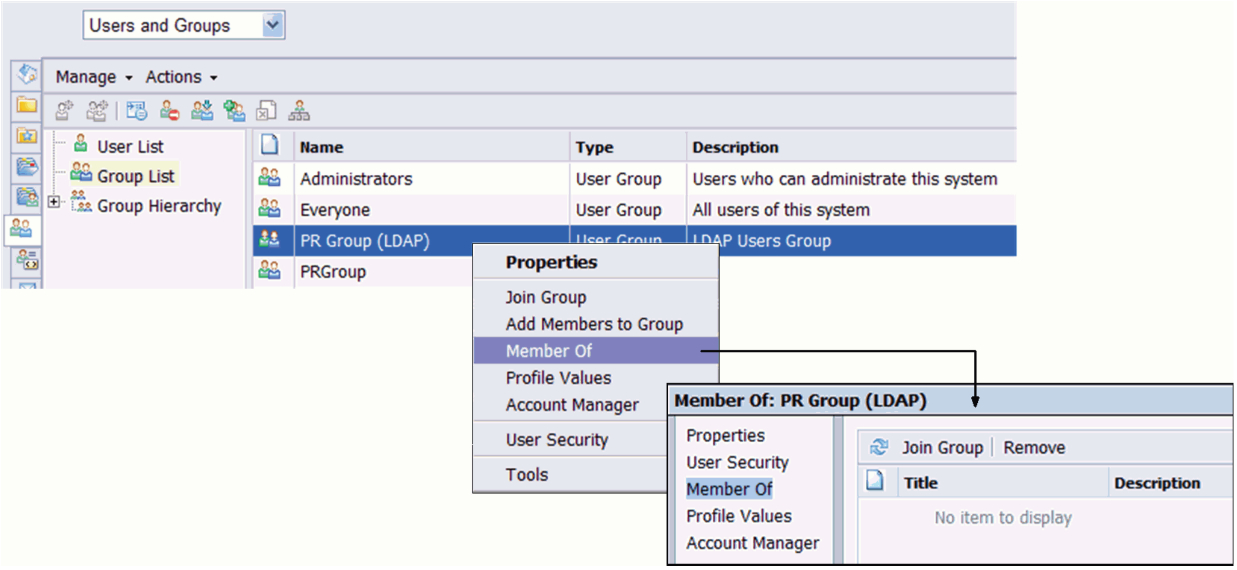
○ New users are created as concurrent users

Attribute Binding Options

16. Scroll downwards and click **Update.**
17. Map the LDAP member group whose users you want to authenticate through LDAP.

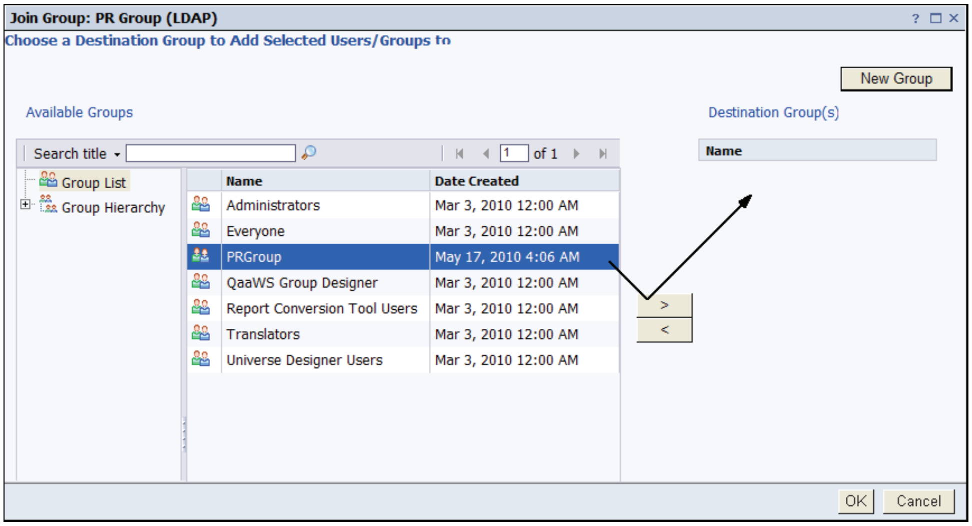
    For example, PR Group is the member group whose users are part of Argus Insight and use LDAP authentication for access to BusinessObjects.
18. Select **Create a new account for every added LDAP alias** under the New Alias Options on the LDAP window.

19. Close the window.
20. Navigate to **Home, Group List,** and then right-click **PR Group (LDAP)** and select **Member Of.** The Member Of dialog box opens.



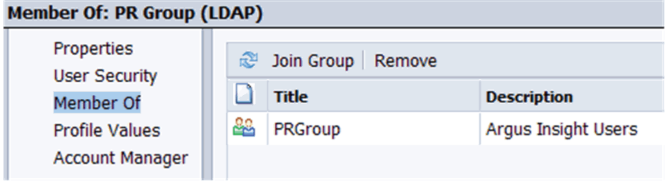
| Name | Type | Description |
|---|---|---|
| Administrators | User Group | Users who can administrate this system |
| Everyone | User Group | All users of this system |
| PR Group (LDAP) | User Group | LDAP Users Group |
| PRGroup | | |

21. Click **Join Group.**
22. Navigate to **Group List,** select **PRGroup,** and then click the right arrow (**>**) to add the PRGroup into the Destination Group.



| Name | Date Created |
|---|---|
| Administrators | Mar 3, 2010 12:00 AM |
| Everyone | Mar 3, 2010 12:00 AM |
| PRGroup | May 17, 2010 4:06 AM |
| QaaWS Group Designer | Mar 3, 2010 12:00 AM |
| Report Conversion Tool Users | Mar 3, 2010 12:00 AM |
| Translators | Mar 3, 2010 12:00 AM |
| Universe Designer Users | Mar 3, 2010 12:00 AM |

23. Click **OK.** Note that PR Group (LDAP) is now a member of the PRGroup.



| Title | Description |
|---|---|
| PRGroup | Argus Insight Users |

# 8

# 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 comprises the following sub-sections:

- Uploading the Argus Insight.xdrz file to BIP
- Creating PRMART JDBC Connection
- Managing Users and Roles: BI Publisher Security Model
- Managing Users and Roles: Oracle Fusion Middleware Security Model
- Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model
- Configuring BIP Roles and Permissions: BI Publisher Security Model

## 8.1 Uploading the Argus Insight.xdrz file to BIP

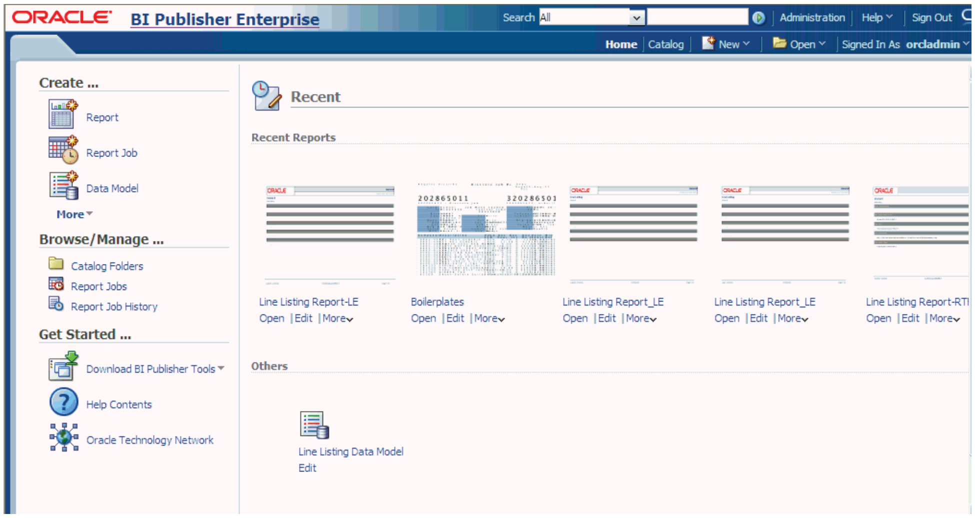
> **Note:** You must be logged in to BIP with the BI Admin User credentials to be able to upload the **Argus Insight.xdrz** file. You can refer to Table 8–3 for more information on the BI Admin User.

To upload the **Argus Insight.xdrz** file to BIP, execute the following steps:

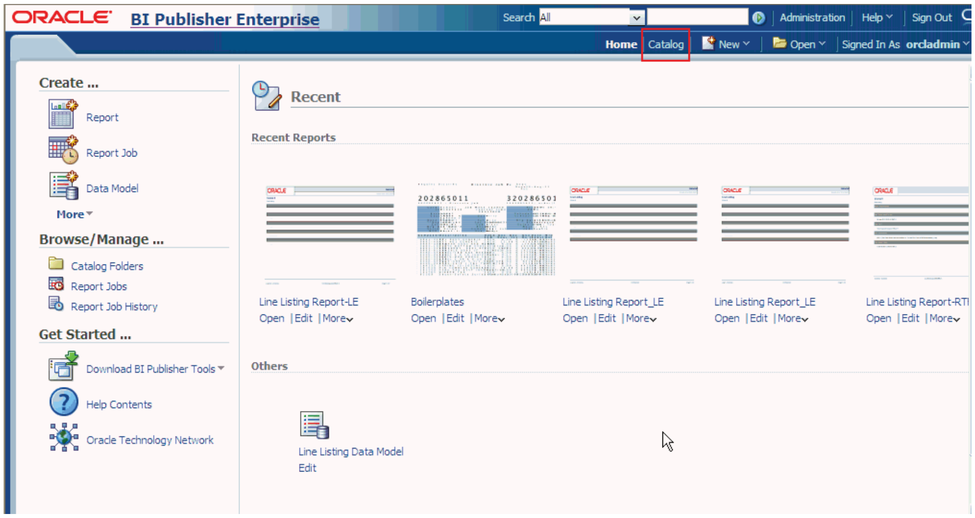
1. Copy the **Argus Insight.xdrz** file from the following location on the Argus Insight Web Server to the local file system:

   Drive:\<Argus Insight Installation Folder>\ArgusInsight\BIP\Repository

2. Log on to BIP using the BI Admin User credentials. This displays the BIP Home Page as depicted in the following figure:

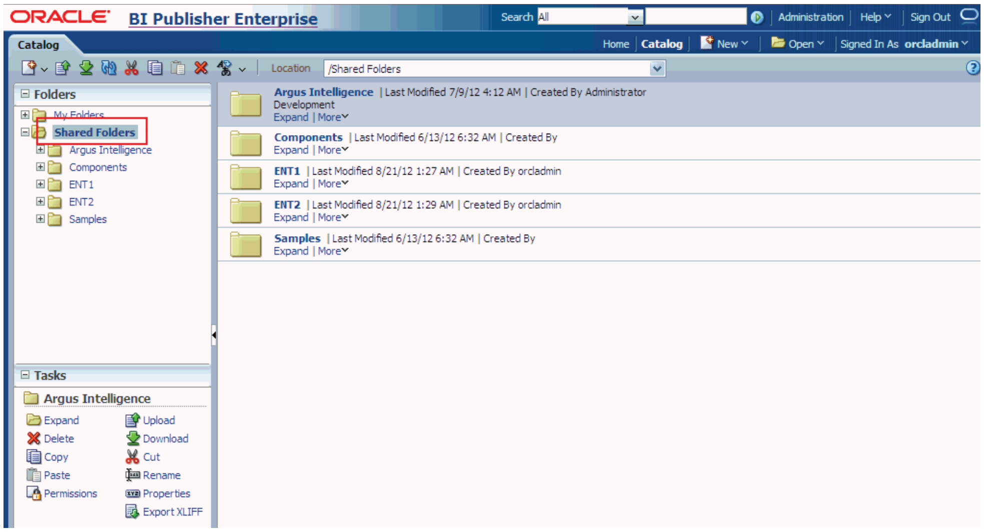


3. Click **Catalog** as highlighted in the following figure:

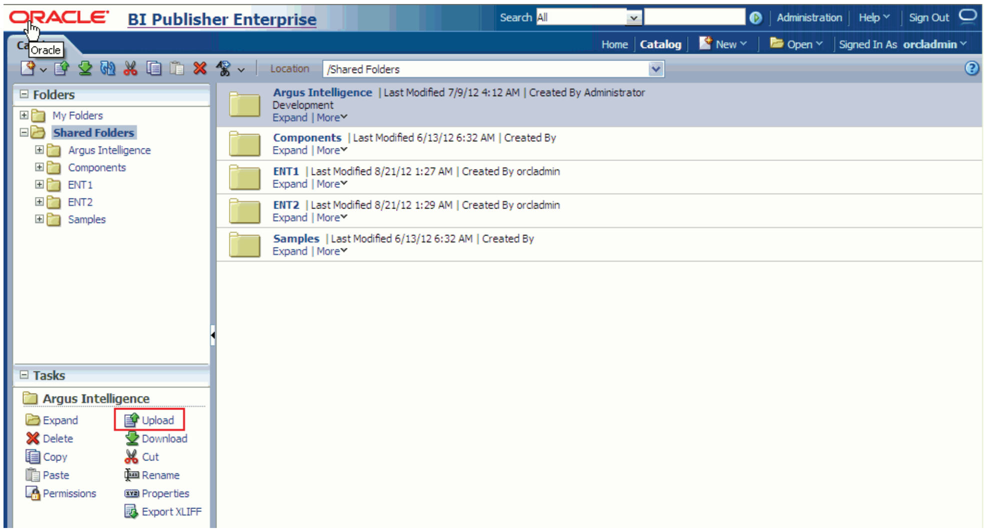


This displays the **Catalog** screen with the **Folders** and **Tasks** sections.

4. Click **Shared Folders** in the **Folders** section as shown in the following figure:


ORACLE BI Publisher Enterprise
Search All
Administration | Help | Sign Out
Catalog
Home | Catalog | New | Open | Signed In As orcladmin
Location /Shared Folders
Folders
My Folders
Shared Folders
Argus Intelligence
Components
ENT1
ENT2
Samples
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
Tasks
Argus Intelligence
Expand
Upload
Delete
Download
Copy
Cut
Paste
Rename
Permissions
Properties
Export XLIFF

5. Click **Upload** in the **Tasks** section as highlighted in the following figure:



**Argus Intelligence** | Last Modified 7/9/12 4:12 AM | Created By Administrator
Development
Expand | More

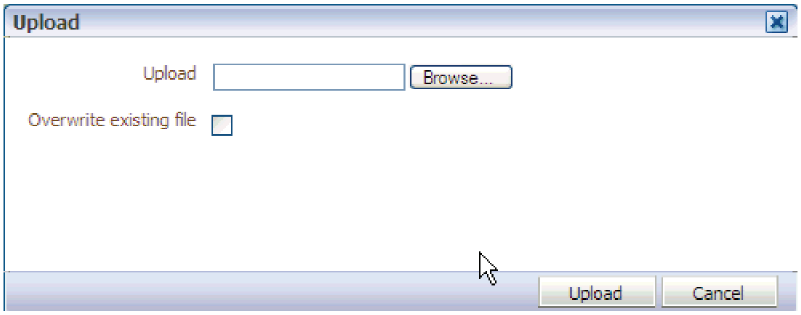
**Components** | Last Modified 6/13/12 6:32 AM | Created By
Expand | More

**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

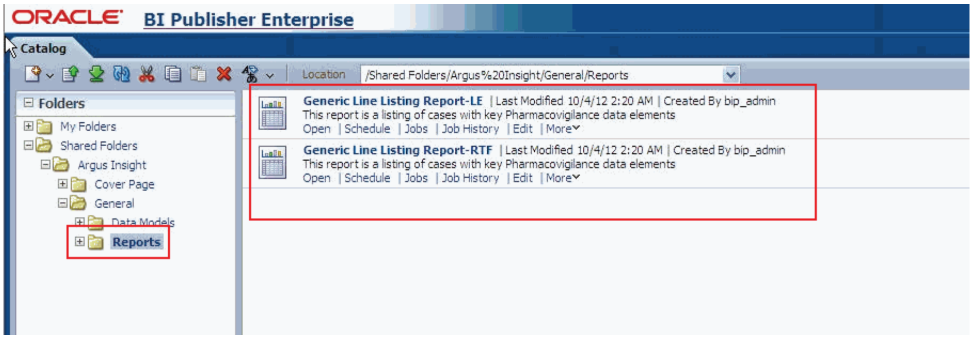
This displays the **Upload** dialog box as shown in the following figure:



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**. Once done, 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 as highlighted in the following figure:



**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

## 8.2 Creating PRMART JDBC Connection

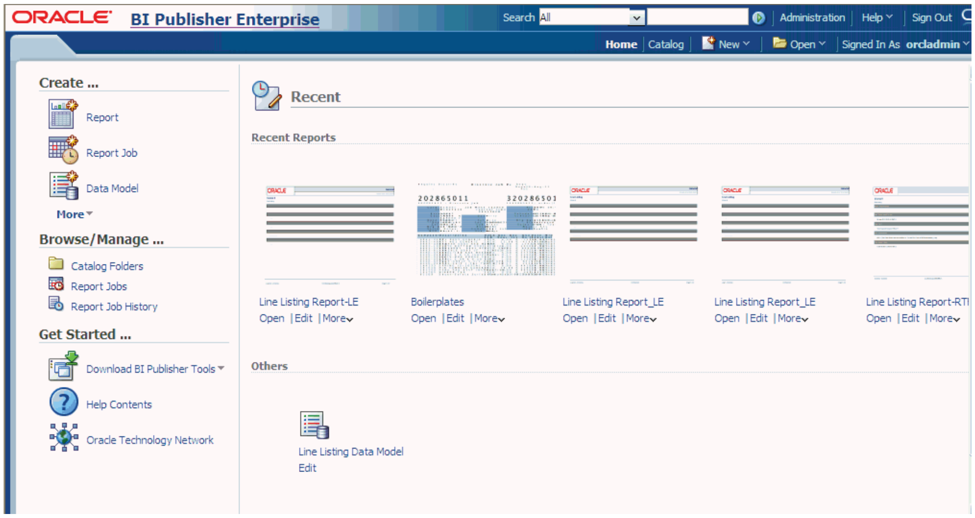
If you are installing BIP on a Windows machine, the TNS entry of Argus Insight must be added in **TNSNAMES.ora** file of the BIP Web Server.

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

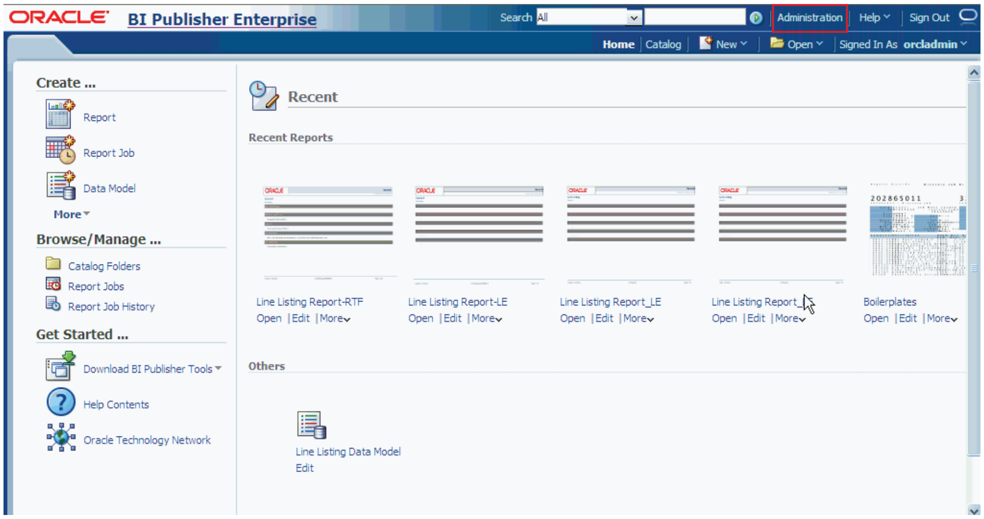
Once you have uploaded the **Argus Insight.xdrz** file to BIP, you also need to create a connection between the BIP and the database.

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

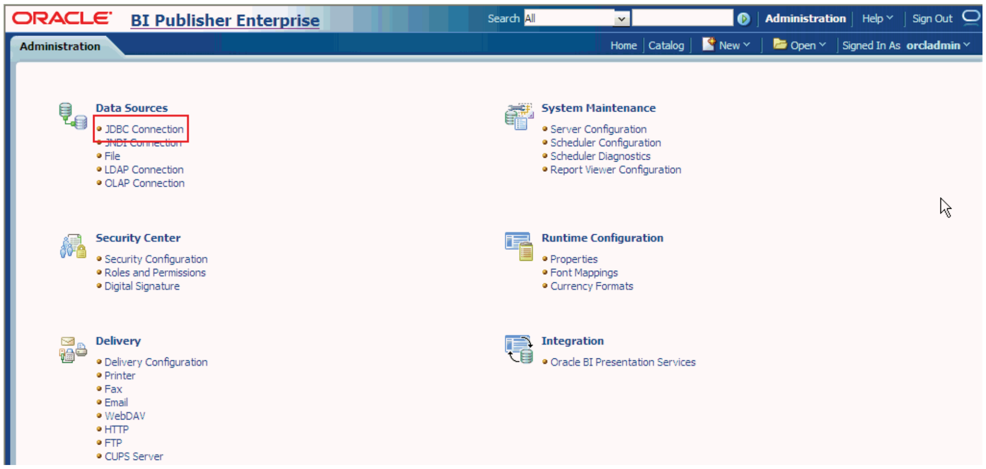
1. Log on to BIP using the administrator credentials. This displays the BIP Home Page as depicted in the following figure:



2. Click **Administration** as highlighted in the following figure:

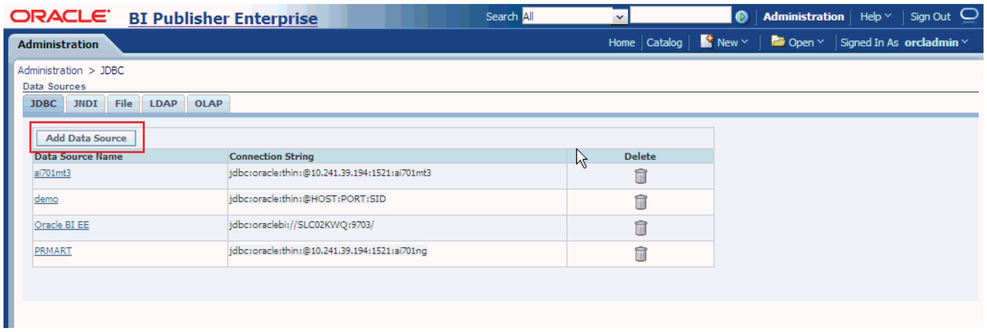


3. Click **JDBC Connection** in the **Data Sources** section as shown in the following figure:



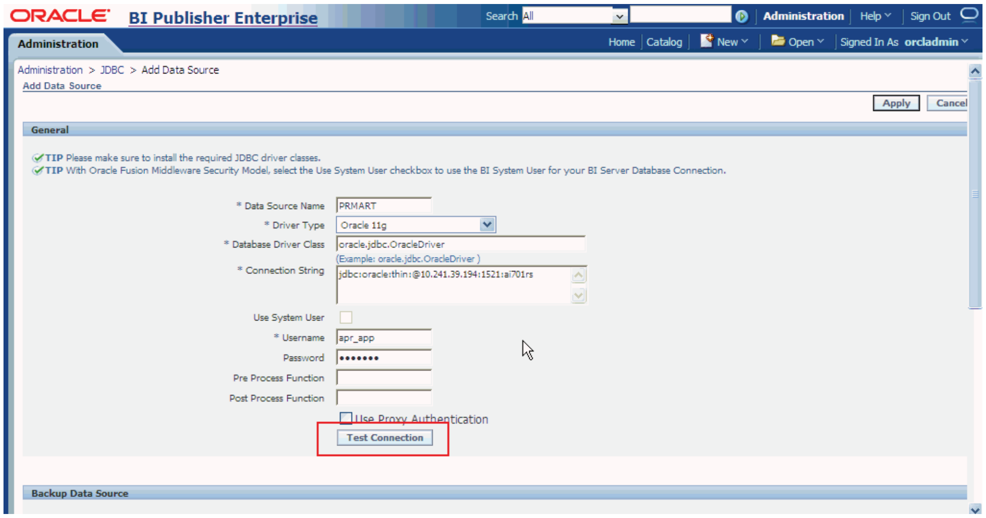
This displays the **Data Sources** Screen.

4. Click **Add Data Source** as highlighted in the following figure:



| 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 | |

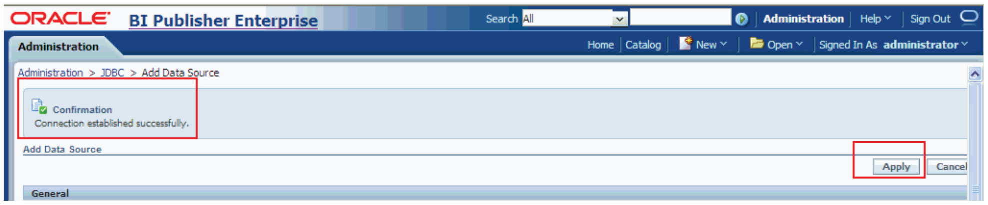
5. In the **Add Data Source** section:
   a. Enter **PRMART** in the **Data Source Name** field.
   b. Select the database from the **Driver Type** drop-down list. This auto-populates the **Database Driver Class** field.
   c. Enter the connection string in the **Connection String** field. You must enter all the details in lower case in this field.
   d. Enter the username (Argus Insight application DB user, for example, apr_app) to connect to the database in the **Username** field.
   e. Enter the password for the user in the **Password** field.
   f. Click **Test Connection** as shown in the following figure:



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.

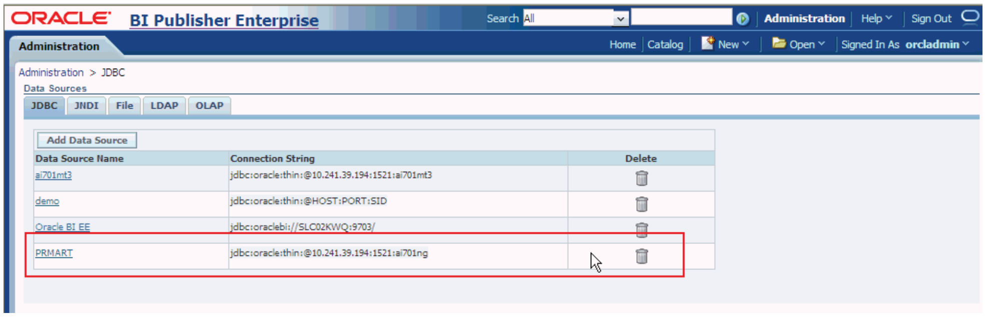
* Data Source Name: PRMART
* Driver Type: Oracle 11g
* Database Driver Class: oracle.jdbc.OracleDriver
(Example: oracle.jdbc.OracleDriver )
* Connection String: jdbc:oracle:thin:@10.241.39.194:1521:ai701rs
Use System User: ☐
* Username: apr_app
Password: •••••••
Pre Process Function:
Post Process Function: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

If successful, this displays a confirmation message, as shown in the following figure:


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

Confirmation
Connection established successfully.

6. Click **Apply**. This displays the **PRMART** Data Source in the list of already existing data source names as shown in the following figure:



| 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 | 🗑 |

This successfully creates a connection between BIP and the database.

## 8.3 Managing Users and Roles: BI Publisher Security Model

Once 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:

- Configuring Server Settings
- Creating Users and Assigning Roles to Users

- Creating Roles, Adding Data Sources, and Assigning Roles

## 8.3.1 Configuring Server Settings

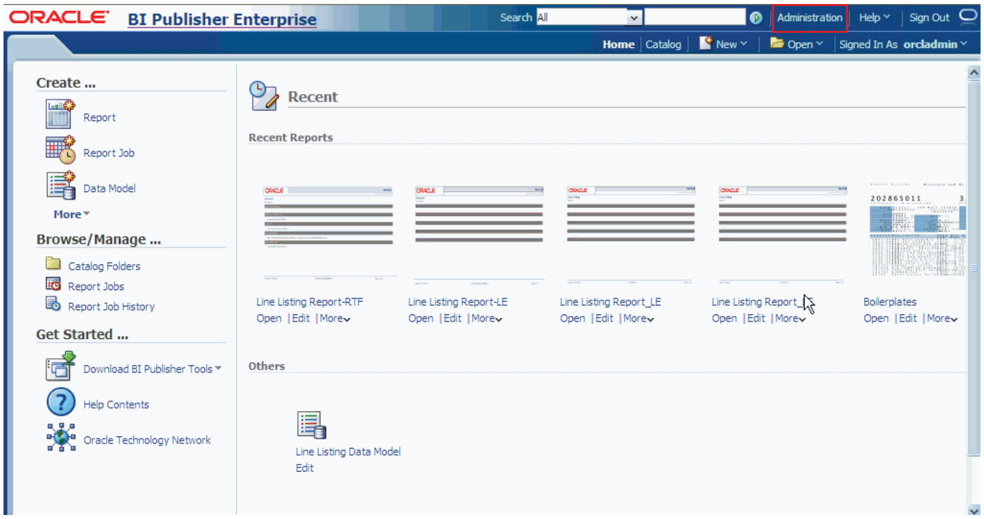
---

**Note:** When using file systems such as NFS, Windows, or NAS for the repository, ensure that the file system is secured.

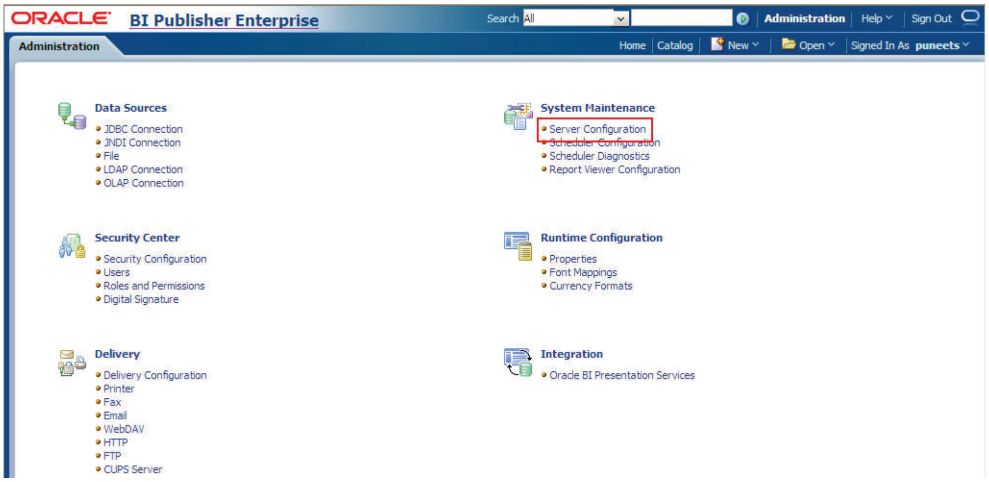
---

To configure the server settings for the BI Publisher Security Model, execute the following steps:

1. Log on to BIP using the administrator credentials. This displays the BIP Home Page.
2. Click **Administration** as highlighted in the following figure:



3. Click **Server Configuration** in the **System Maintenance** section as highlighted in the following figure:



   This displays the **Server Configuration** Screen.

4. In the **Catalog** section, select **Oracle BI Publisher - File System** from the **Catalog Type** drop-down list. If the Catalog Type is not Oracle BI Publisher - File System,

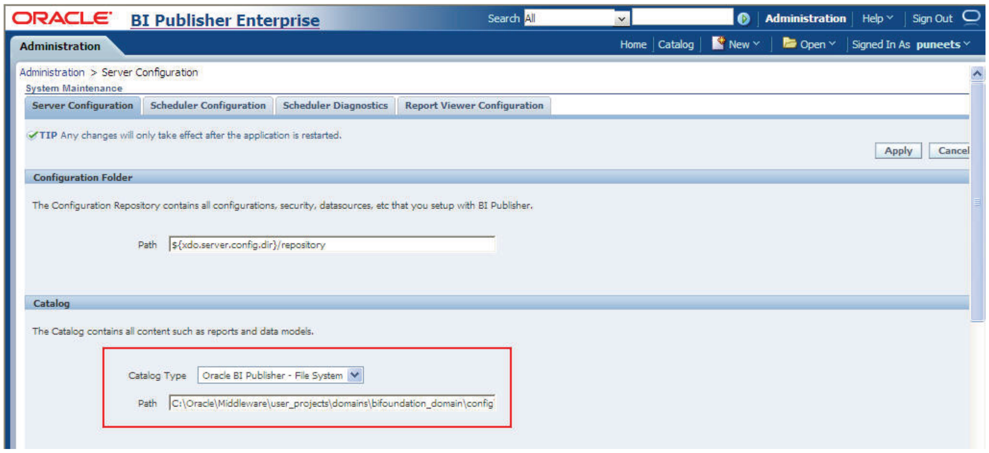
the folder level permission settings cannot be done in BIP. Refer to the BIP Technical Reference document for more information.

---

**Note:** Only **Oracle BI Publisher - File System** is supported in this release.

---

5. Enter the path where all BIP folders, data models, and BIP reports will be stored in the BIP server as highlighted in the following figure:



TIP Any changes will only take effect after the application is restarted.

The Configuration Repository contains all configurations, security, datasources, etc that you setup with BI Publisher.

Path: ${xdo.server.config.dir}/repository

The Catalog contains all content such as reports and data models.

Catalog Type: Oracle BI Publisher - File System

Path: C:\Oracle\Middleware\user_projects\domains\bifoundation_domain\config

6. Click **Apply** to save the changes.
7. Restart the BI server.

---

**Note:** Because the repository is in the file system, the case sensitivity of folder and Report Names is determined by the platform on which you run BI Publisher. For Windows-based environments, the repository object names are not case-sensitive. For UNIX-based environments, the Repository Object Names are case-sensitive.

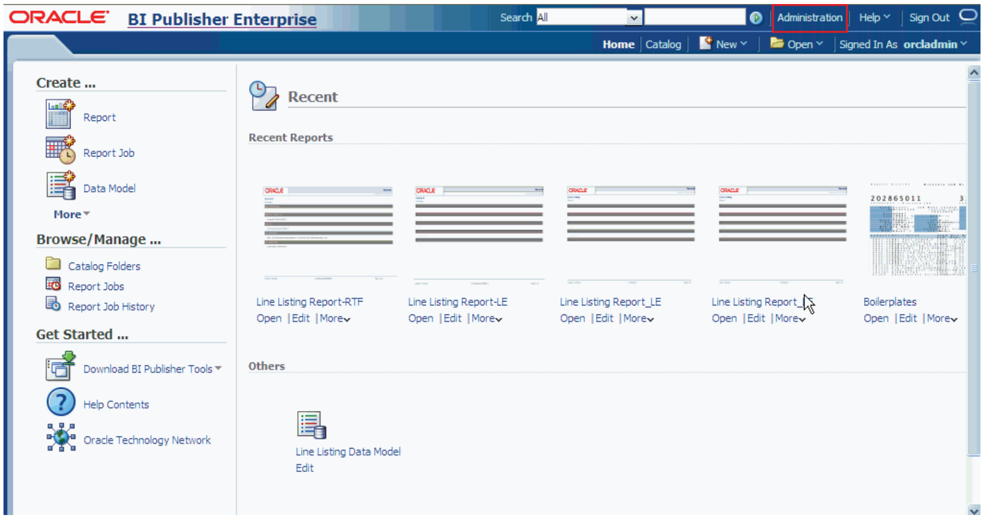
---

For more information, refer to the Configuring Server Properties section of the Administrator's guide for Oracle BIP.

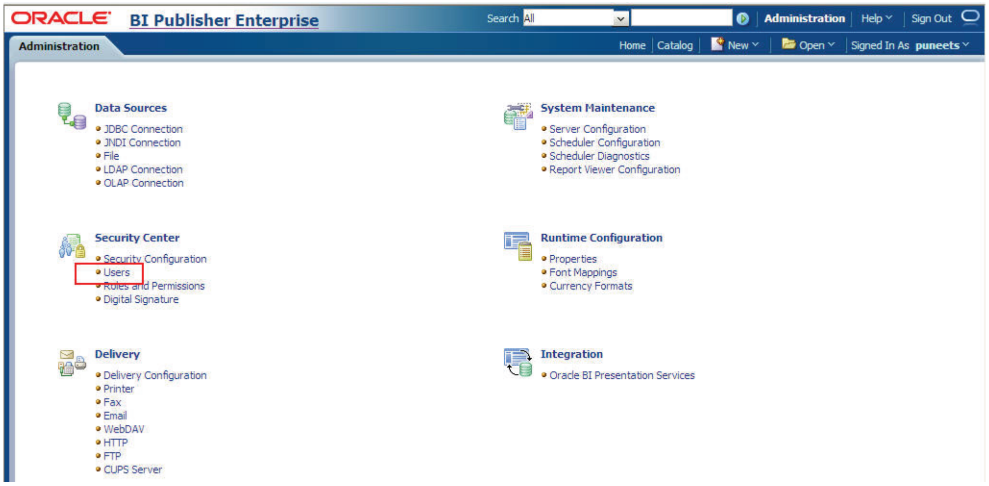
## 8.3.2 Creating Users and Assigning Roles to Users

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

1. Log on to BIP using the administrator credentials. This displays the BIP Home Page.
2. Click **Administration** as highlighted in the following figure:

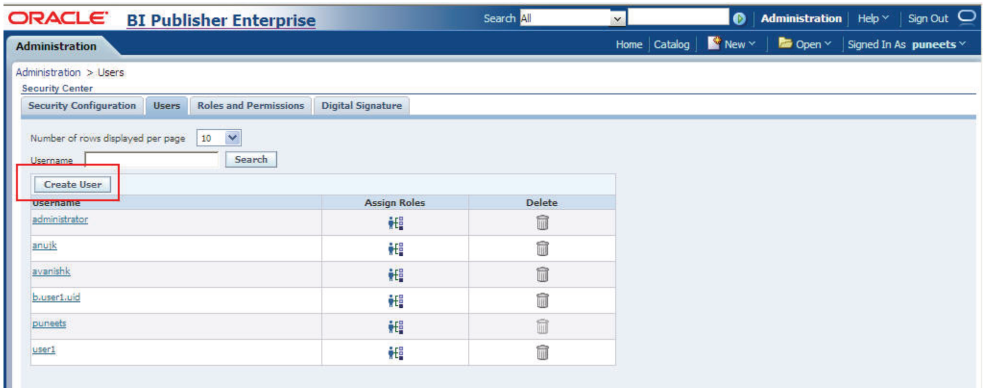


3. Click **Users** in the **Security Center** section as highlighted in the following figure:



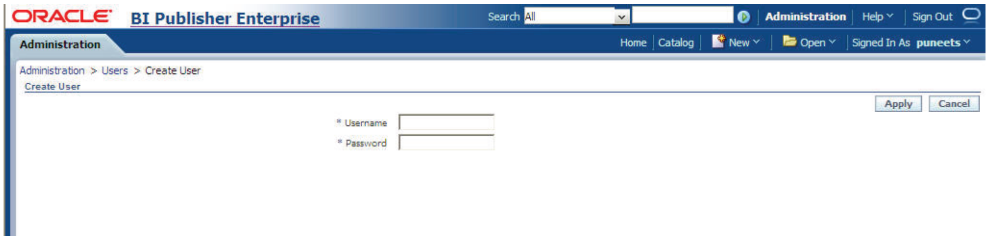
This displays the **Users** screen.

4. Click **Create User** as highlighted in the following figure:



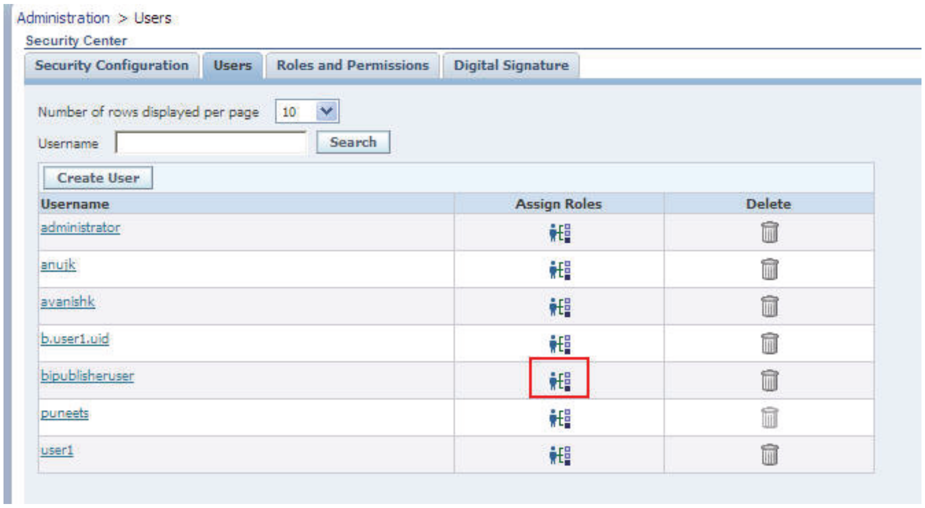
| Username | Assign Roles | Delete |
|---|---|---|
| administrator | | |
| anujk | | |
| avanishk | | |
| b.user1.uid | | |
| puneets | | |
| user1 | | |

This displays the **Create User** Screen as shown in the following figure:



5. Enter the name of the user in the **Username** field.
6. Enter the password in the **Password** field.
7. Click **Apply**. The name of the user is displayed in the list of existing users.

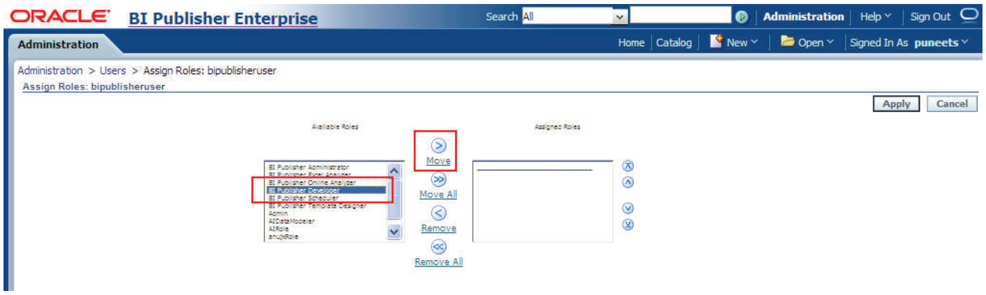
   Once you have created the user, you need to assign the required roles to the user.
8. Click the Assign Roles icon corresponding to the user that you have created as highlighted in the following figure:



| Username | Assign Roles | Delete |
|---|---|---|
| administrator | | |
| anujk | | |
| avanishk | | |
| b.user1.uid | | |
| bipublisheruser | | |
| puneets | | |
| user1 | | |

This displays the Assign Roles Screen for the user. 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 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. Select the role that you want to assign to the user from the **Available Roles** section and click **Move(>)** to move the selected role to the **Assigned Roles** section as depicted in the following figure:


ORACLE BI Publisher Enterprise
Search All
Administration
Help
Sign Out
Home
Catalog
New
Open
Signed In As puneets
Administration > Users > Assign Roles: bipublisheruser
Assign Roles: bipublisheruser
Apply
Cancel
Available Roles
Assigned 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
Move
Move All
Remove
Remove All

10. Click **Apply**. This assigns the selected roles to the user.

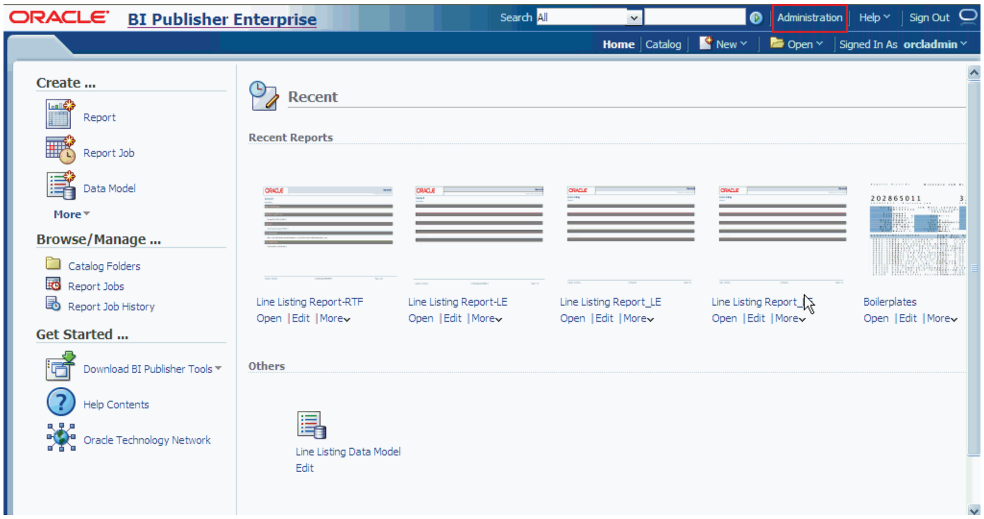
    For the list of users that you need to configure using BIP, refer to the Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model section of this chapter.

## 8.3.3 Creating Roles, Adding Data Sources, and Assigning Roles

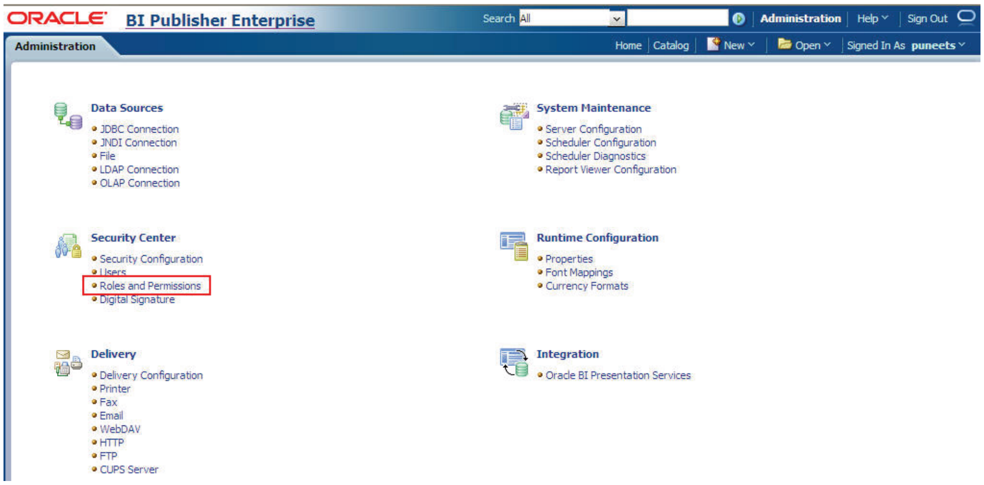
In addition to creating users and assigning them the required roles, you also need to create certain roles, add data sources, and assign them the required roles.

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. This displays the BIP Home Page.
2. Click **Administration** as highlighted in the following figure:

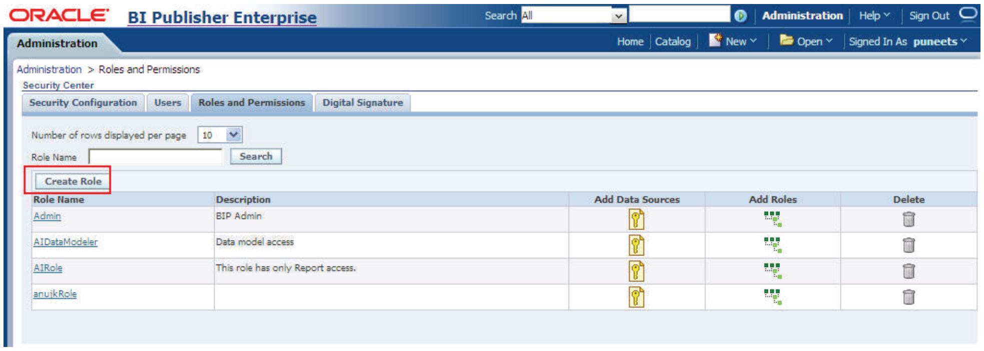


3. Click **Roles and Permissions** in the **Security Center** section as highlighted in the following figure:



   This displays the **Roles and Permissions** Screen.

4. Click **Create Role** as shown in the following figure:



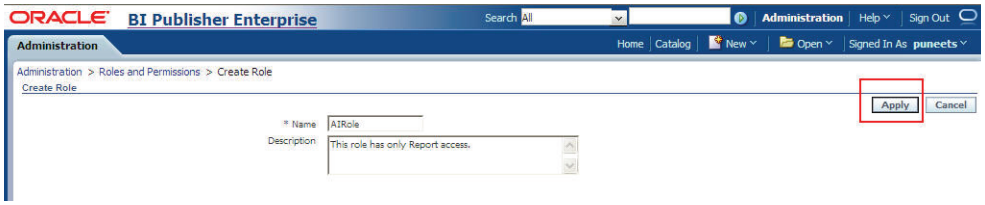
| Role Name | Description | Add Data Sources | Add Roles | Delete |
|---|---|---|---|---|
| Admin | BIP Admin | | | |
| AIDataModeler | Data model access | | | |
| AIRole | This role has only Report access. | | | |
| anuikRole | | | | |

This displays the **Create Role** Screen.

5. Enter the name of the role in the **Name** field.

6. Enter the description for the role in the **Description** field.

7. Click **Apply** to create the new role, as highlighted in the following figure:

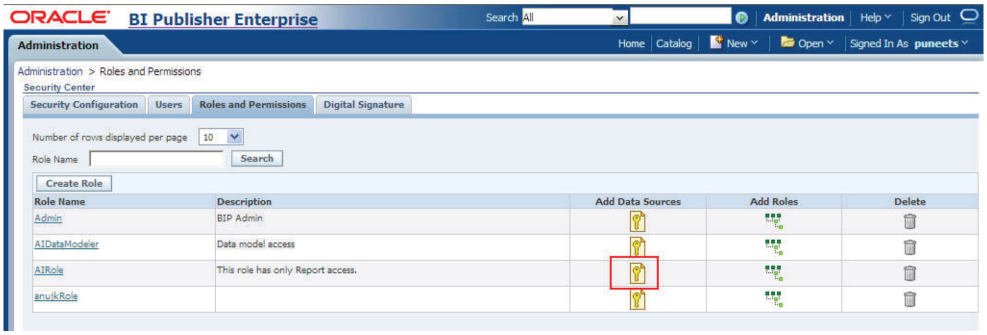


* Name: AIRole

Description: This role has only Report access.

This displays the role in the list of existing roles on the **Roles and Permissions** Screen.

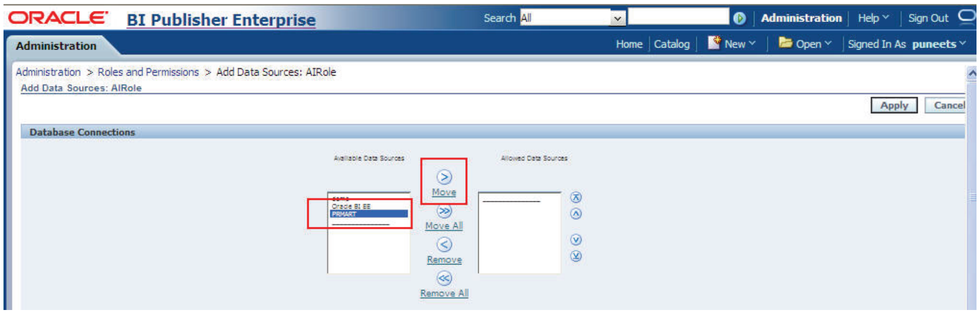
8. Click Add Data Sources Icon, corresponding to the role which you have just created, as depicted in the following figure:



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

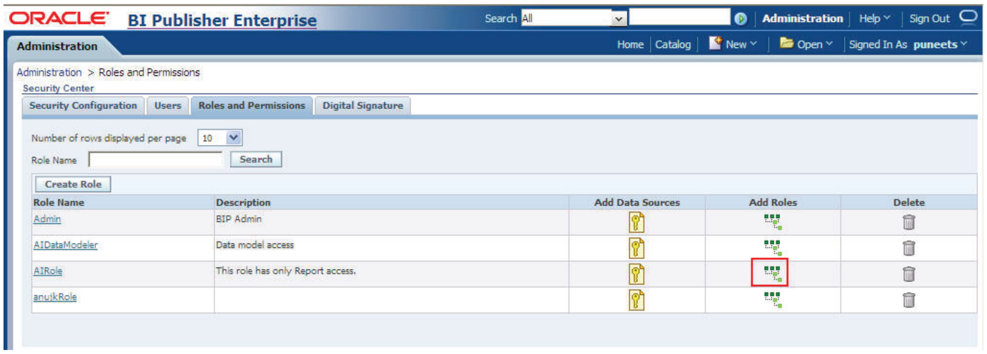
This displays the **Add Data Sources** Screen.

9. Select **PRMART** from the **Available Data Sources** section and click **Move(>)** to move it to the **Allowed Data Sources** section, as highlighted in the following figure:



10. Click **Apply** to save the changes. This again displays the **Roles and Permissions** Screen. See Creating PRMART JDBC Connection section for the steps to create the JDBC connection.

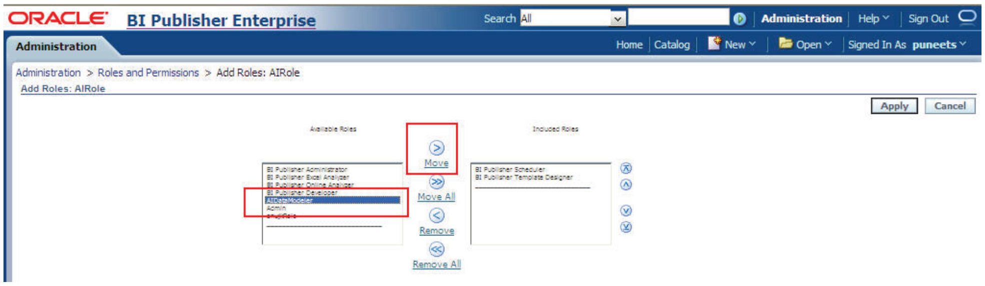
11. Click the Add Roles icon, corresponding to the role which you have just created to add the required roles, as shown in the following figure:



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

This displays the **Add Roles** Screen.

12. Select the roles that you want to include for the role from the **Available Roles** section and click **Move(>)** to move the selected roles to the **Included Roles** section, as highlighted in the following figure:



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

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

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

## 8.4 Managing Users and Roles: Oracle Fusion Middleware Security Model

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 Security Model.

This section comprises the following sub-sections:

- Configuring Server Settings
- Creating Users and Assigning Roles to Users
- Creating Roles, Adding Data Sources, and Assigning Roles in WebLogic Enterprise Manager
- Creating Application Policy

### 8.4.1 Configuring Server Settings

The steps to configure the server settings in the Oracle Fusion Middleware Security Model are exactly the same as that of the BI Publisher Security Model. Refer to Configuring Server Settings for the steps to configure the server settings.

### 8.4.2 Creating Users and Assigning Roles to Users

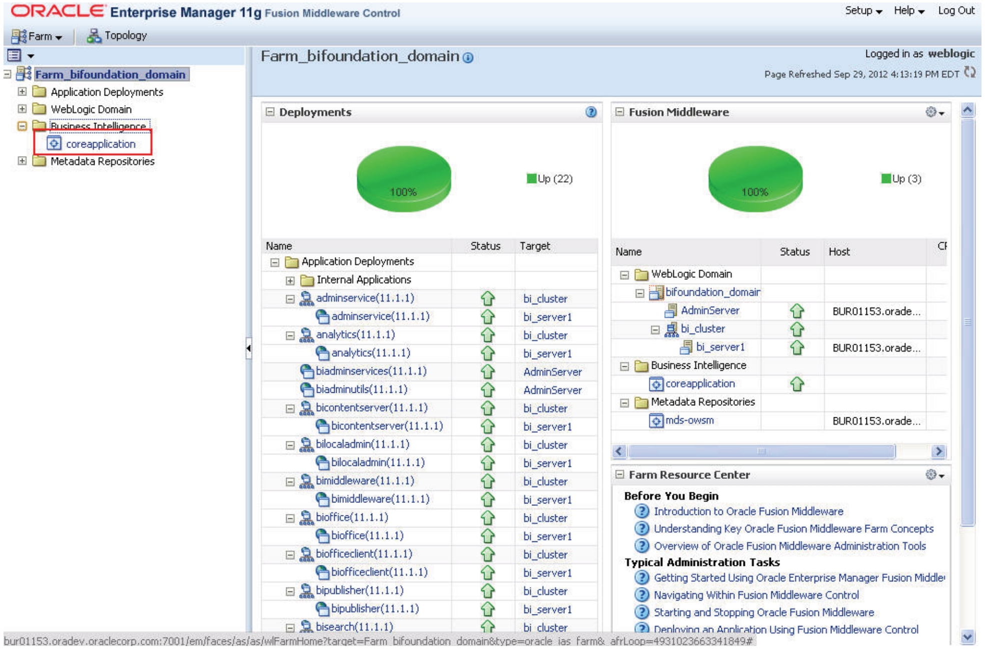
Creating users for LDAP or SSO users is done using the LDAP servers which is beyond the scope of this manual.

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

### 8.4.3 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. This displays the Enterprise Manager home page with a list of folders in the left pane.
2. Expand the **Business Intelligence** folder in the left pane and click **coreapplication**, as shown in the following figure:



Farm_bifoundation_domain

| 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 |

| Name | Status | Host |
|---|---|---|
| WebLogic Domain | | |
| bifoundation_domair | | |
| AdminServer | ⇧ | BUR01153.orade... |
| bi_cluster | ⇧ | |
| bi_server1 | ⇧ | BUR01153.orade... |
| Business Intelligence | | |
| coreapplication | ⇧ | |
| Metadata Repositories | | |
| mds-owsm | | BUR01153.orade... |

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

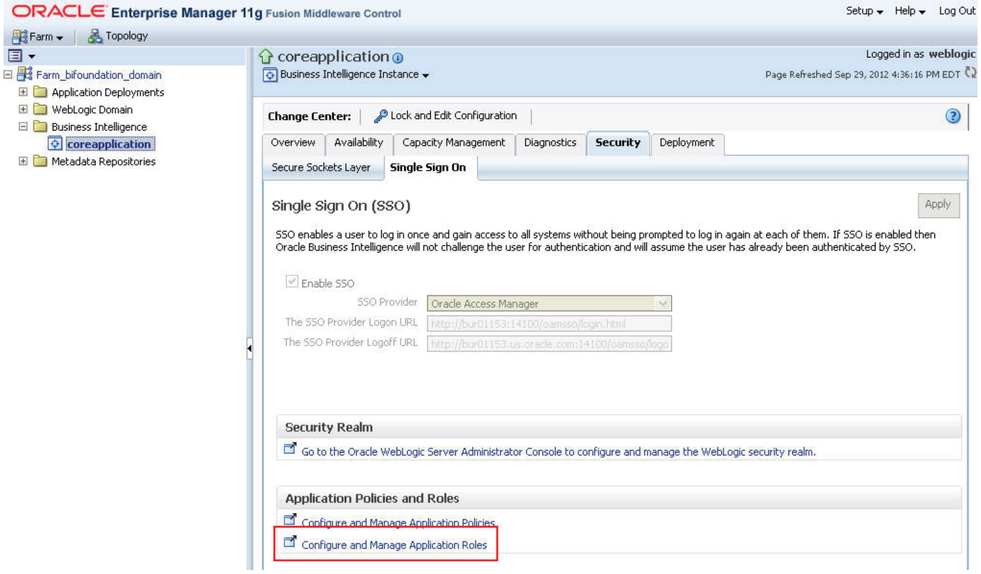
Starting and Stopping Oracle Fusion Middleware

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#

This displays the **coreapplication** Screen in the right pane.

3. Click **Configure and Manage Application Roles** in the **Application Policies and Roles** section, as shown in the following figure:



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

Security Realm

Go to the Oracle WebLogic Server Administrator Console to configure and manage the WebLogic security realm.

Application Policies and Roles

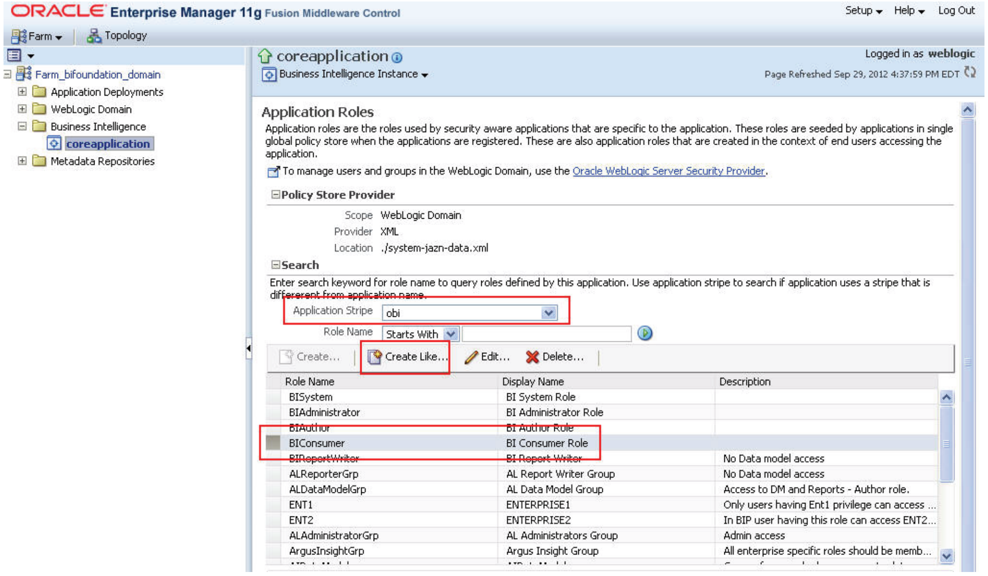
Configure and Manage Application Policies

Configure and Manage Application Roles

This displays the **Application Roles** Screen.

4. Select the required application stripe from the **Application Stripe** drop-down list.

5. Select any existing role (for example, **BIConsumer**) and click **Create Like**, as shown in the following figure:



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

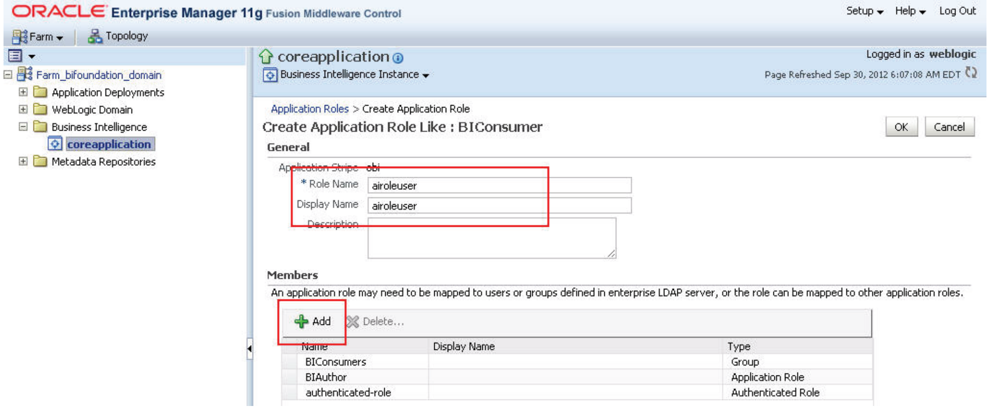
| Role Name | Display Name | Description |
|---|---|---|
| BISystem | BI System Role | |
| BIAdministrator | BI Administrator Role | |
| BIAuthor | BI Author Role | |
| BIConsumer | BI Consumer Role | |
| BIReportWriter | BI Report Writer | No Data model access |
| ALReporterGrp | AL Report Writer Group | 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... |

This displays the **Create Application Role** Screen.

6. Enter the name of the role in the **Role Name** field.

7. Enter the display name and description for the role in the **Display Name** and **Description** fields. These are optional fields.

8. Click **Add** to add any existing application role/group/user to the new role as shown in the following figure:



Logged in as **weblogic**

Page Refreshed Sep 30, 2012 6:07:08 AM EDT

Application Roles > Create Application Role

Create Application Role Like : BIConsumer

**General**

Application Stripe obi
* Role Name airoleuser
Display Name airoleuser
Description

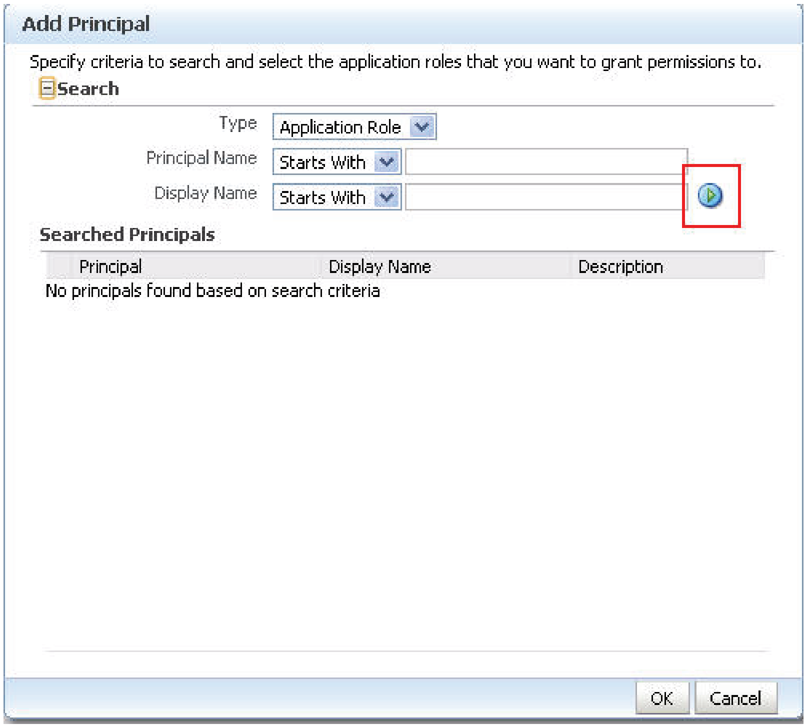
**Members**

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 |

This displays the **Add Principal** Screen.

9. Click the > icon close to the **Display Name** field to display the list of all the roles, groups, and users that are created in LDAP server, as highlighted in the following figure:



Add Principal

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

Type: Application Role

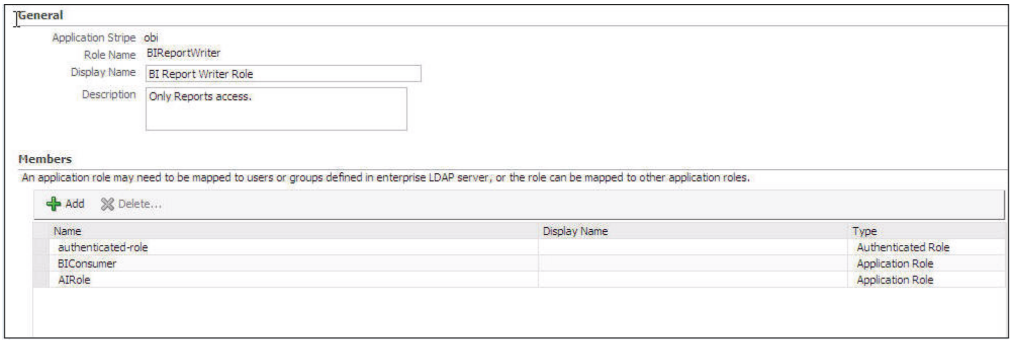
Principal Name: Starts With

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, as shown in the following figure:



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 |

---

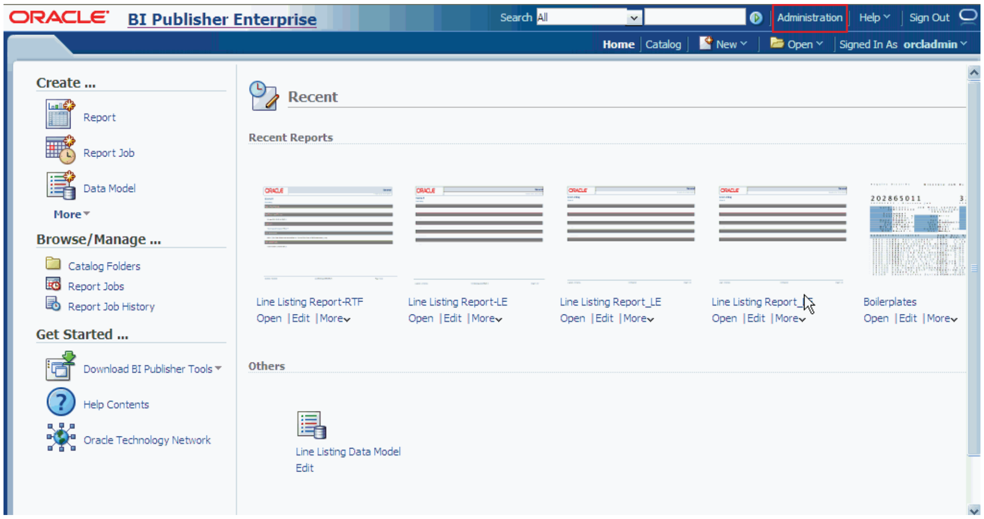
**Note:** The **BIReportWriter** role must be added to the **BIReportWriter** application policy. You can refer to the Creating Application Policy section for the steps to create the application policy for the **BIReportWriter** role.

---

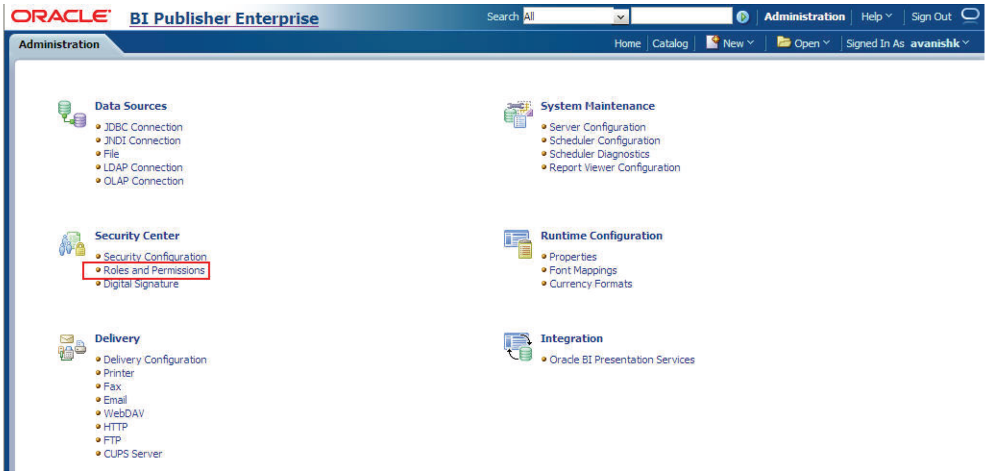
11. Repeat steps 8 to 10 to add more roles, users, and groups to the new role.
12. Click **OK** on the **Create Application Role** Screen to save the changes.

    Once 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. This displays the BIP Home Page.

14. Click **Administration** as highlighted in the following figure:

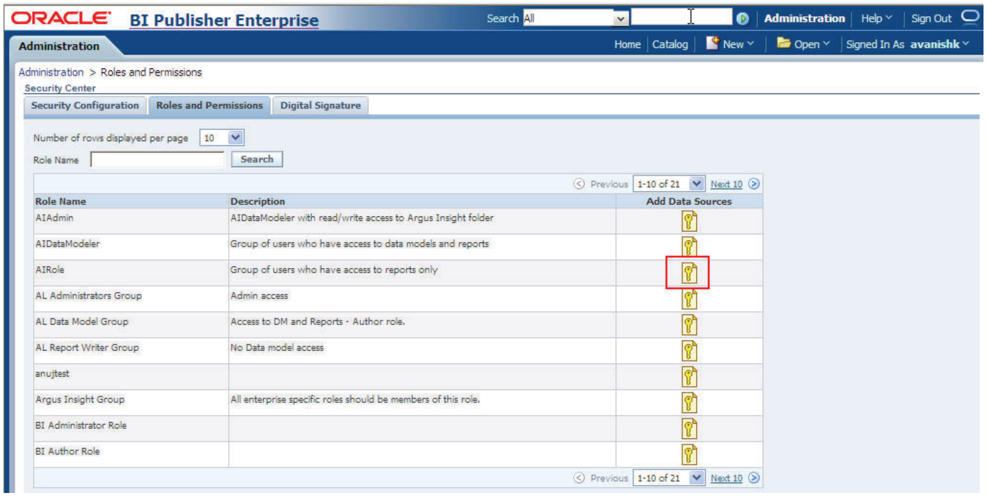


15. Click **Roles and Permissions** in the **Security Center** section as highlighted in the following figure:



This displays the **Roles and Permissions** Screen. You can view the name of the new role which you have just created in the list of role names.

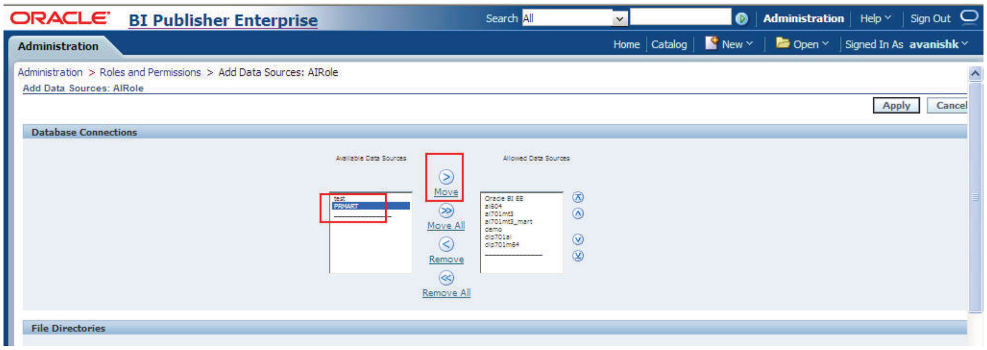
16. Click the Add Data Sources icon corresponding to the name of the new role, as depicted in the following figure:



| Role Name | Description | Add Data Sources |
|---|---|---|
| AIAdmin | AIDataModeler with read/write access to Argus Insight folder | |
| AIDataModeler | Group of users who have access to data models and reports | |
| AIRole | Group of users who have access to reports only | |
| AL Administrators Group | Admin access | |
| AL Data Model Group | Access to DM and Reports - Author role. | |
| AL Report Writer Group | No Data model access | |
| anujtest | | |
| Argus Insight Group | All enterprise specific roles should be members of this role. | |
| BI Administrator Role | | |
| BI Author Role | | |

This displays the **Add Data Sources** Screen.

17. Select **PRMART** from the **Available Data Sources** section and click the **Move (>)** icon to move the PRMART data source to the **Allowed Data Sources** section as shown in the following figure:



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

    For more information, refer to the Creating Application Roles Using Fusion Middleware Control section of the Oracle Administrator's guide for Oracle BIP.

    For the list of roles that need to be configured, refer to the Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model section of this chapter.

## 8.4.4 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 Report Writer policy, you must have created an empty role in the Enterprise Manager.

---

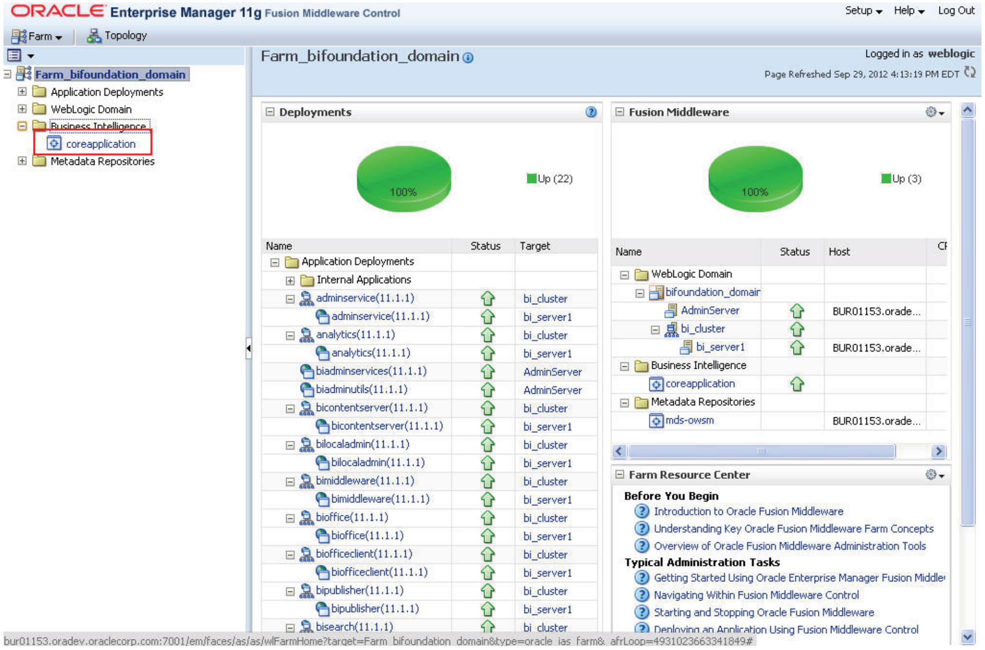
**Note:** The steps mentioned in this section are valid for creating **BIReportWriter** application policy.

---

To create the application policy for the new role, execute the following steps:

1. Log on to the Enterprise Manager. This displays the Enterprise Manager home page with a list of folders in the left pane.

2. Expand the **Business Intelligence** folder in the left pane and click **coreapplication**, as shown in the following figure:



| 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 |

| Name | Status | Host |
|---|---|---|
| WebLogic Domain | | |
| bifoundation_domair | | |
| AdminServer | ↑ | BUR01153.oracle... |
| bi_cluster | ↑ | |
| bi_server1 | ↑ | BUR01153.oracle... |
| Business Intelligence | | |
| coreapplication | ↑ | |
| Metadata Repositories | | |
| mds-owsm | | BUR01153.oracle... |

Before You Begin

- Introduction to Oracle Fusion Middleware
- Understanding Key Oracle Fusion Middleware Farm Concepts
- Overview of Oracle Fusion Middleware Administration Tools

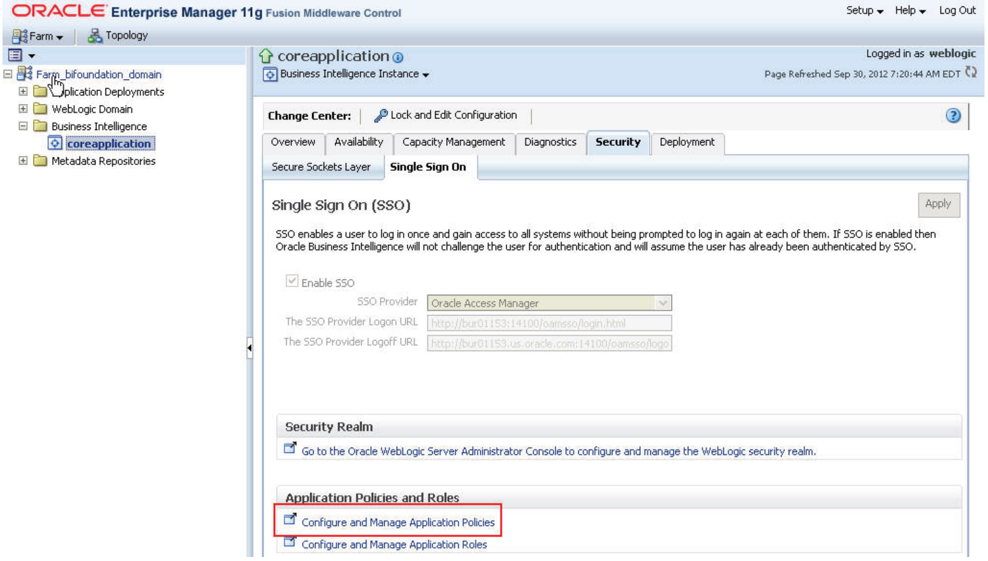
Typical Administration Tasks

- 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#

This displays the **coreapplication** Screen in the right pane.

3. Click **Configure and Manage Application Policies** in the **Application Policies and Roles** section, as shown in the following figure:



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.

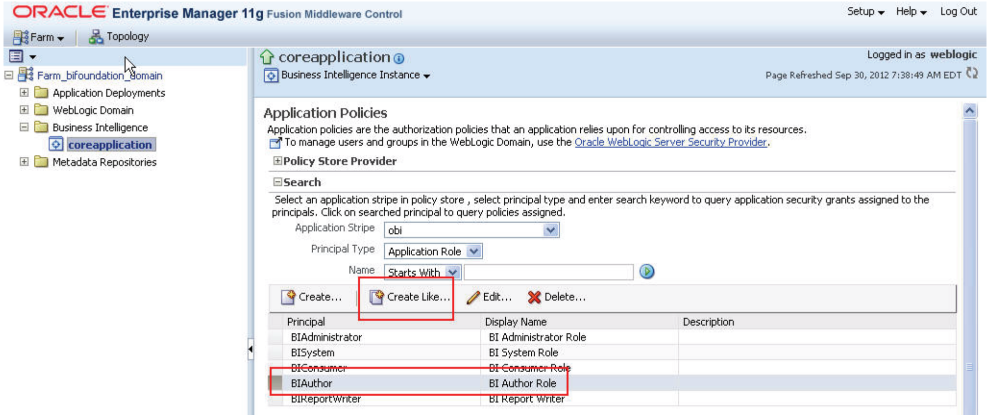
Configure and Manage Application Policies

Configure and Manage Application Roles

This displays the **Application Policies** Screen.

4. Select **obi** from the **Application Stripe** drop-down list.

5. Select the **BIAuthor** policy and click **Create Like** as shown in the following figure:



Logged in as weblogic

Page Refreshed Sep 30, 2012 7:38:49 AM EDT

Application Policies

Application policies are the authorization policies that an application relies upon for controlling access to its resources.

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

Select an application stripe in policy store , select principal type and enter search keyword to query application security grants assigned to the principals. Click on searched principal to query policies assigned.

Application Stripe obi

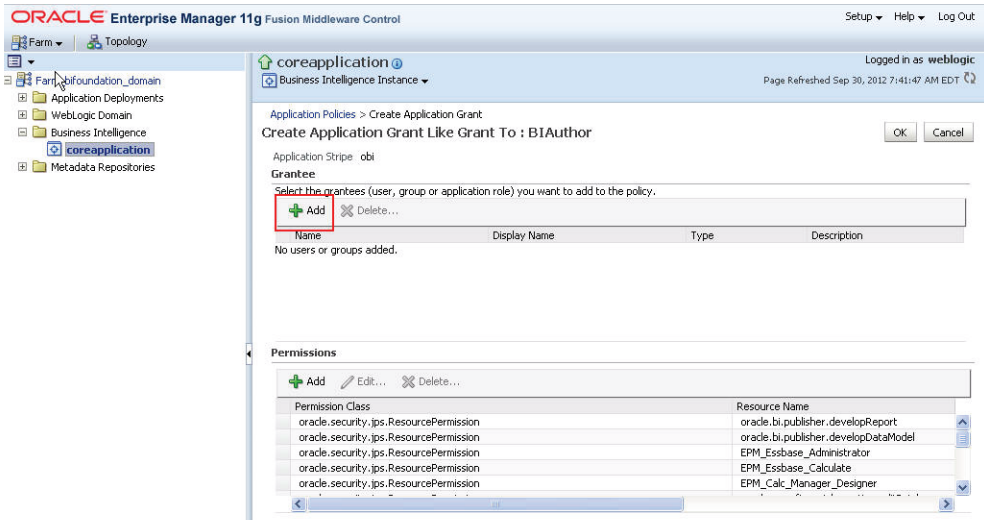
Principal Type Application Role

Name Starts With

| Principal | Display Name | Description |
|---|---|---|
| BIAdministrator | BI Administrator Role | |
| BISystem | BI System Role | |
| BIConsumer | BI Consumer Role | |
| BIAuthor | BI Author Role | |
| BIReportWriter | BI Report Writer | |

This displays the **Create Application Grant Like** Screen with the **Grantee** and **Permissions** sections.

**6.** Click **Add** in the **Grantee** section, as highlighted in the following figure:



Logged in as weblogic

Page Refreshed Sep 30, 2012 7:41:47 AM EDT

Create Application Grant Like Grant To : BIAuthor

Application Stripe obi

Grantee

Select the grantees (user, group or application role) you want to add to the policy.

| Name | Display Name | Type | Description |
|---|---|---|---|

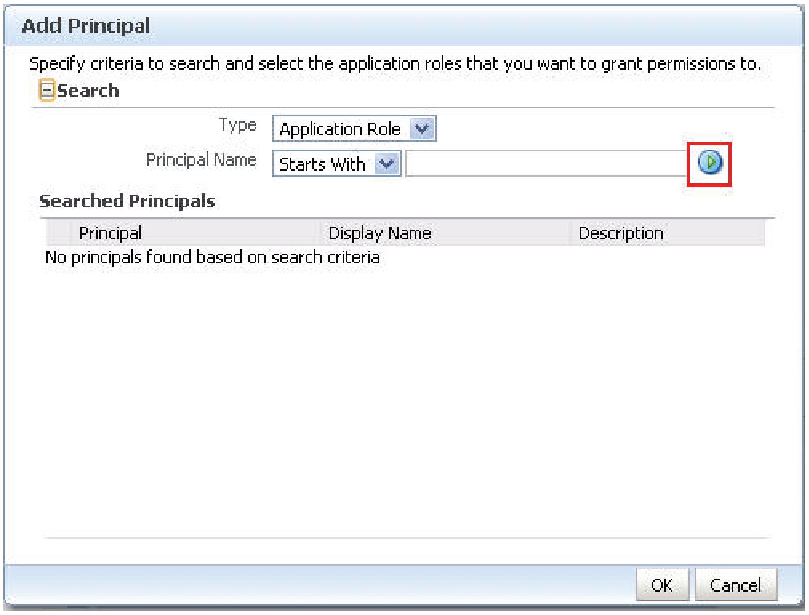
No users or groups added.

Permissions

| Permission Class | Resource Name |
|---|---|
| oracle.security.jps.ResourcePermission | oracle.bi.publisher.developReport |
| oracle.security.jps.ResourcePermission | oracle.bi.publisher.developDataModel |
| oracle.security.jps.ResourcePermission | EPM_Essbase_Administrator |
| oracle.security.jps.ResourcePermission | EPM_Essbase_Calculate |
| oracle.security.jps.ResourcePermission | EPM_Calc_Manager_Designer |

This displays the **Add Principal** Screen.

**7.** Click the > icon close to the **Principal Name** field to retrieve the list of all the available application roles, as shown in the following figure:



Add Principal

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

Search

Type: Application Role

Principal Name: Starts With

Searched Principals

| Principal | Display Name | Description |
|---|---|---|

No principals found based on search criteria

8. Select the name of the role from the **Searched Principals** section (for example, BIReportWriter) and click **OK**. This again displays the **Create Application Grant Like** Screen.
9. Select the **developDataModel** Resource Name from the list of Permission Classes and click **Delete.**
10. Click **OK** to apply the changes.

## 8.5 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 Managing Users and Roles: BI Publisher Security Model and Managing Users and Roles: Oracle Fusion Middleware Security Model sections of this chapter.

### 8.5.1 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.

### 8.5.2 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.

### 8.5.3 Report Writer 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.

### 8.5.4 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).

### 8.5.5 Configuring BIP Roles

The following table illustrates the Roles that you need to configure using BIP:

***Table 8–1 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** |
| 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** |

### 8.5.6 Folder Level Permissions

This section explains the Folder Level permissions that you need to grant using BIP.

Refer to the **About Catalog Permissions** section in Oracle Administrator's Guide for Oracle BIP for more information.

***Table 8–2 Folder Level Permissions***

| Folder | Roles to be added | Permissions |
|---|---|---|
| Argus Insight | AIAdminRole | Full access |
| **Argus Insight** > **General** > **Data Model** | AIDataModelerRole, AIRole | AIDataModelerRole - Full access<br>AIRole - Read, Run, Schedule, and View report |
| **Argus Insight** > **General** > **Reports** | AIRole | Full access |
| **Argus Insight** > **CoverPage** | AIRole | Full access |
| Enterprise specific folders | Enterprise Specific Admin Role | Full access |
| Enterprise Specific Folder -- Data Model | Enterprise Modeler Role, Enterprise Report Role | Enterprise Modeler Role - Full access<br>Enterprise Report Role -Read, Run, Schedule, and View report |
| Enterprise Specific Folder - Reports | Enterprise Report Role | Full access |

## 8.6 Configuring BIP Roles and Permissions: BI Publisher Security Model

This section explains the users, which you need to create, and the roles that you need to assign to those users using the BI Publisher.

This section comprises the following sub-sections:

- Argus Insight Specific Users and Roles
- Enterprise Specific Users and Roles

### 8.6.1 Argus Insight Specific Users and Roles

The Argus Insight folder comprises two sub-folders:

- Data Models
- Reports

There are three types of Argus Insight specific users and their corresponding roles. The following is the list of users that you need to create along with the name of the role for each user:

- **User Name:** AIAdminRole Users, **Role Name:** AIAdminRole
- **User Name:** AIDataModeler Users, **Role Name:** AIDataModelerRole
- **User Name:** AIRole Users, **Role Name:** AIRole

In addition to these users that you need to create, there is a default BI Admin User for the application. This user is a super user with a BIP administration access and has also got access to upload the Argus Insight repository.

The access to the Data Models and Reports folder depends on the type of the user and the role assigned to that user. In addition, the BI publisher also allows you to add roles

(Nested Role) to a role (Super Role). In that case, the user with the Super Role privileges also has the privileges of the nested role. For example, a user has been assigned an X role and you add Y role to the X role, that user also has the privileges of the Y role, even though Y role is not directly assigned to the user.

You can refer to Managing Users and Roles: BI Publisher Security Model or Managing Users and Roles: Oracle Fusion Middleware Security Model section, depending on the Security Model that you are using for the steps to create users, create roles, and assign roles to users and roles.

The following table lists the Argus Insight specific users that you need to create, the roles that you need to assign to the users, and the description about the privileges for each user and role:

***Table 8–3 Argus Insight Specific Users and Roles***

| Name of the User/Role | Users/Roles to be added | Description |
|---|---|---|
| BI Admin User | BI Administration (Functional Role) | The BI Admin User has access to upload the Argus Insight repository and works as a Super user who has BIP Administration access. |
| AIAdminRole | AIDataModelerRole | The user with this role has full access to the **Argus Insight** Folder. |
| AIAdminRole Users | AIAdminRole | This user has full access to the **Argus Insight** Folder. |
| AIDataModelerRole | BI Publisher Developer<br>AIRole | The user with this role has access to the Argus Insight **Data Models** and **Reports** folders. |
| AIDataModeler Users | AIDataModelerRole | The user has access to Argus Insight **Data Models** and **Reports** folders. |
| AIRole | BITemplate Designer and BI Publisher Scheduler roles | The users belonging to this role have read-only access to the Argus Insight **Data Models** folder and full access of the Argus Insight **Reports** folder. |
| AIRole Users | AIRole | This user has read-only access to the Argus Insight **Data Models** folder and full access to the Argus Insight **Reports** folder. |

## 8.6.2 Enterprise Specific Users and Roles

In addition to the Argus Insight specific users and roles, you can also create Enterprise specific users and roles, and add extra privileges to those users and roles by adding Argus Insight specific roles to them.

Similar to the Argus Insight folder, each enterprise comprises the **Data Models** and **Reports** folder.

There are three types of Enterprise specific users and their corresponding roles. The following is the list of enterprise specific users that you need to create along with the name of the role for each user:

- **User Name:** Enterprise Specific Admin Users, **Role Name:** Enterprise Admin Role
- **User Name:** Enterprise Modeler Role Users, **Role Name:** Enterprise Modeler Role
- **User Name:** Enterprise Report Role Users, **Role Name:** Enterprise Report Role

*Table 8–4 Enterprise Specific Users and Roles*

| Name of the User/Role | Users/Roles to be added | Description |
|---|---|---|
| Enterprise Admin Role | AIAdminRole (Created in 8.6.1 section) | The user belonging to this role has full access to the Enterprise specific folder.<br>In addition, the user belonging to this role also has full access to the Argus Insight folder. |
| Enterprise Specific Admin Users | Enterprise Admin Role | This user has full access to the Enterprise specific Folder.<br>In addition, this user has full access to the Argus Insight folder. |
| Enterprise Modeler Role | AIDataModelerRole (Created in 8.6.1 section)<br>Enterprise Report Role | The user belonging to this role has access to:<br>Argus Insight **Data Models** folder (Full access)<br>Argus Insight **Reports** folder (Read, Run, Schedule, View report)<br>Enterprise specific **Data Models** folder (Full access)<br>Enterprise specific **Reports** folder (Read, Run, Schedule, View report) |
| Enterprise Modeler Role Users | Enterprise Modeler Role | This user has access to:<br>Argus Insight **Data Models** folder (Full access)<br>Argus Insight **Reports** folder (Read, Run, Schedule, View report)<br>Enterprise specific **Data Models** folder (Full access)<br>Enterprise specific **Reports** folder (Read, Run, Schedule, View report) |
| Enterprise Report Role | AIRole (Created in 8.6.1 section) | The user belonging to this role has access to:<br>Argus Insight **Data Models** folder (Read only)<br>Argus Insight **Reports** folder (Full access)<br>Enterprise specific **Data Models** folder (Read only)<br>Enterprise specific **Reports** folder (Full access) |
| Enterprise Report Role Users | Enterprise Report Role | This user has access to:<br>Argus Insight **Data Models** folder (Read only)<br>Argus Insight **Reports** folder (Full access)<br>Enterprise specific **Data Models** folder (Read only)<br>Enterprise specific **Reports** folder (Full access) |

For information on the Folder Level permissions that you need to grant using BIP, refer to the Folder Level Permissions section.

## 9

# Managing the Argus Insight Cryptography Key

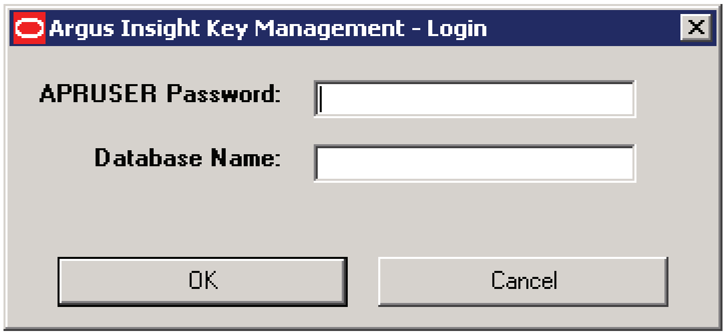
This chapter describes how to update the cryptography key in Argus Insight *after* the key has been updated in Argus Safety.

## 9.1 Updating the Cryptography Key

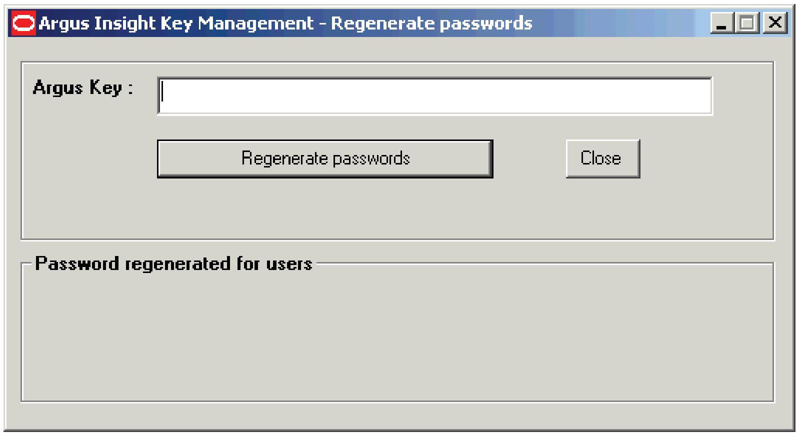
After the cryptography key has been updated in Argus Safety, you must update the cryptography key in Argus Insight. This process will update all the required passwords in Argus Insight using the new key.

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 opens.



4. Log in to the Key Management tool:
   a. Enter the password for the APR_USER.
   b. Enter the name of the Argus Insight database.
   c. Click **OK.** The system authenticates your login and then opens the Argus Insight Key Management - Regenerate passwords dialog box.


Argus Insight Key Management - Regenerate passwords
Argus Key :
Regenerate passwords
Close
Password regenerated for users

5. Enter the new key from the Argus Safety Server. You can copy this key from the ArgusSecureKey.ini file, which is present on all Argus Safety Servers. 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 system:

   - Displays whether the regeneration process was successful (or failed)
   - Lists the passwords that changed

   **Note:** The list of changed passwords for the Cognos version of Argus Insight will be different from the list for the BusinessObjects version.

## 9.1.1 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. If you failure to copy the files, the Cognos Server or any other Argus Insight Web Server will not function.

## 9.1.2 Restarting IIS and Running ETL

After you change the cryptography key, you must complete the following steps on the Argus Insight Web Server for your changes to take effect:

1. Restart the Internet Information Services (IIS).
2. Run the incremental ETL.

# 10

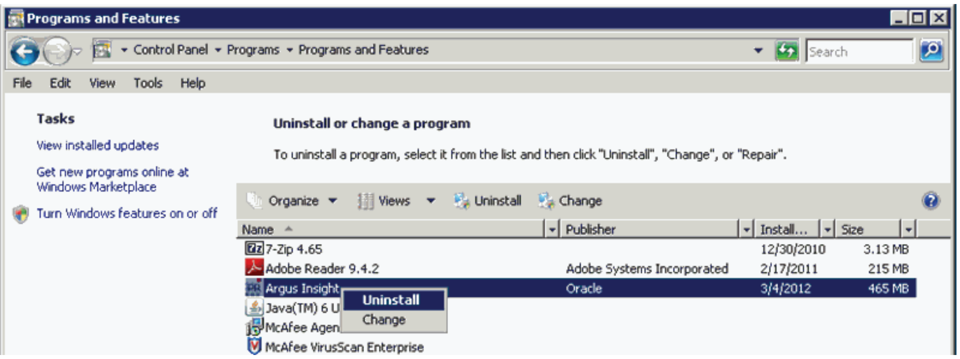
# Uninstalling the Argus Insight Application

This chapter describes how to uninstall the Argus Insight application.

## 10.1 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 select **Uninstall** from the menu.

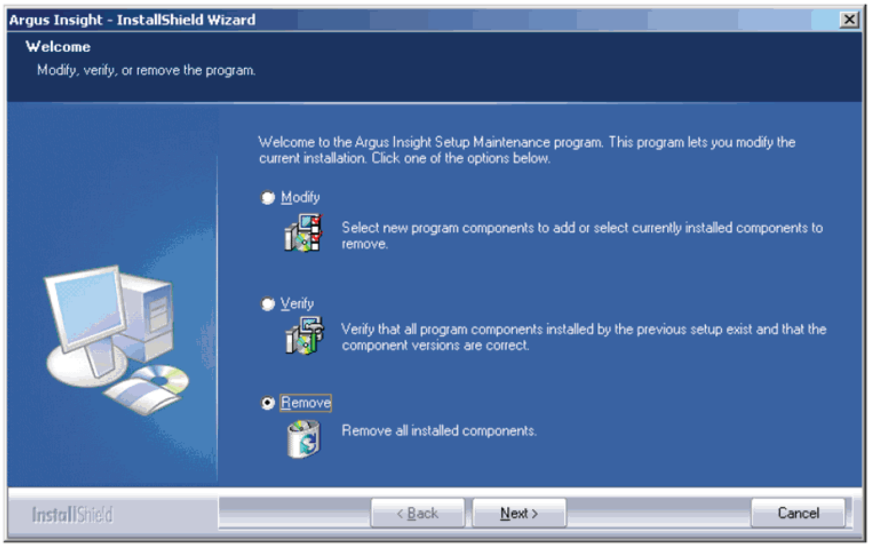

Programs and Features
Control Panel ▾ Programs ▾ Programs and Features
Search
File Edit View Tools Help
Tasks
View installed updates
Get new programs online at Windows Marketplace
Turn Windows features on or off
Organize ▾ Views ▾ Uninstall Change
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click "Uninstall", "Change", or "Repair".

| Name | Publisher | Install... | Size |
|---|---|---|---|
| 7-Zip 4.65 | | 12/30/2010 | 3.13 MB |
| Adobe Reader 9.4.2 | Adobe Systems Incorporated | 2/17/2011 | 215 MB |
| Argus Insight | Oracle | 3/4/2012 | 465 MB |
| Java(TM) 6 U | | | |
| McAfee Agen | | | |
| McAfee VirusScan Enterprise | | | |

The system starts the Argus Insight wizard and opens the Welcome screen with options for modifying, verifying, and removing programs.


Argus Insight - InstallShield Wizard
Welcome
Modify, verify, or remove the program.

Welcome to the Argus Insight Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

○ Modify

Select new program components to add or select currently installed components to remove.

○ Verify

Verify that all program components installed by the previous setup exist and that the component versions are correct.

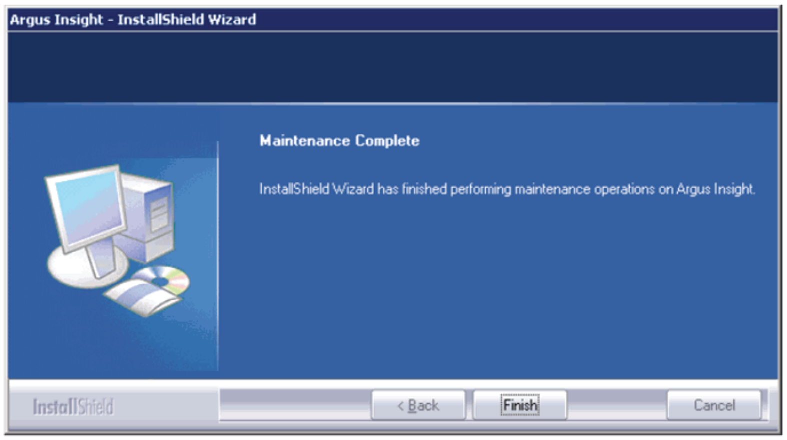
● Remove

Remove all installed components.

5. Select **Remove** and click **Next.**

   The wizard prompts you to confirm that you want to completely remove the selected application and all of its features.

6. Select **Yes** to continue. The wizard uninstalls the Argus Insight application and reports when the process is completed.



Maintenance Complete

InstallShield Wizard has finished performing maintenance operations on Argus Insight.

7. Click **Finish.** The wizard informs you that the system must be restarted to complete the uninstall 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.

### 10.1.1 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.

### 10.1.2 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.

## 10.2 Uninstalling Argus Insight from the Business Intelligence Server

With Argus Insight, you can use either Cognos 8 or BusinessObjects for your Business Intelligence tool. To uninstall Argus Insight from either the Cognos Server or the BusinessObjects Server, follow the procedures in Section 10.1, "Uninstalling Argus Insight from the Web Server."