Oracle® Argus Insight

Installation Guide

Release 7.0.3

E41483-01

August 2013

ORACLE®

Oracle Argus Insight Installation Guide, Release 7.0.3

E41483-01

Contents

4 Configuring the Argus Insight Application

5 Extracting, Transforming, and Loading Data

Preface

This *Oracle Argus Insight Installation Guide* describes installing — or upgrading to — Argus Insight 7.0.3. 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

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.

Conventions

The following text conventions are used in this document:

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

1 Introduction

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

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

This chapter includes the following topics:

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 through a query. The query retrieves a set of specific type of cases (*Case Series*) from the data mart and then runs the report on only those cases.

Use these Argus Insight components to retrieve the Case Series: *Query By Example (QBE)*, *Filters*, and *Advanced Conditions*. Next, run one of these reports on the Case Series: the built-in *Standard Reports* or the custom reports.

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

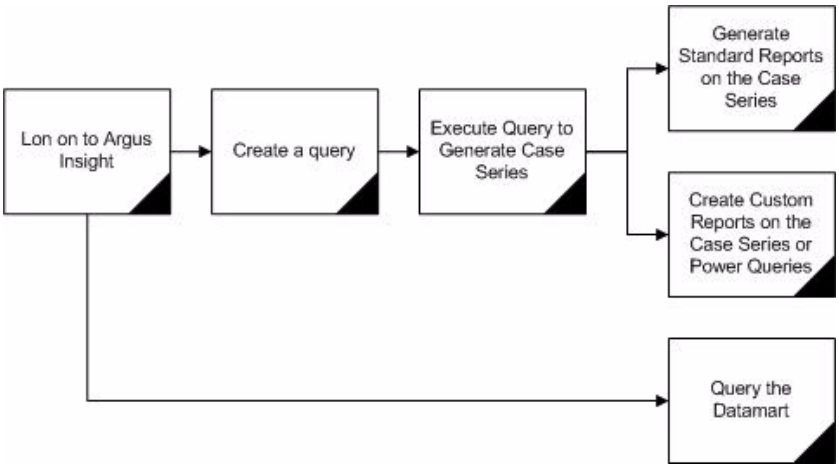


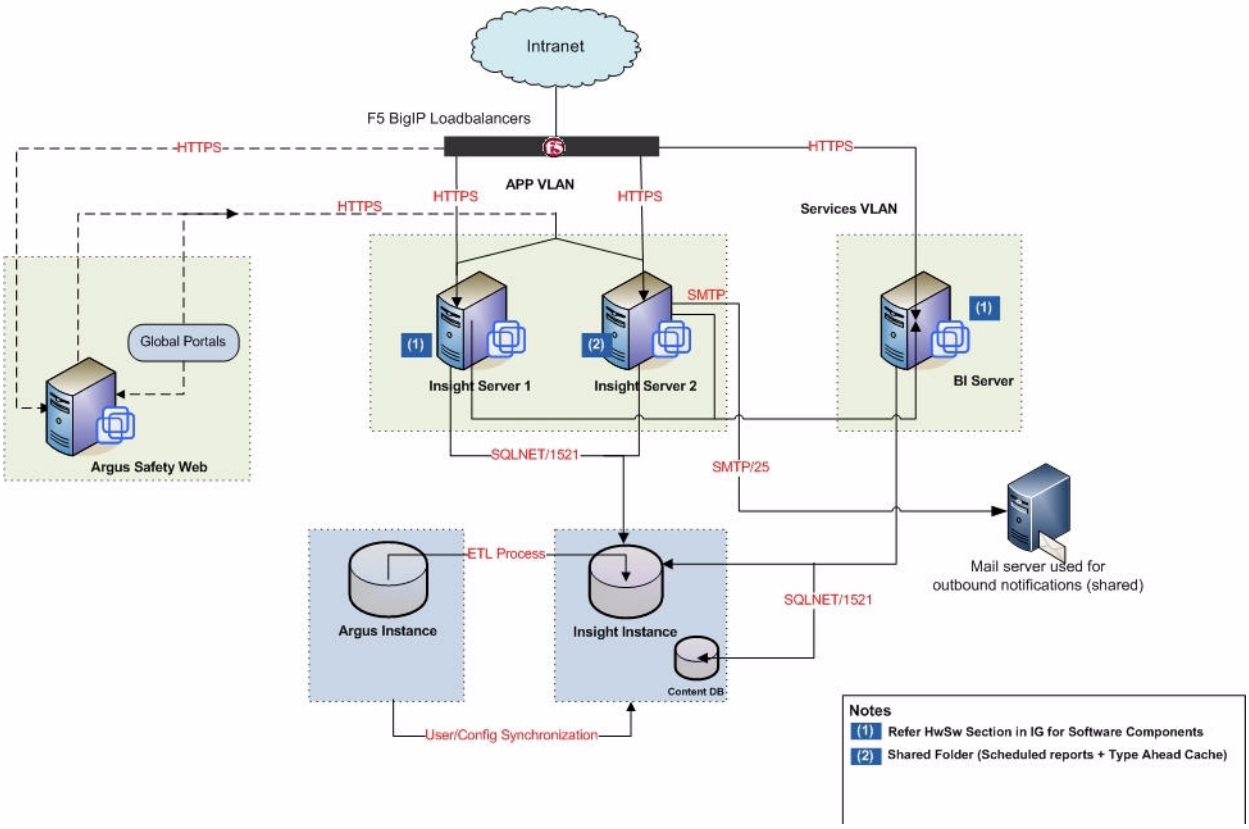
Table 1–1 describes the various features of Argus Insight:

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 the General category. Typically, these reports are run on the 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
- BI Publisher, BusinessObjects Server or Cognos (depending on which Business Intelligence tool you are using with Argus Insight)

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

- Database Server
- Argus Insight Client

Table 1–2 Argus Insight Software and Hardware Requirements

Component	Requirements
Argus Insight Web Server	**Supported Operating Systems:** ■ Windows 2008 R2 SP1 Enterprise (64 bit) ■ Windows 2008 R2 SP1 Standard (64 bit) ■ Windows 2008 SP2 Enterprise (32 bit) ■ Windows 2008 SP2 Standard (32 bit) **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ Oracle Client 11.2.0.3 (32 bit) (with SQL Plus, SQL Loader, Oracle and OLEDB Objects) ■ Oracle Data Provider 11.2.0.3 for .Net **Hardware Requirements:** ■ Up to 5000 cases in the system: 2x2.6 GHz processors, 4 GB memory ■ More than 5000 cases in the system: 4x2 GHz processors, 8 GB memory **Additional Software Requirements:** ■ Dotnet Framework 3.5 Service Pack 1 ■ IIS 7.5 (IIS 6.0 compatibility pack should also be installed) ■ Microsoft Internet Explorer 8.0, or 9.0 ■ Microsoft Visual C++ 2008 SP1 Redistributable ■ MSXML 6.0 **Note:** The Argus Insight Web Server should be configured for Simple Mail Transfer Protocol (SMTP) for email support.
BI Publisher (BIP)	**Supported Operating Systems:** ■ Oracle Enterprise Linux X86 (Version: 5.5.0.0.0 and 5.7.0.0) ■ Oracle Enterprise Linux X86-64 (Version: 5.5.0.0.0 and 5.7.0.0) ■ Solaris 10 ■ Solaris 11 ■ Oracle Enterprise Linux 6.2 UEK ■ Windows 2008 R2 SP1 Enterprise (64 bit) ■ Windows 2008 R2 SP1 Standard (64 bit) ■ Windows 2008 SP2 Enterprise (32 bit) ■ Windows 2008 SP2 Standard (32 bit) **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ 11.2.0.3 Client **Tool Version:** ■ BIP 11.1.1.6.0
BusinessObjects Server	**Supported Operating Systems:** Same as the Argus Insight Web Server **Oracle Database Software:** Oracle Client 11.2.0.3 (32 bit and 64 bit) (with SQL Plus, SQL Loader, Oracle and OLEDB Objects) **Hardware Requirements:** Same as the Argus Insight Web Server **Reporting Tool:** ■ BusinessObjects XI Release 4.0 Service Pack 6

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

Component	Requirements
Cognos Server	**Supported Operating Systems:** Same as the Argus Insight Web Server, or Oracle Enterprise Linux 6.2 UEK (English) **Oracle Database Software:** Same as the Argus Insight Web Server **Hardware Requirements:** Same as the Argus Insight Web Server **Reporting Tool:** ■ Cognos 10.2 BI Server (default installation with all components except Cognos Content Database) ■ Cognos 10.2 BI Modeling (default installation with all components)
Database Server	**Supported Operating Systems:** ■ Oracle Enterprise Linux X86 (Version: 5.5.0.0.0 and 5.7.0.0) ■ Oracle Enterprise Linux X86-64 (Version: 5.5.0.0.0 and 5.7.0.0) ■ Solaris 10 ■ Solaris 11 ■ Oracle Enterprise Linux 6.1 UEK ■ Oracle Enterprise Linux 6.2 UEK ■ Windows 2008 R2 SP1 Enterprise (64 bit) ■ Windows 2008 R2 SP1 Standard (64 bit) ■ Windows 2008 SP2 Enterprise (32 bit) ■ Windows 2008 SP2 Standard (32 bit) **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ Oracle Database Server (Standard/Enterprise - AL32UTF8 character set) - Version 11.2.0.3 (32/64 bit) Oracle Advanced Security Transparent Data Encryption* (Optional) Oracle Advanced Security Network Encryption (Optional) ***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). TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications. Argus Insight product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature. ■ Oracle RAC 11g R2 ■ Exadata 11g R2 **Note:** Oracle database standard edition is supported for single tenant deployment only. **Hardware Requirements:** ■ Up to 5000 cases in the system: 2x2 GHz processors, 4 GB memory ■ More than 5000 cases in the system: 4x2 GHz processors, 16 GB memory

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

Component	Requirements
Argus Insight Client	**Supported Operating Systems:** ■ Windows XP Professional, Service Pack 3 (32 bit), (English version) ■ Windows 7 (32 bit), (English version) ■ Windows 7 (64 bit), (English version) **Hardware Requirements:** ■ 2.0 GHz Minimum, 1 GB Memory **Additional Software Requirements:** ■ Adobe Acrobat Reader 10 ■ Microsoft Excel 2007 or 2010 ■ Microsoft Internet Explorer 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, BI Publisher, BusinessObjects Server, or Cognos Server:

- **Installation Language —** You must install all software with the language setting configured to English. For example, if Oracle is installed in a language other than English, the registry entries are created with different names. Therefore, to avoid errors, install all software in English.
- **Oracle Client —** You must install the Oracle client with the default *ORACLE_HOME* name, provided by the Oracle Universal Installer. Failure to do so will display an error message, stating that the Oracle OLE DB provider was not found during installation.
- **Time Zone —** You must set all servers to the same time zone.
- **Default Language Setting —** All the servers must have the default language setting enabled for US English.

  To enable US English as the default language setting:

  1. Open the Microsoft System Registry Editor.
     a. Click **Start.**
     b. Select **Run.**
     c. 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 BI Publisher

- Ensure that you have disabled the firewall. Alternatively, if the firewall is enabled, ensure that BI Publisher is accessible from other machines on the network.

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.

1.3.1.4 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.

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.

1.3.3 General Installation Notes and Information

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

To do so:

1. Navigate to **Argus Console, System Management** (Common Profile Switches), and select **Network Settings.**
2. 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 and standard reports, and the Schema Creation Tool.

This chapter includes the following topics:

2.1 Before You Install the Argus Insight Application

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

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

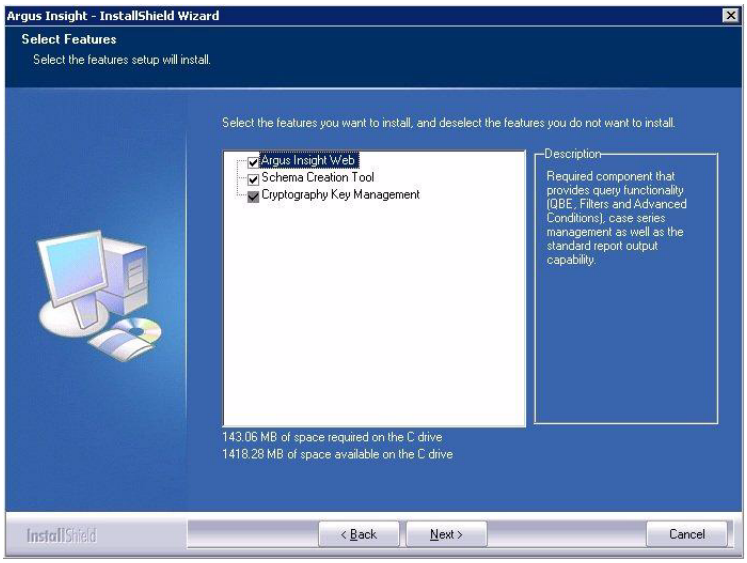
2.2 Installing Argus Insight Components onto the Web Server

Note: If you are upgrading Argus Insight from 7.0.2 to Argus Insight 7.0.3, first uninstall the application using Argus Insight application, and then run the Argus Insight 7.0.3 Installer.

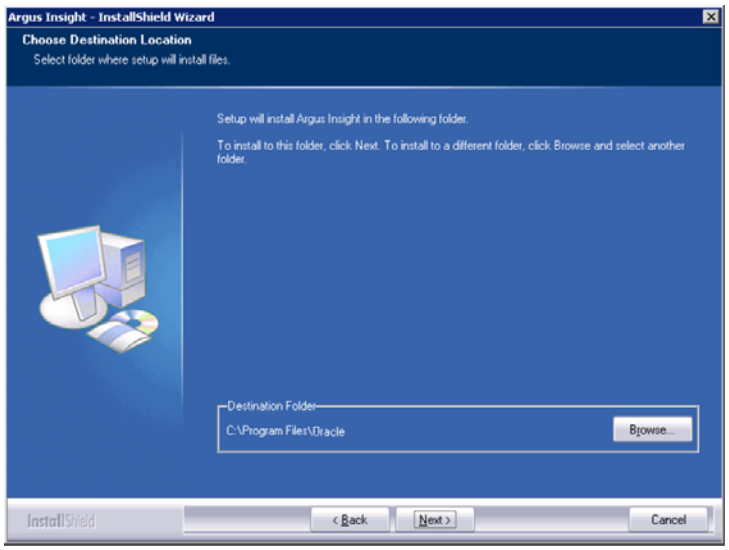
To unistall the existing application, see Section 10, "Uninstalling the Argus Insight Application".

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

1. Download the Argus Insight software from Oracle E-delivery and copy the software to the Argus Insight Web Server.
2. Log in to the Argus Insight Web Server as a user with administrator privileges.
3. Click **setup.exe.** The 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. Enter your user name and company name into the appropriate fields.
6. Click **Next** to continue. The **Select Features** dialog box opens.



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



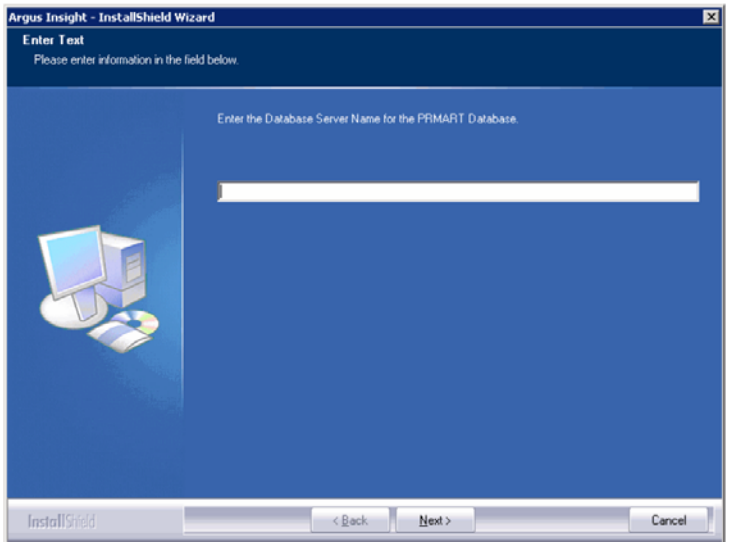
9. Specify the folder into which the system installs the Argus Insight application:

- 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.

10. 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.

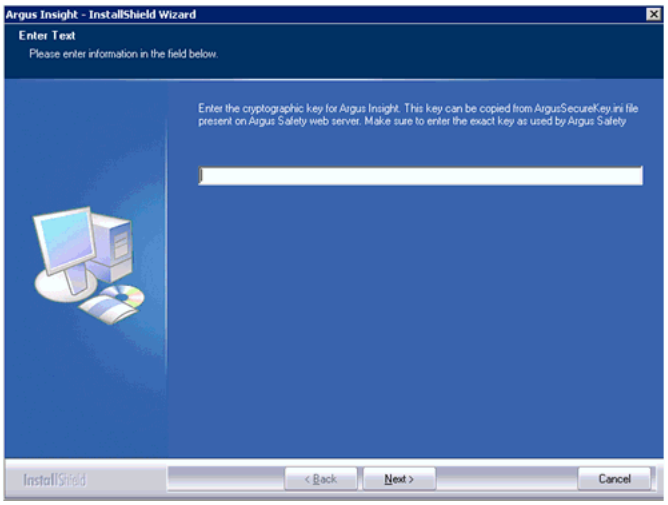
    When the installation is done, the following dialog box opens:



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



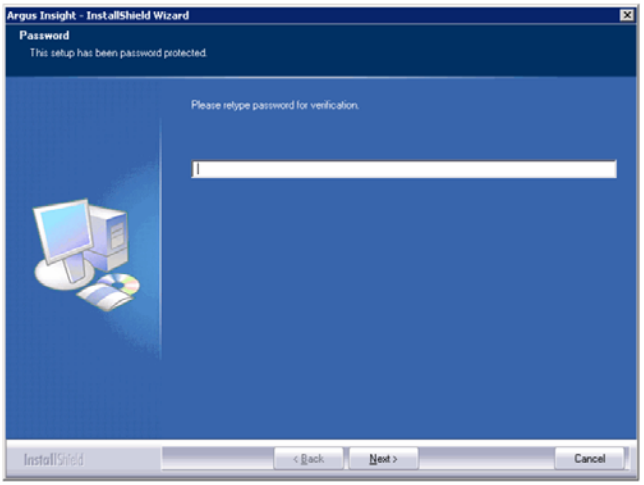
14. Enter the cryptographic key for Argus Insight, and then click **Next** to continue.

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

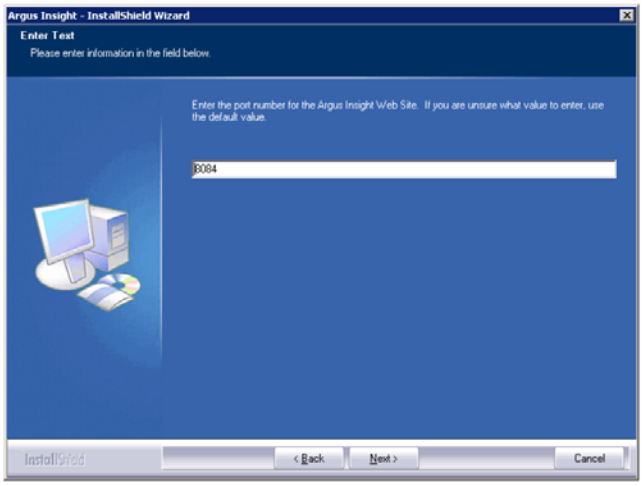
15. Enter the password for APR_USER.

> **Note:** The APR_USER database user provides initial database access to the application user (APR_APP) of Argus Insight. Make sure that this password is the same on all machines where any Argus Insight components are stored.
>
> You will be prompted to create/update this user during schema creation. You can modify this password by running the Argus Insight installer and selecting the Modify option. For information about updating the APR_USER password, see Section 2.2.1, "Changing the APR_USER Password."

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



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

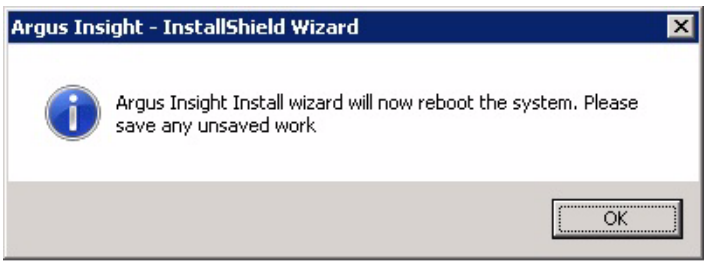


19. Enter the port number you want to assign to the Argus Insight website.

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

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

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



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

2.2.1 Changing the APR_USER Password

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

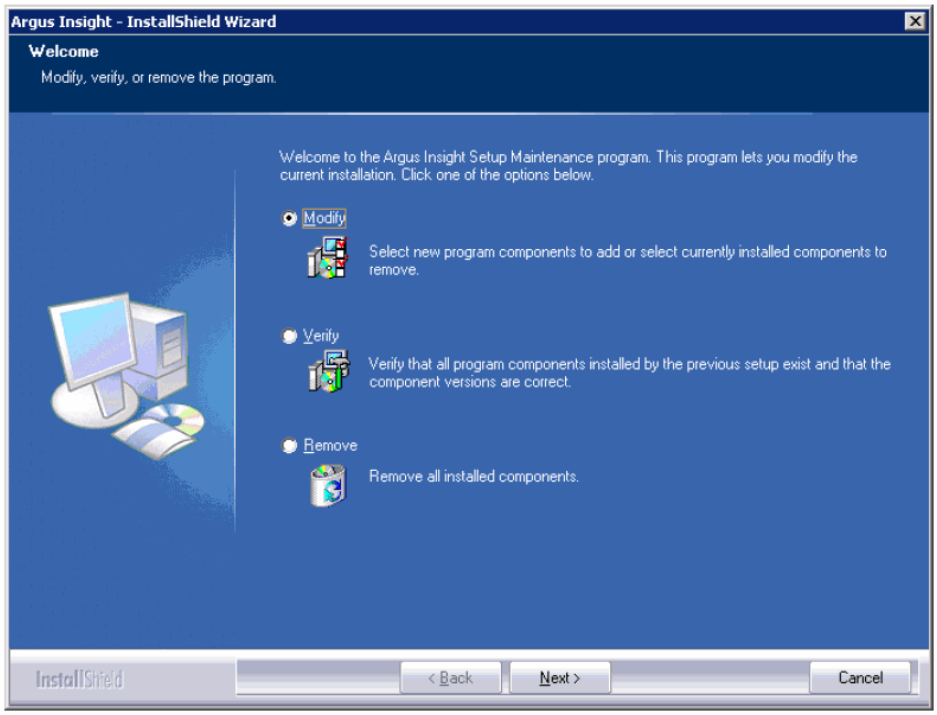
Before changing the password for the APR_USER on any Argus Insight Web Server/Cognos Server:

- 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 10 as your Business Intelligence tool.
- Update the password of APR_USER on database level. You need to update the password at the database level before you can modify the password for the Argus Insight Web Server.

You can modify the password for APR_USER on any Argus Insight Web Server/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.



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.

2.2.2 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:

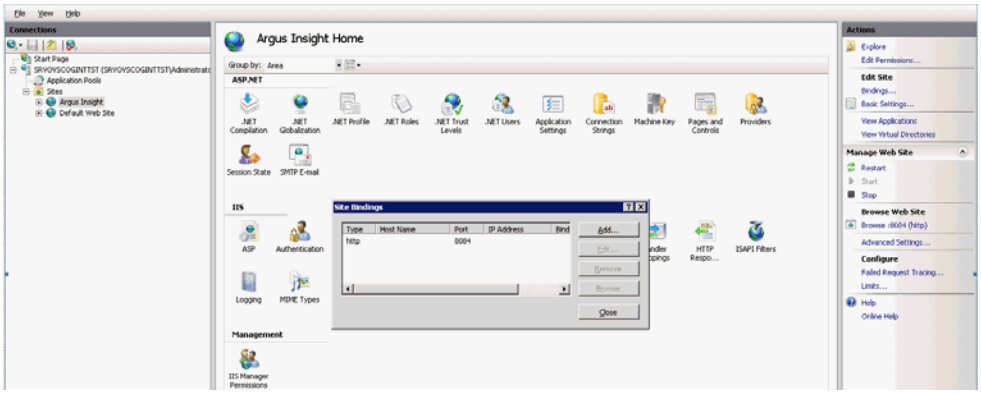
   Argus_Insight_Installation_Directory\Oracle\ArgusInsight\Bin
2. Drag and drop the adodb.dll from that location into the following folder:

   drive:\WINDOWS\assembly

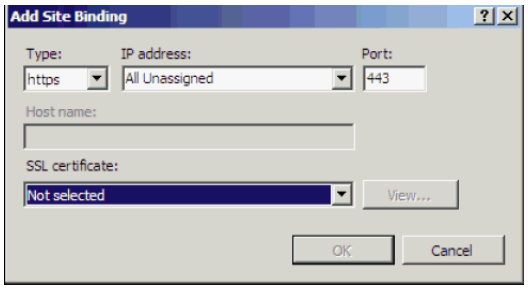
2.3 Enabling SSL Support for the Argus Insight Website

To enable SSL support for the Argus Insight website:

1. Log in to the Argus Insight Web Server.
2. Obtain and install the SSL certificate.
3. Go to IIS Manager.
4. Select **Argus Insight** and then select **Bindings.** The Site Bindings dialog box opens.



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



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 database users:

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

This chapter includes the following topics:

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

3.2.2 Database I/O Configuration

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

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

Database I/O Configuration	Total Number of Cases Small (< 30,000)	Medium (30,000 to 200,000)	Large (200,000 to 1,000,000)	Extra Large (> 1,000,000)
Number and Size of Redo Log Files	Default	3 X 500 MB	5 X 500 MB	5 X 500 MB
	The value depends on the characteristics of the I/O subsystem such as the I/O bandwidth, storage disks type, and RAID level. (Oracle recommends RAID 1+0 or similar.)			
TEMP Tablespace Size	32 GB	32 GB	64 GB	128 GB
UNDO Tablespace Size	16 GB	32 GB	64 GB	128 GB
	The recommended UNDO tablespace size is based on the projections with the following two parameter values: RETENTION=NOGUARANTEE UNDO_RETENTION=900 (seconds)			

3.2.3 Recommended Configuration for the Database Server

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

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

Database Server Configuration	Total Number of Cases 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

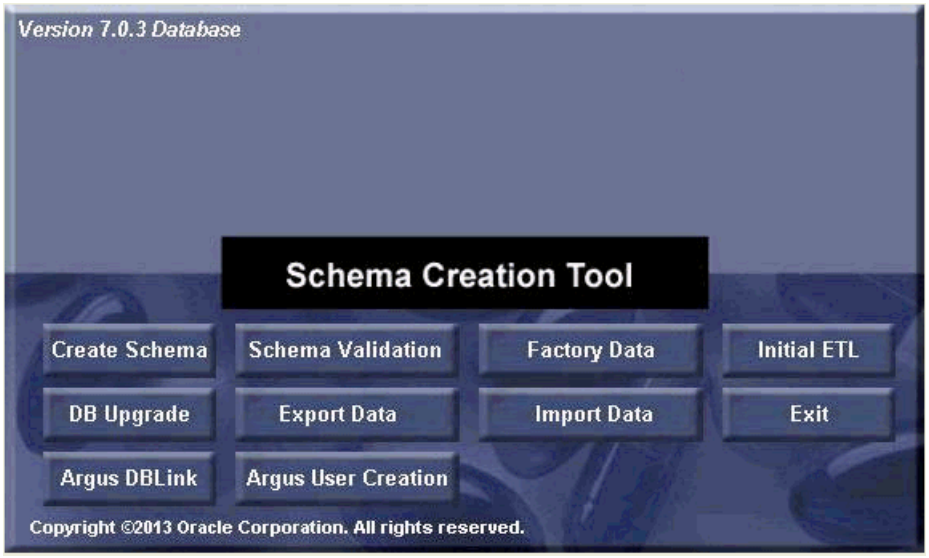
Table 3–4 (Cont.) Tablespaces Created for the Argus Insight Data Mart

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 7.0.2 database to an Argus Insight 7.0.3 database. See Section 3.8, "Upgrading Database from Argus Insight 7.0.2 to Argus Insight 7.0.3" for more information.
- **Export Data —** Exports data. For details, see Section 4.8.1, "Exporting Data" for more information.
- **Import Data —** Imports data. For details, see Section 4.8.2, "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

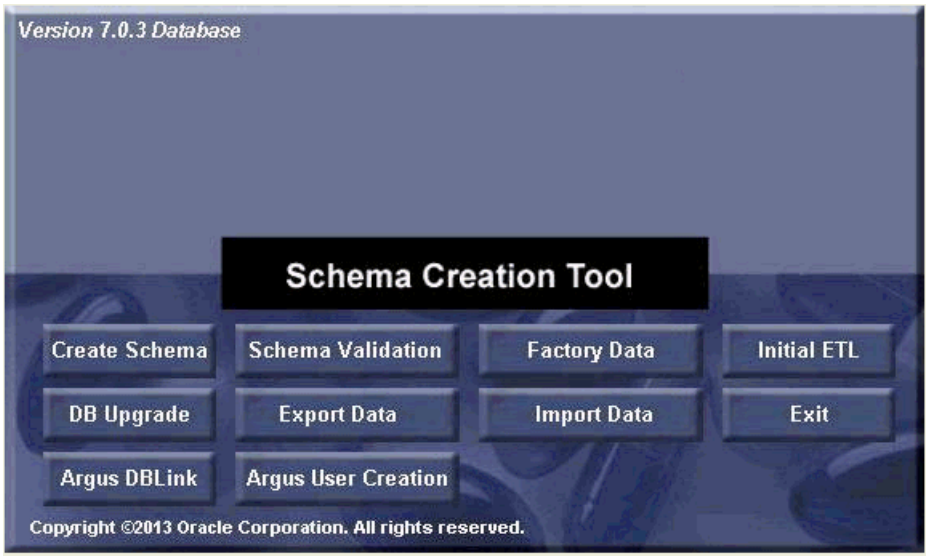
This section describes the tasks associated with creating the database schema:

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

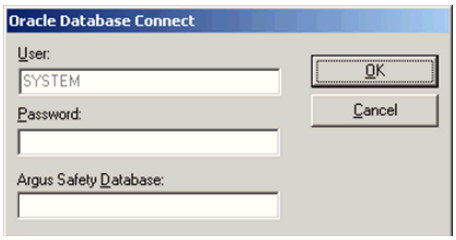
3.5.1 Creating Users and Roles in the Argus Safety Database

To create users and roles:

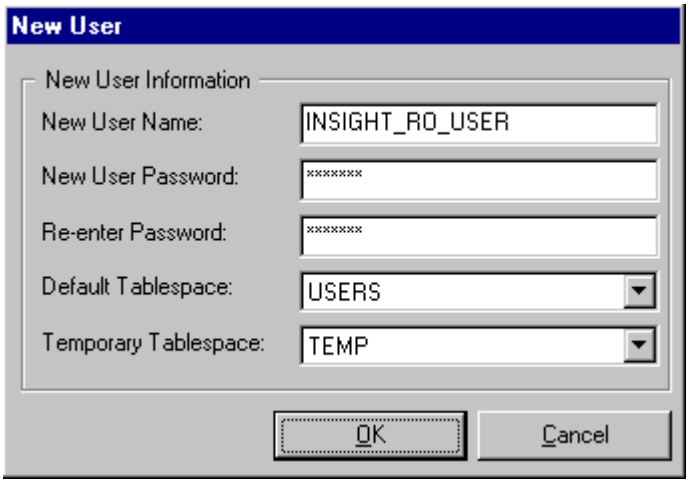
1. Start the Argus Insight Schema Creation Tool.



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



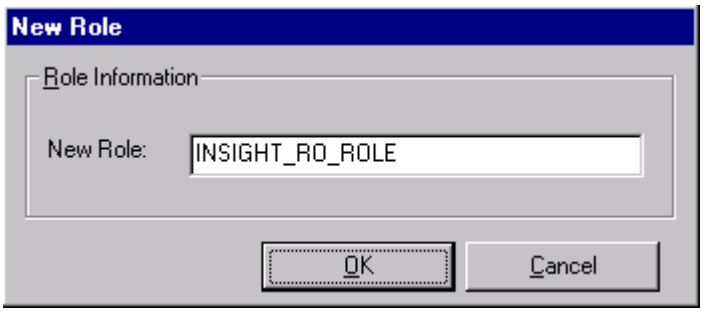
3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the SYSTEM user.
   b. In the **Argus Safety Database** field, type the name of your Argus Safety Database instance.
   c. Click **OK.** The Argus Safety Read Only User Creation dialog box opens.
4. Click **New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



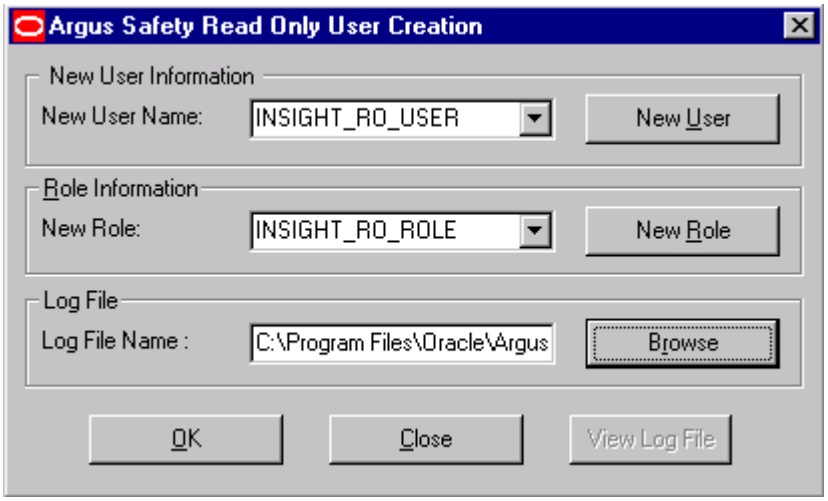
5. Complete the New User dialog box as follows:
   a. Enter a name for the new user.
   b. Specify and confirm the password for the user.
   c. Select the default and temporary tablespaces required by your corporate standards, or leave the default values.
   d. Click **OK.** The system returns to the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

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

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



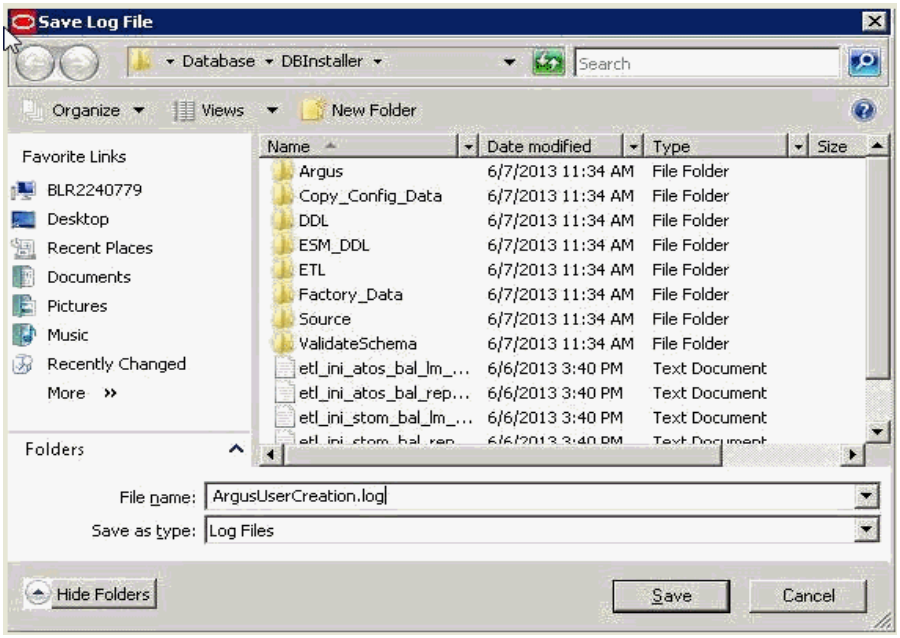
7. Enter the name of the new role to create and then click **OK.** The system returns to the Argus Safety Read Only User Creation dialog box.



Note: In case you have upgraded the database from Argus Insight 7.0.2 to 7.0.3, you can also select the existing user, which you have already created earlier, from the **New User Name** drop-down list.

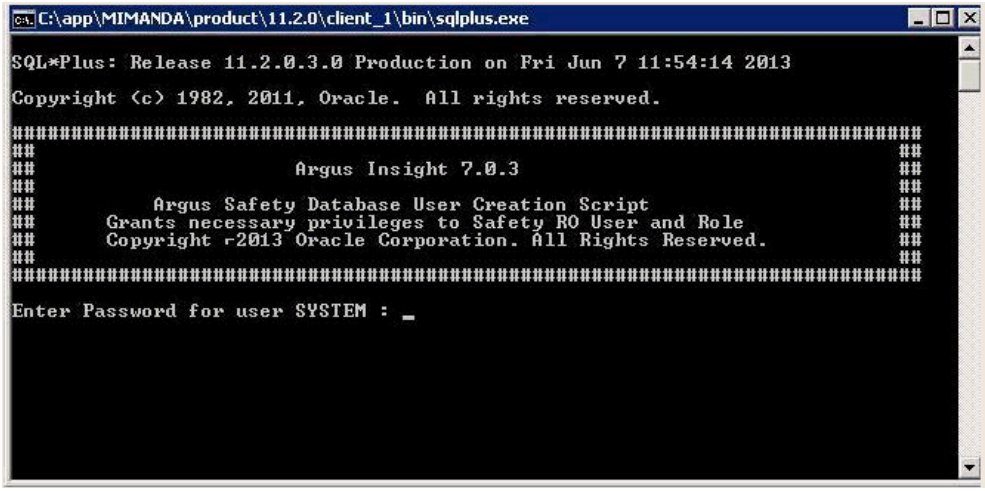
---

8. Complete the Argus Safety Read Only User Creation dialog box as follows:
   a. In the **New User Name** field, select **INSIGHT_RO_USER.**
   b. In the **New Role** field, select **INSIGHT_RO_ROLE.**
   c. In the **Log File Name** field, enter the complete path for the location and name of the log file. Alternatively, you can click **Browse** to select the location for the log file, enter the file name, and then click **Save.**

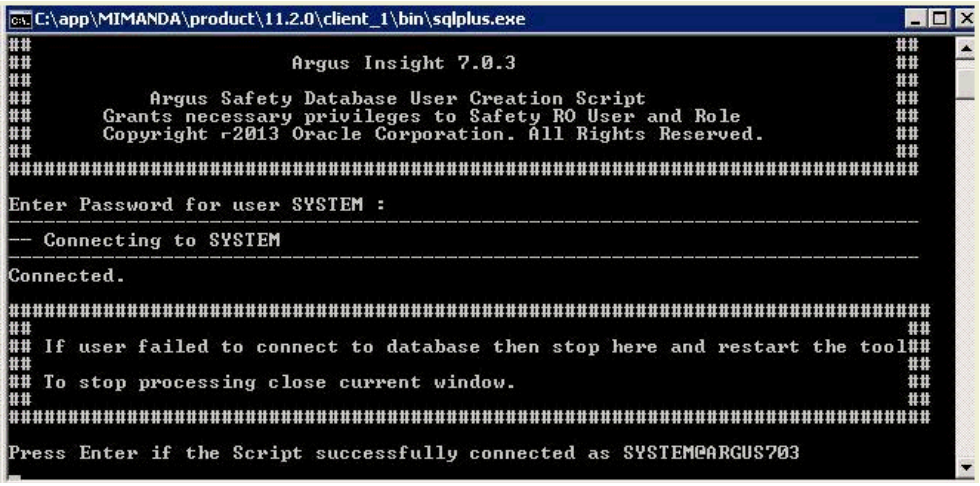


9. Click **OK** when you are ready to create the specified user with the specified role.

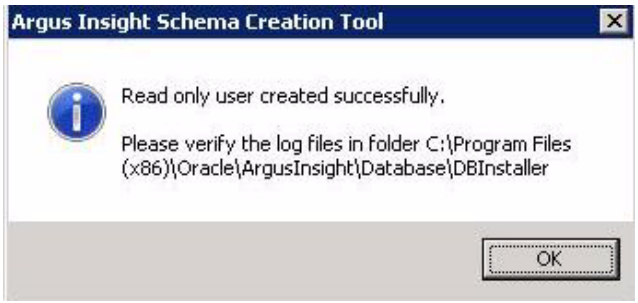
   The system displays the command prompt as shown in the following figure:



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:



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:



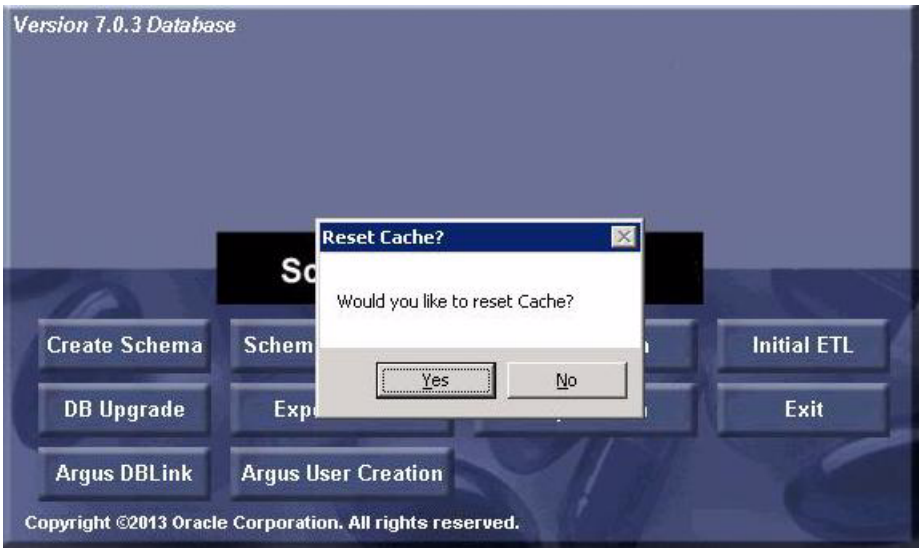
15. Click **OK** to close the message box. The system returns to the **Argus Safety Read Only User Creation** dialog box.
16. Click **View Log File.**
    a. Review the information in the log file and check for any errors.
    b. Close the log file when you are done reviewing.
17. Click **Close** to 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.

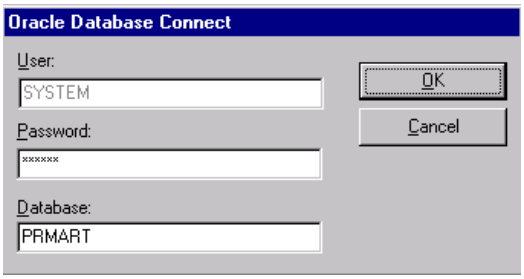
If you **do not** have remote access to SYS user, execute the **ai_sys{grant}.sql** script through SYS user. This SQL script is located in the following folder:

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

---

To create a new schema for Argus Insight:

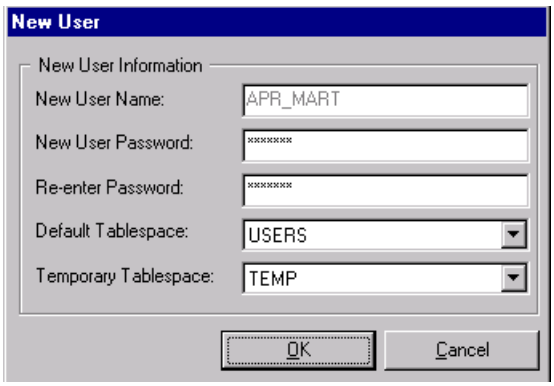
1. Start the Argus Insight Schema Creation Tool.
2. Click **Create Schema.** The **Oracle Database Connect** dialog box opens.



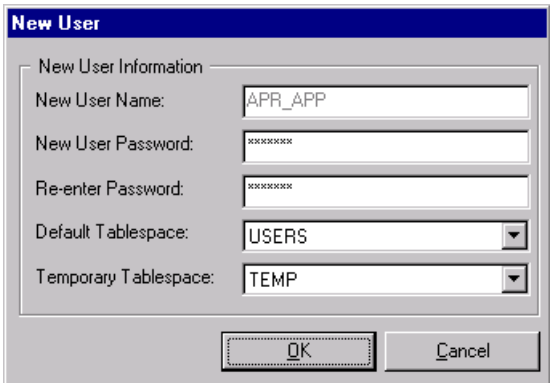
3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the SYSTEM user.
   b. In the **Database** field, type the TNS entry for the Argus Insight Database.
   c. Click **OK.**

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.



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.

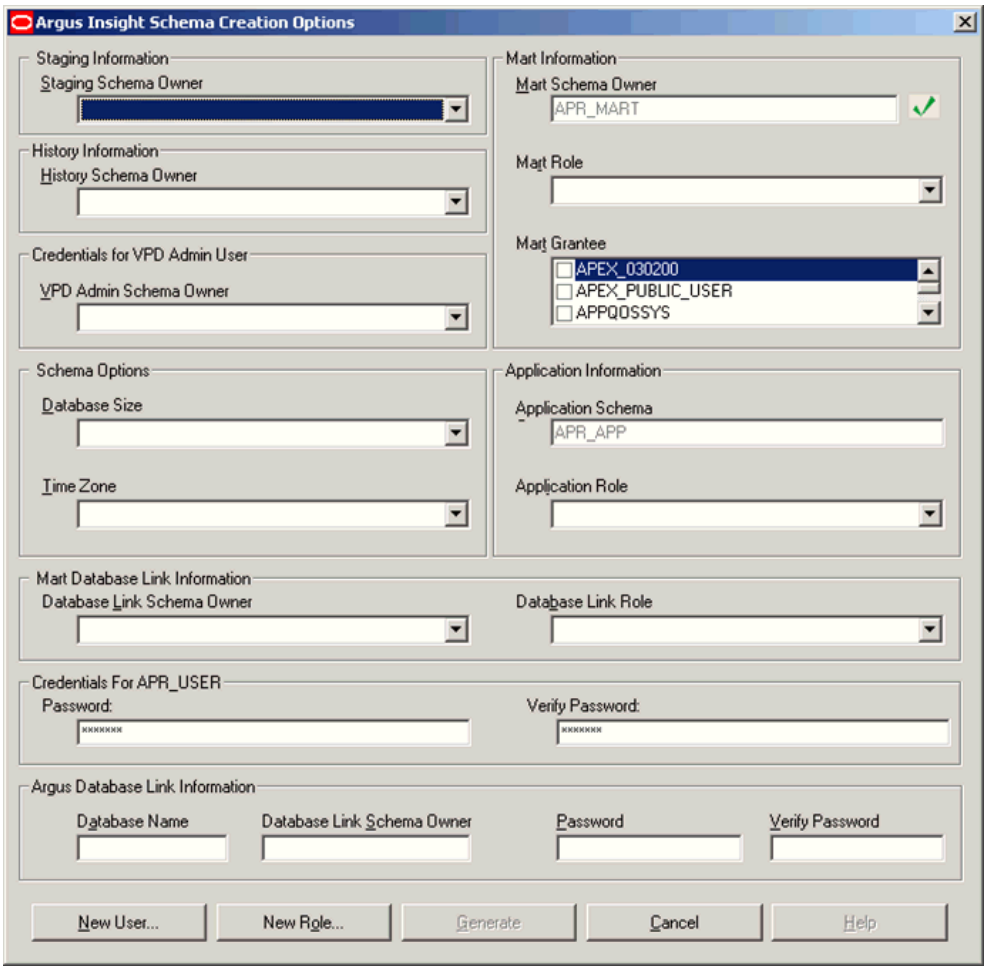


6. Enter a password for the **APR_APP** user, and then re-enter to confirm the password.

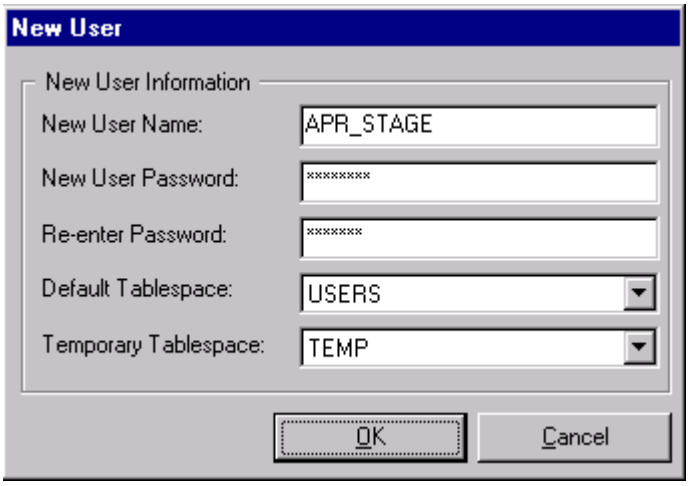
Note: Argus Insight uses the **APR_APP** user account for all application access and reporting. The password for this user is stored in encrypted form in the **CMN_PROFILE_GLOBAL** table. If you need to change this password in the future or if you forget the password, you must contact Oracle Support 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.



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



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

- APR_LINK_USER
- APR_HIST
- RLS_USER

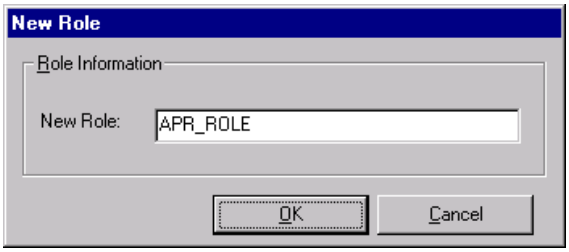
b. In the **New User Password** field, type the password for the specified user.

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 the above users.

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



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.

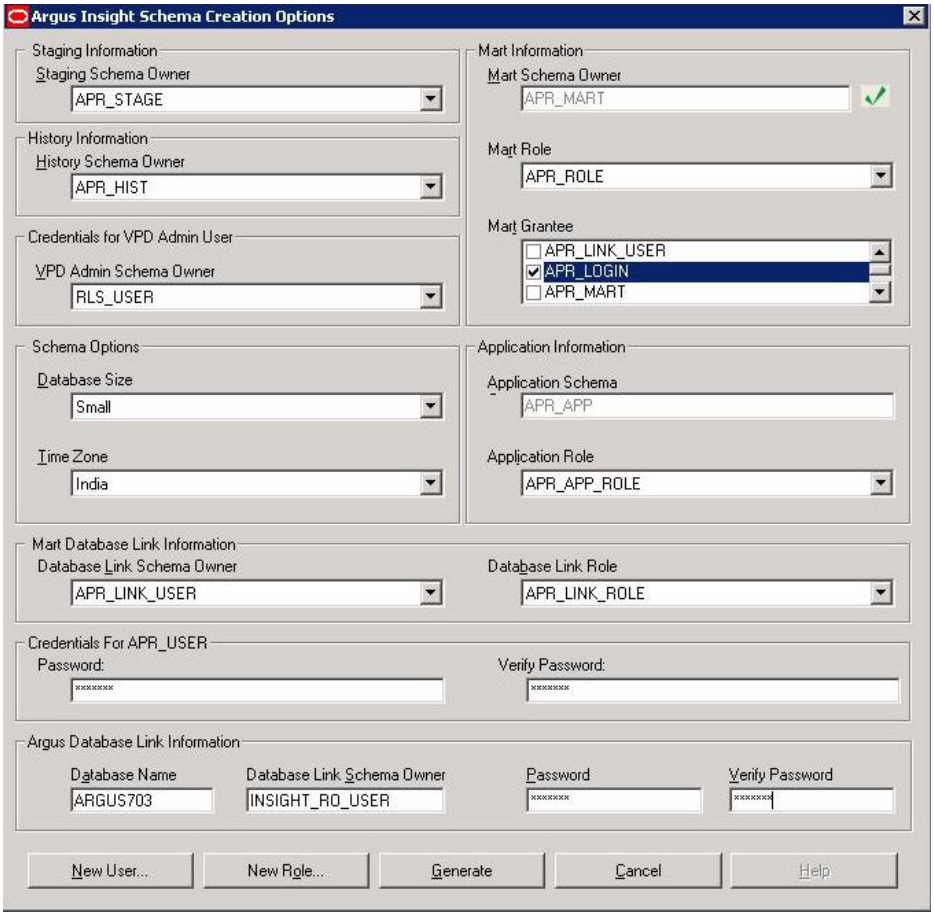
m. Enter the password for the **INSIGHT_RO_USER** in the **Password** field.

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

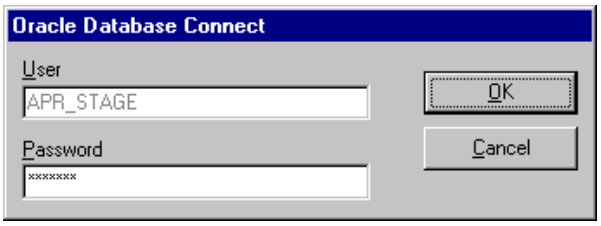
o. Optionally, in the Credentials for **APR_USER** section, enter and verify a new password only if you want to change the password for **APR_USER**.

All these inputs have been depicted in the following figure:

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

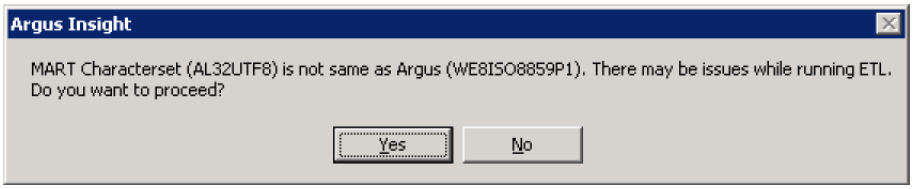


11. Click **Generate.** The system prompts for the password of the staging user (APR_STAGE user).



12. Enter the password and click **OK**. The system checks that Argus Insight and Argus Safety use the same character set. How the system continues depends on the result:

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

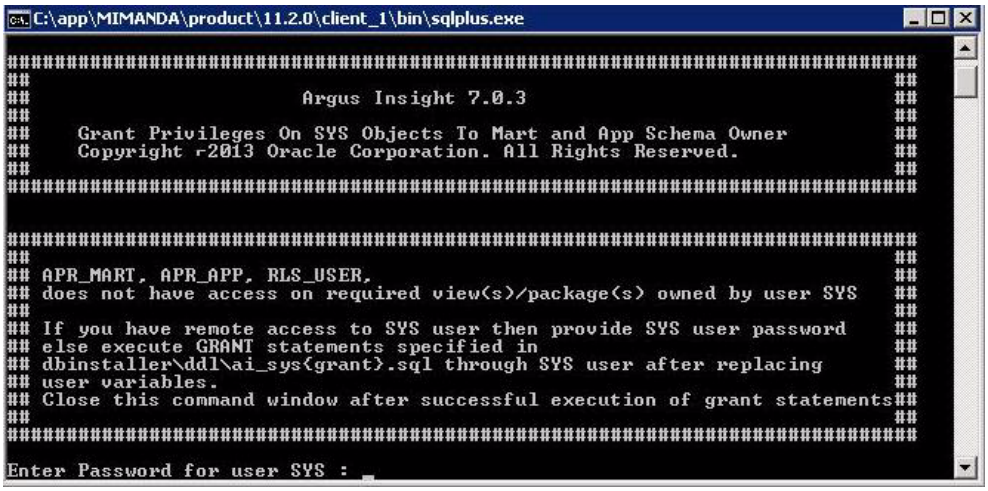


  Determine whether you want to continue with the schema creation.

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

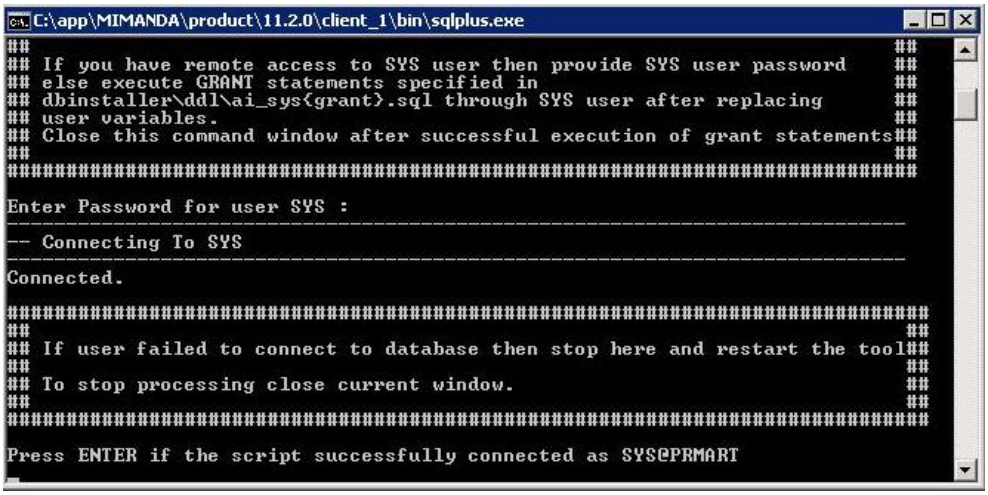
  If the Argus Safety database uses the ISO character set and the Argus Insight database uses the UTF character set, then the system can proceed by ignoring the character set difference. In this case, you can click **Yes.**

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



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:



    OR

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

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

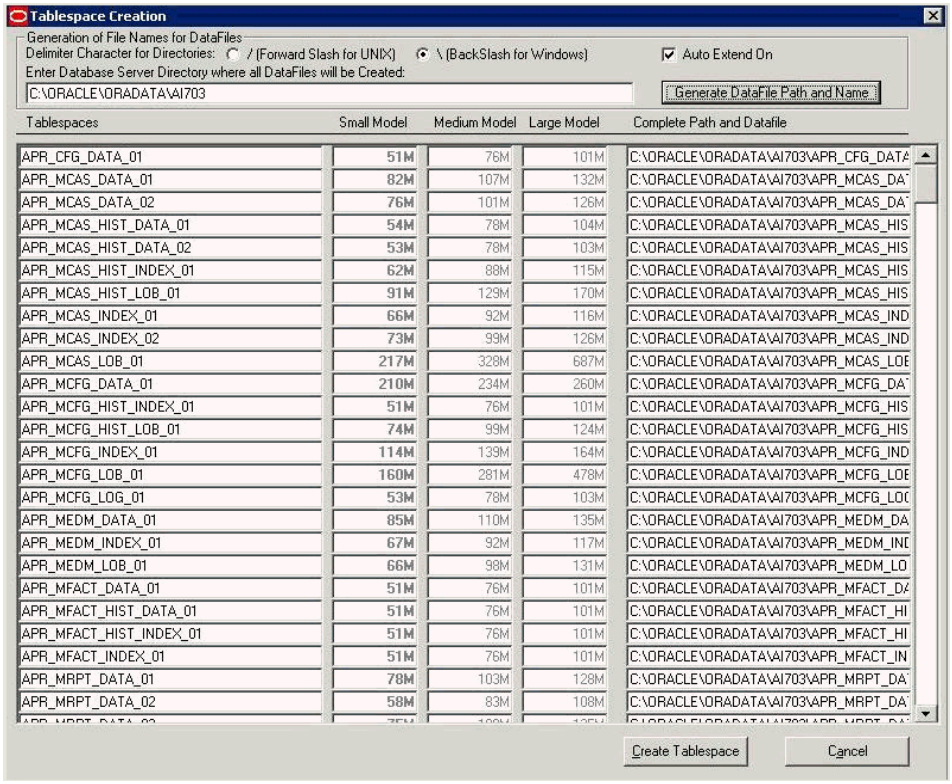
    Open the **ai_sys{grant}.sql** file from the above mentioned location.

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

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

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

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



17. Complete the Tablespace Creation screen as follows:

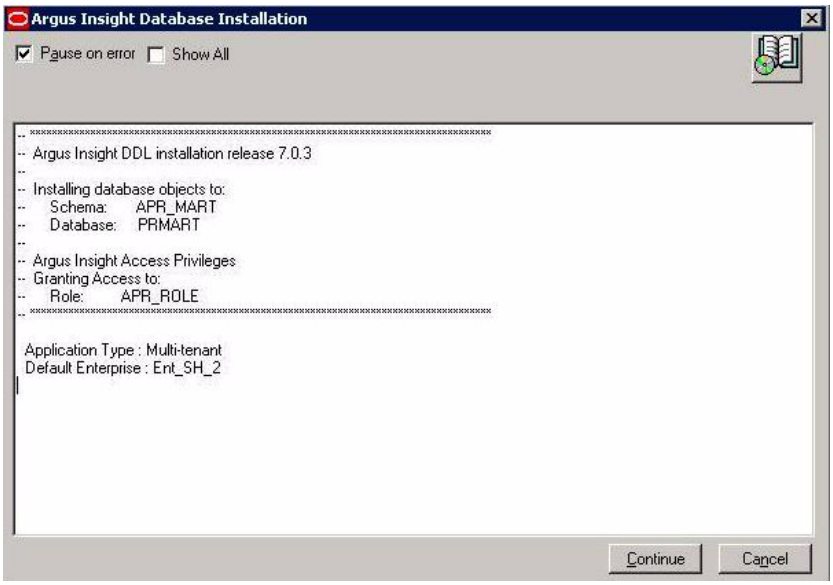
    a. In the **Enter Database Server Directory where all Data Files will be Created** field, enter the complete path to the directory for the tablespace data files that will be used by Argus Insight. For example, /u01/app/oracle/SMTEST. Note that the directory you specify must already exist.

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

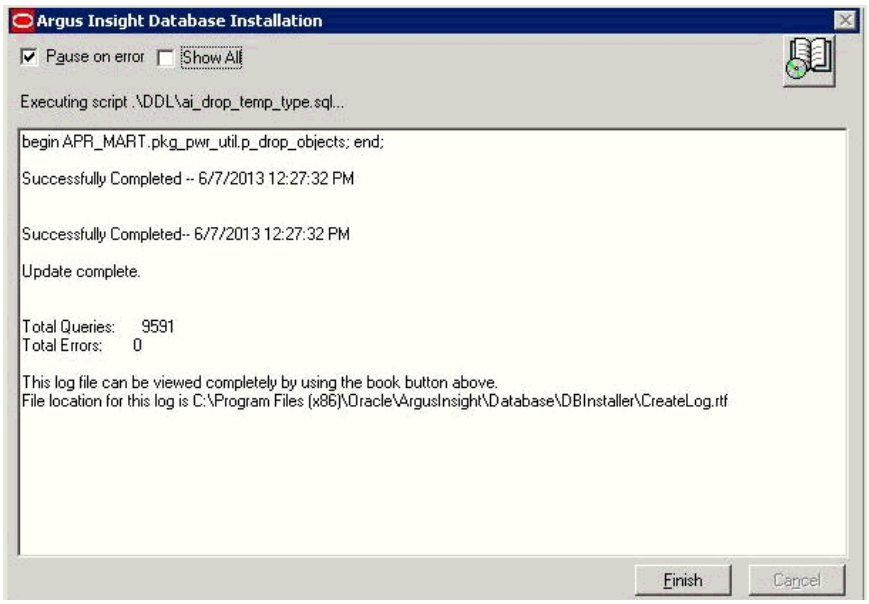
    Note that the system automatically selected the delimiter character to use for the directory path based on the Database Server operating system.

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:



20. Click **Continue** to start the schema creation. The system executes the scripts, displays status information during the schema creation process, and reports when the update is completed.



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

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

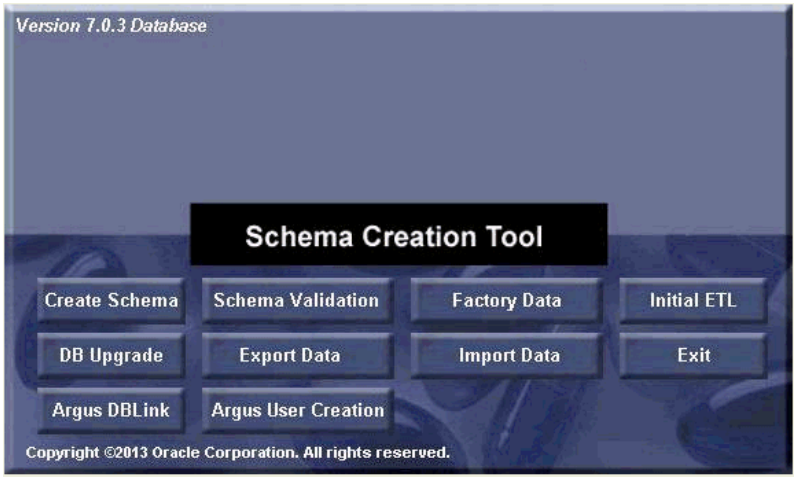
    drive:\Argus_Insight_Working\AI703\Database\DBInstaller\CreateLog.rtf

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

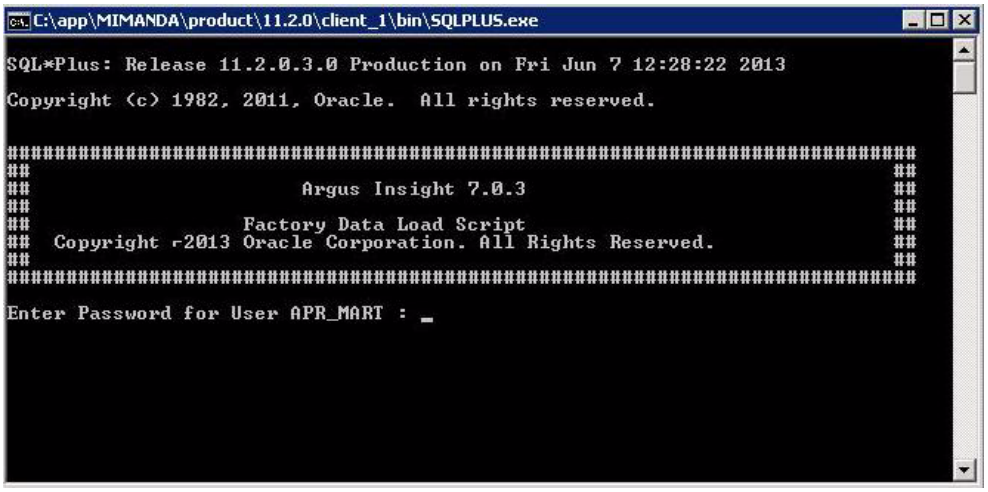
3.5.4 Loading Factory Data

To load the factory data:

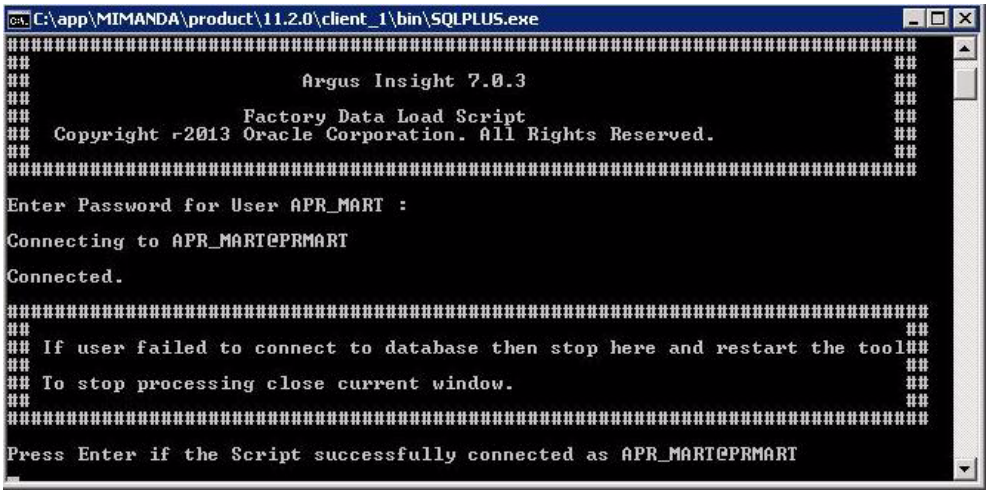
1. Start the Argus Insight Schema Creation Tool.



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



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



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**.

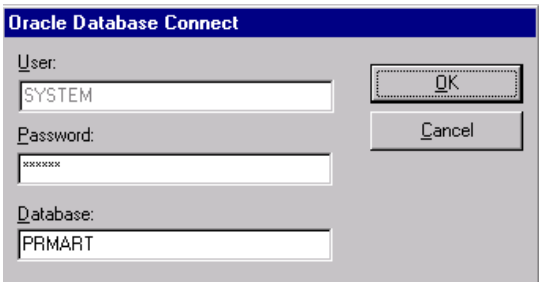
5. Press **Enter** again. Argus Insight displays the following message when it finishes loading the factory data:

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

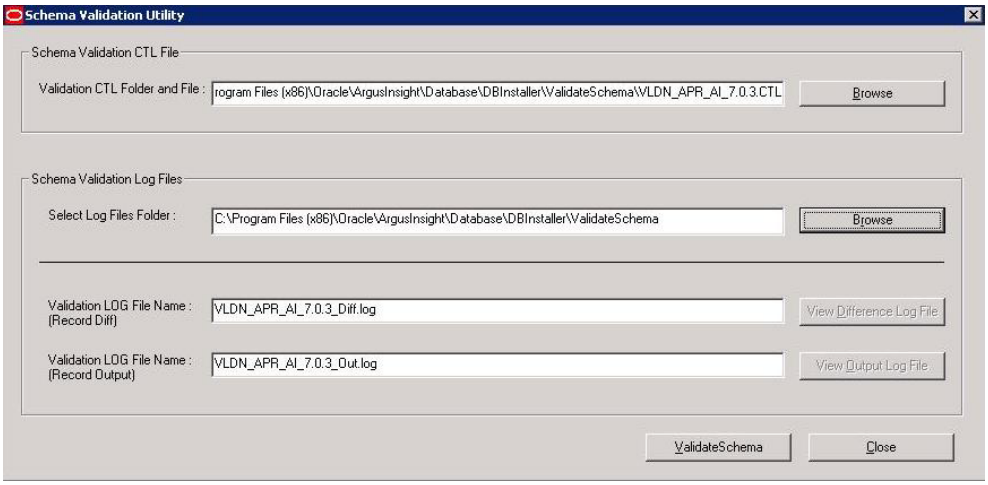
3.6 Validating the Schema

To validate the database schema:

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



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.



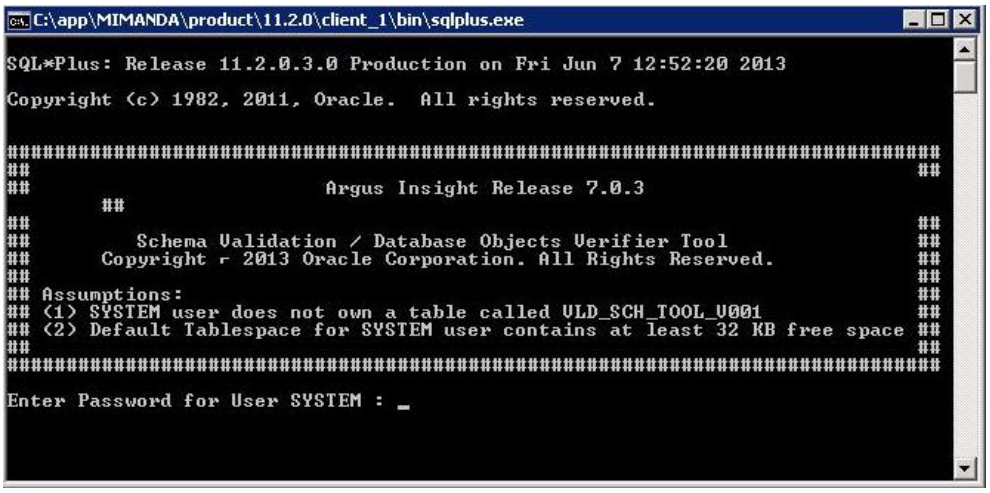
4. Complete the Schema Validation Utility dialog box as follows:

   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.

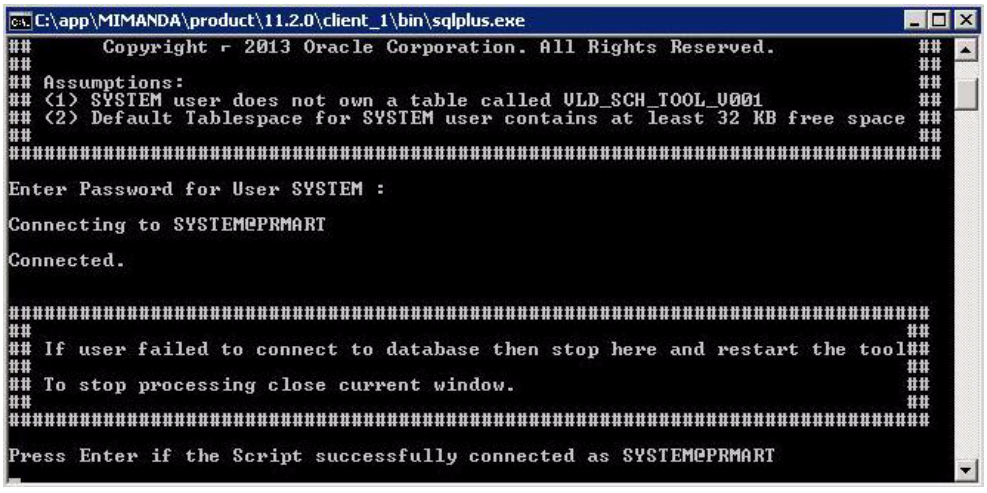
   b. For the **Select Log Files Folder** field, click **Browse** next to the field to navigate to and select the log files folder. Click **OK** to close the Select Folder dialog box and return to the Schema Validation Utility dialog box.

   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.

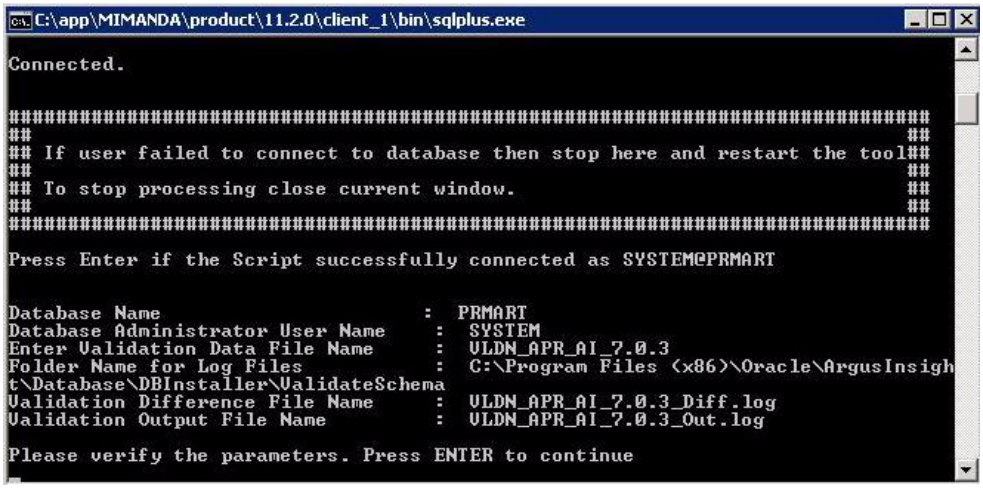
5. Click **Validate Schema.** This displays the following command screen:



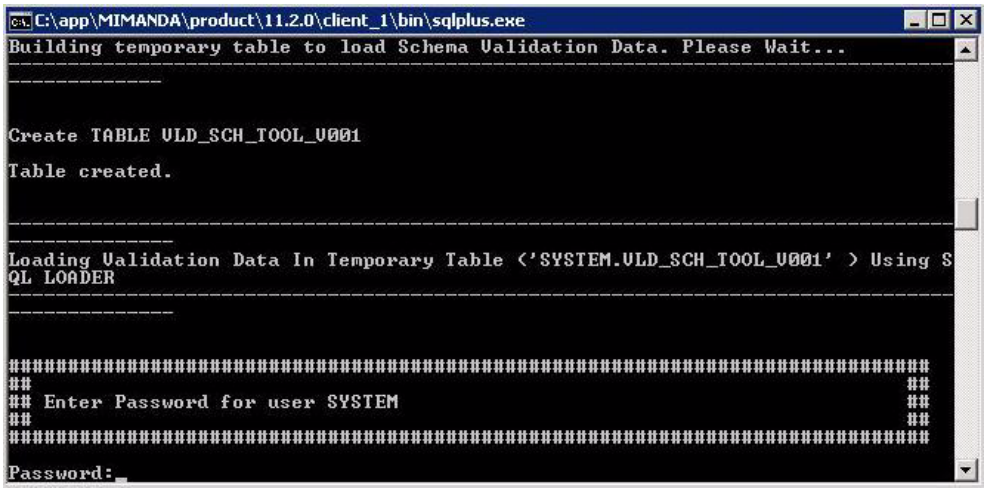
6. Enter the password for the **SYSTEM** user and press **Enter**. This displays the following command screen:



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:

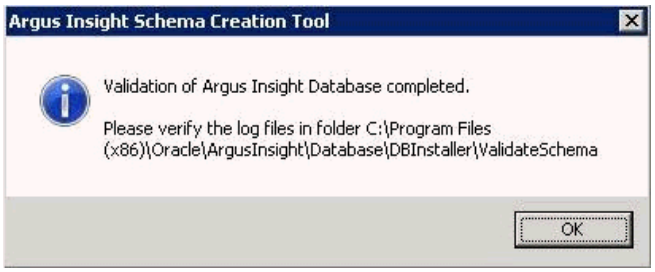


8. Review the information on the command screen and press **Enter.** This displays the following command screen:



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:



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.

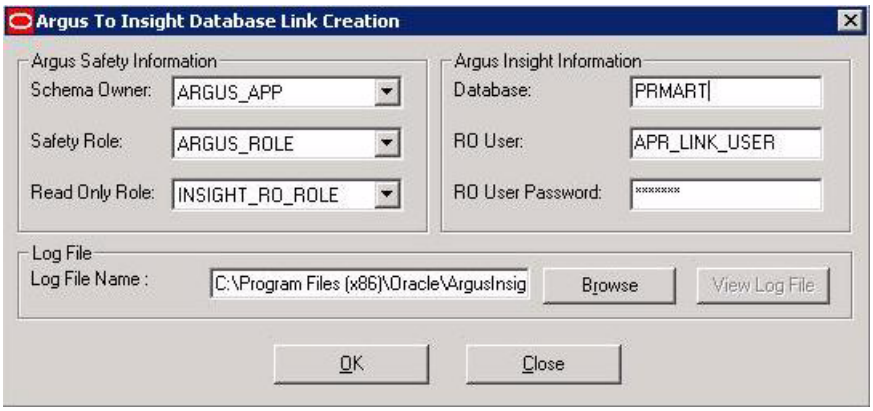
3.7 Creating a Database Link from Argus Safety to Insight Database

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:

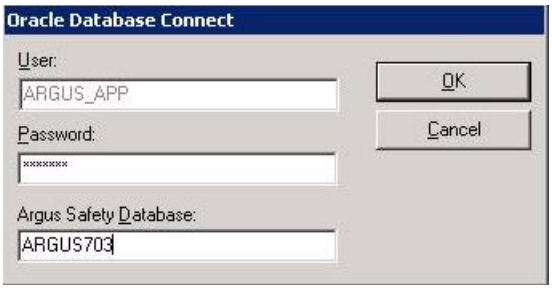
1. Start the Argus Insight Schema Creation Tool.
2. Click **Argus DBLink.**
3. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the SYSTEM user.
   b. In the **Argus Safety Database** field, type the name of your Argus Safety database.
   c. Click **OK.**

   The Argus To Insight Database Link Creation dialog box opens.



4. Complete the fields in the Argus Safety Information section as follows:
   a. In the **Schema Owner** field, select the user account that owns the Argus Safety schema.
   b. In the **Safety Role** field, select the Argus Safety role.
   c. In the **Read Only Role** field, select the **INSIGHT_RO_ROLE,** which was created in Argus Safety.
5. Complete the fields in the Argus Insight Information section as follows:
   a. In the **Database** field, enter the name of the Argus Insight database.
   b. In the **RO User** field, enter the name of the read-only user. See step 8 (a) of the Section 3.5, "Creating the Database Schema" section (**APR_LINK_USER**).
   c. In the **RO User Password** field, enter the password for the read-only user.
6. Click the **Log File Name** field to specify the name of the log file that will store the DBLink creation information. You 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.

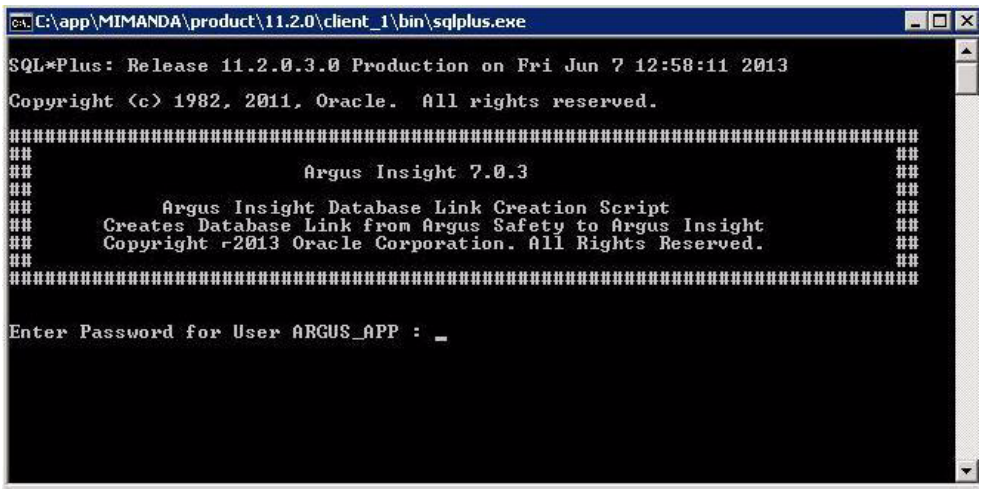


8. Enter the **ARGUS_APP** password and the Argus Safety database information. Click **OK.**

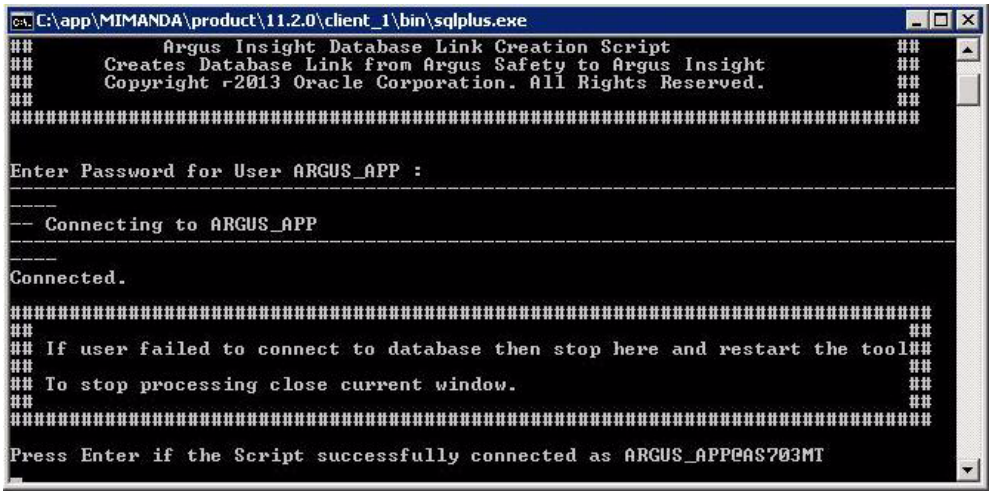
   The system then prompts for the information to connect to the database as the SYSTEM user.

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

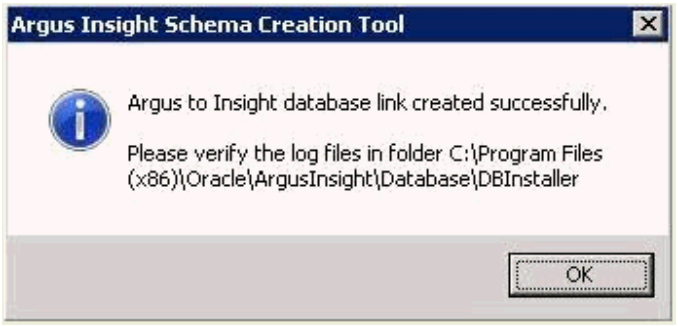
   The system displays the following screen:



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



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:



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.

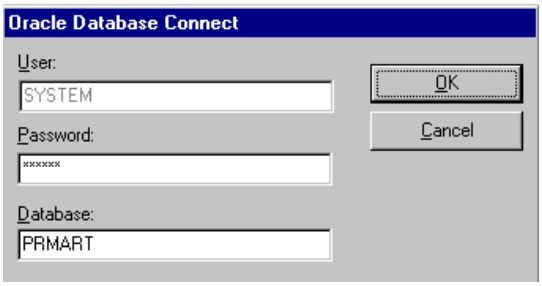
3.8 Upgrading Database from Argus Insight 7.0.2 to Argus Insight 7.0.3

Note: The Argus Insight upgrade process will delete the entire Cognos/BusinessObjects Report Scheduling information from the Argus Insight database. If you intend to retain this information, you must ensure that before starting the upgrade process, you have taken a back-up of this information.

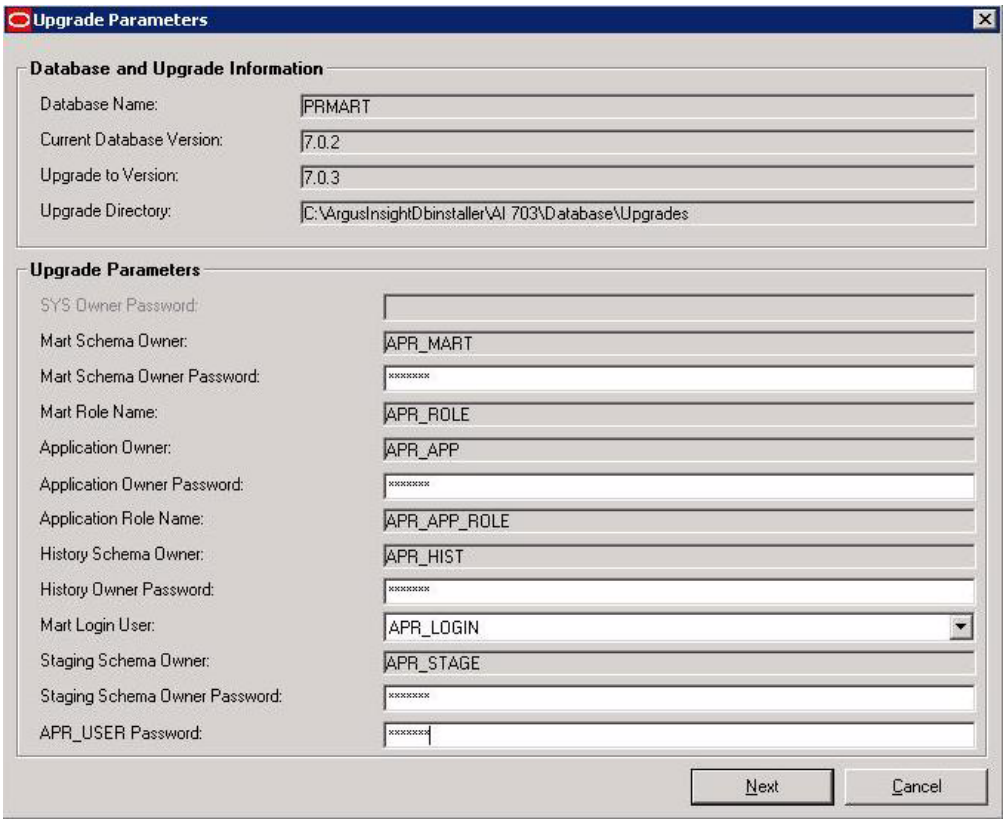
The scheduling information of CIOMS, CIOMS II Line listing and Medwatch reports will still be available after the upgrade process.

To upgrade the database from Argus Insight 7.0.2 to Argus Insight 7.0.3:

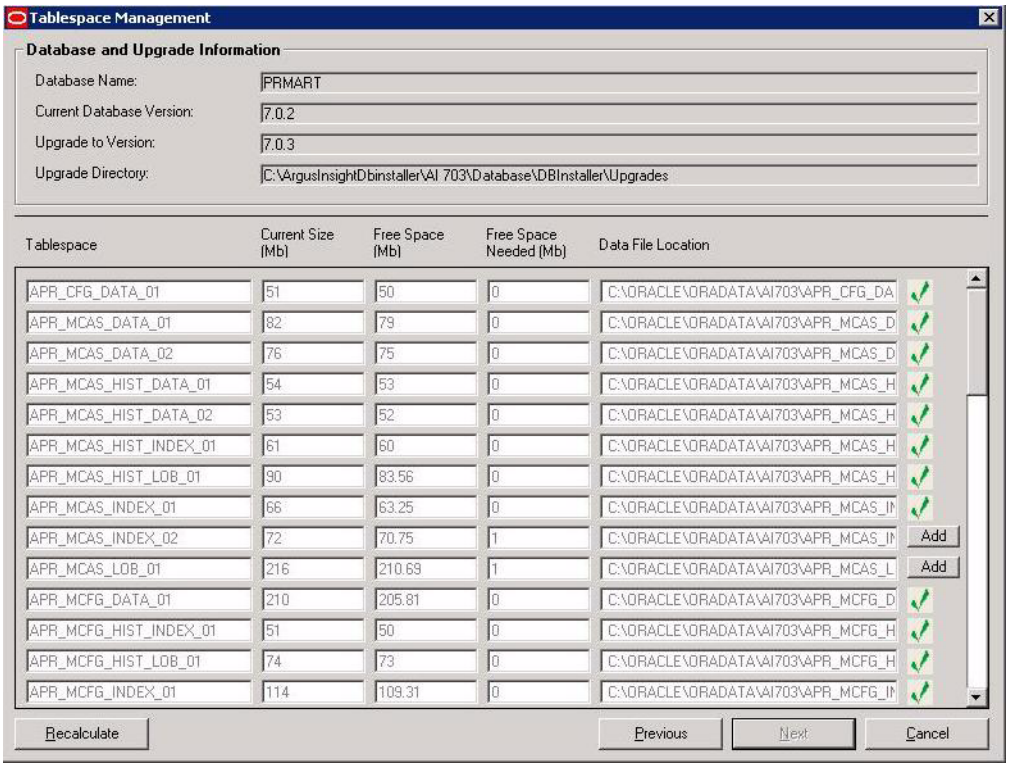
1. Start the Argus Insight Schema Creation Tool.
2. Click **DB Upgrade.** The Oracle Database Connect dialog box opens.



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.



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.



6. Verify that all tablespaces have enough free space.

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

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

   - Click **Add** to add a new datafile to the existing tablespace.

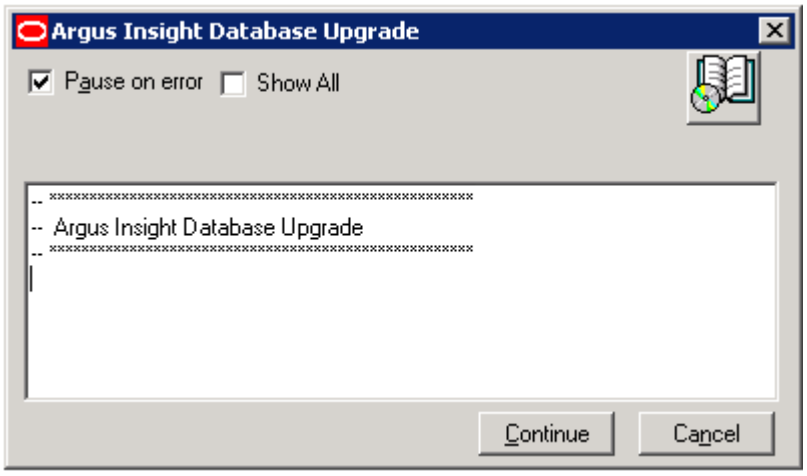
     You will be prompted to add a name for the new datafile, containing the required additional space.

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

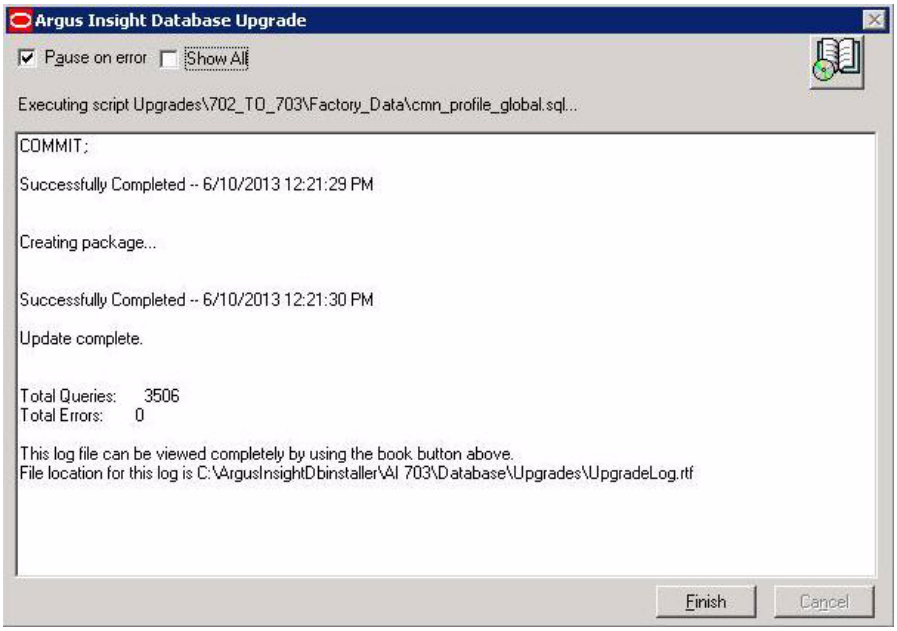
     After resizing, click the **Recalculate** button to re-evaluate the tablespace size and refresh the tablespace grid, as per the updated tablespace size.

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

7. Click **Next.**



8. Click **Continue** to start the upgrade process. During the upgrade process, the system loads the factory data, and then displays a message reminding you to check the Factory_Data folder for any .BAD files.
9. Click **OK** to continue. The system executes the upgrade scripts, displays status information during the update, and reports when the update is completed.



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

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

    drive:\Program Files\Oracle\ArgusInsight\Database\Upgrades\UpgradeLog.rtf
11. Click **Finish** to close the dialog box.
12. Once you have upgraded the database from Argus Insight 7.0.2 to Argus Insight 7.0.3, 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:

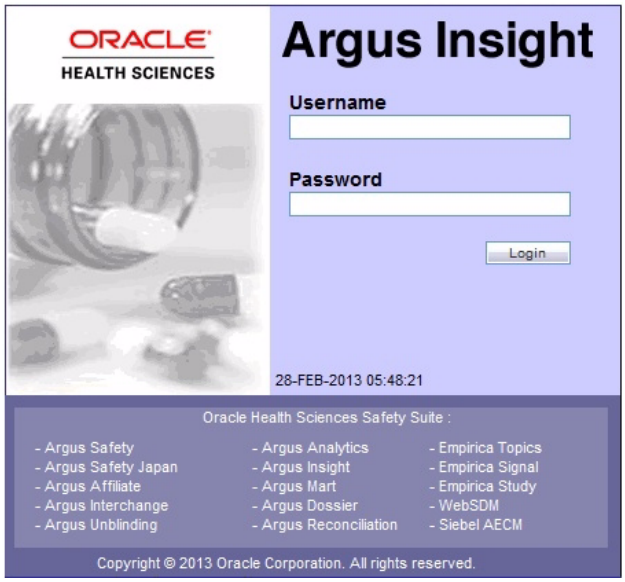
4.1 Logging In to Argus Insight for Configuration and Setup

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:

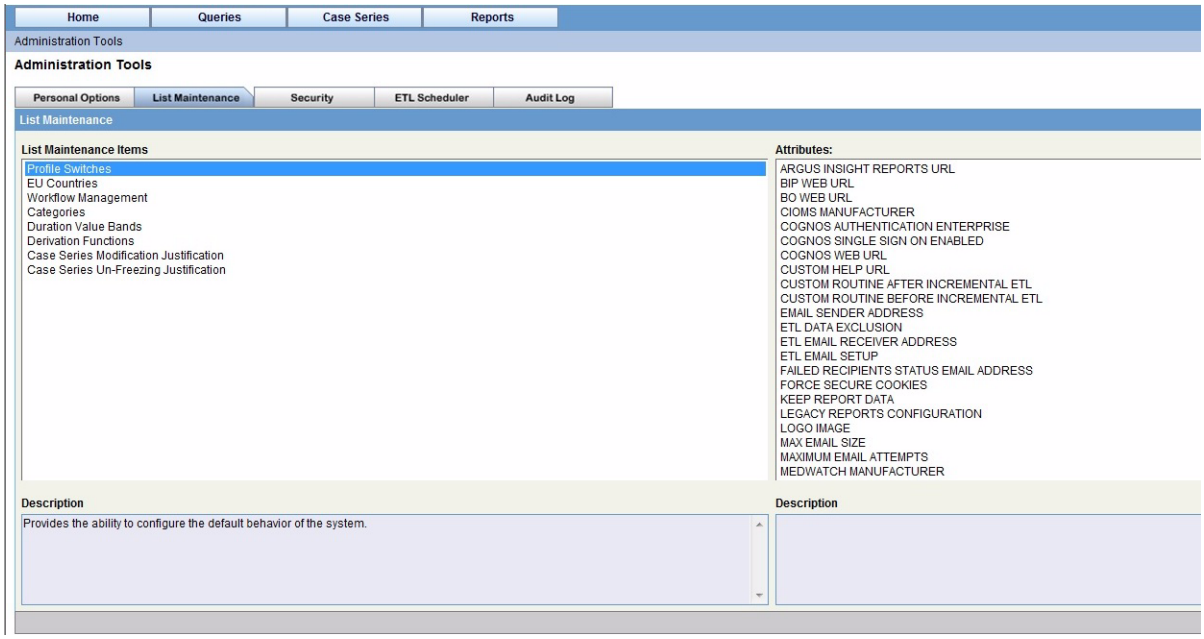
- *Oracle Argus Insight CMN Profile Enterprise Table Guide* (CMN_PROFILE_ENTERPRISE.pdf)
- *Oracle Argus Insight CMN Profile Global Table Guide* (CMN_PROFILE_GLOBAL.pdf)

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.

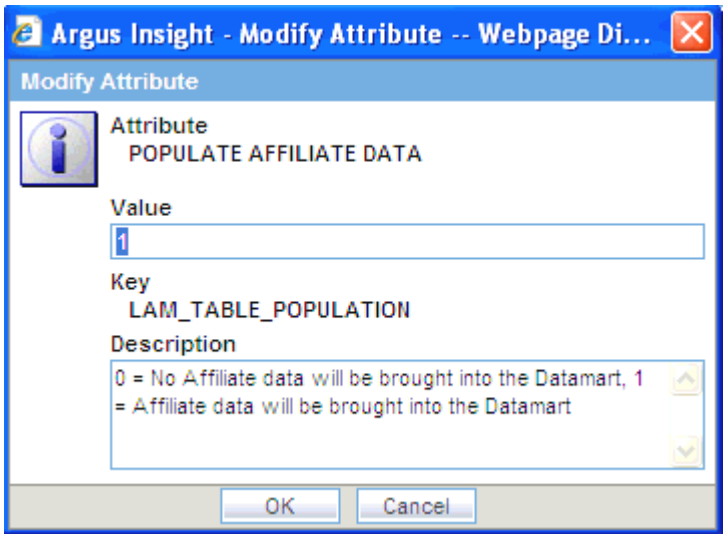
Figure 4–1 List Maintenance Tab with the Profile Switches



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:



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

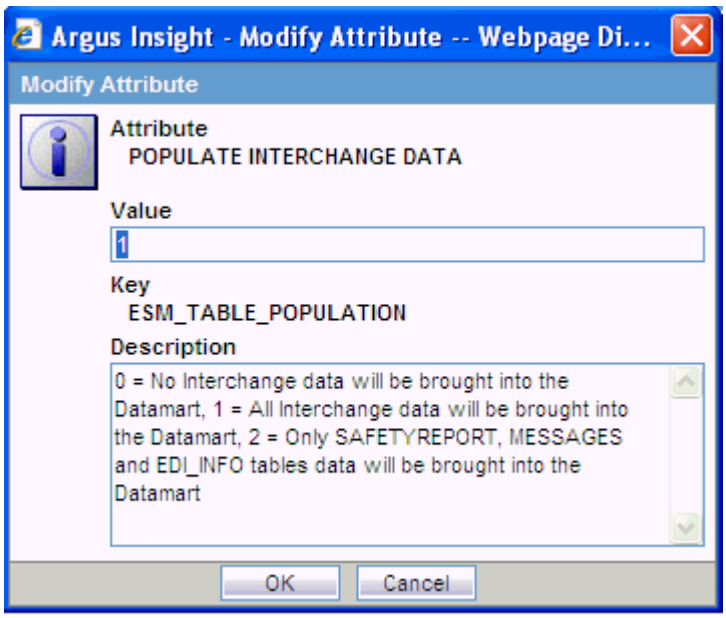
0 = Do not bring any affiliate data into the data mart.

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:



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

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

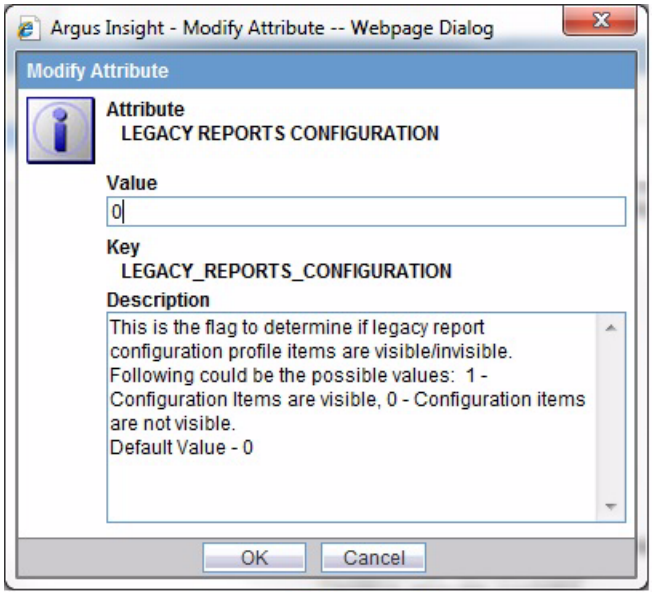
1 = Bring all interchange data into the data mart.

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 **LEGACY REPORTS CONFIGURATION** from the Attributes group. Argus Insight uses this attribute to determine if Legacy Report Configuration profile items are visible/invisible.

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



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

      1 = Configuration items are visible

      0 = Configuration items are not visible

Note: If Legacy Reports Configuration switch is set to 1, then legacy reports switches becomes available for obsolete reports, and you must configure the following switches:

- POPULATE NARRATIVE LANGUAGES TABLE
- COMPANY LOGO PATH
- DAYS TO LOCK
- UDN COLUMN FOR SUPPLIER NAME
- FOLLOW-UP ACTION CODE
- POPULATE DLL SLL REPORTS TABLE DATA

To configure these switches, refer to Argus Insight 7.0.2 Installation Guide.

---

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

4.2.3 Setting the Email Attributes

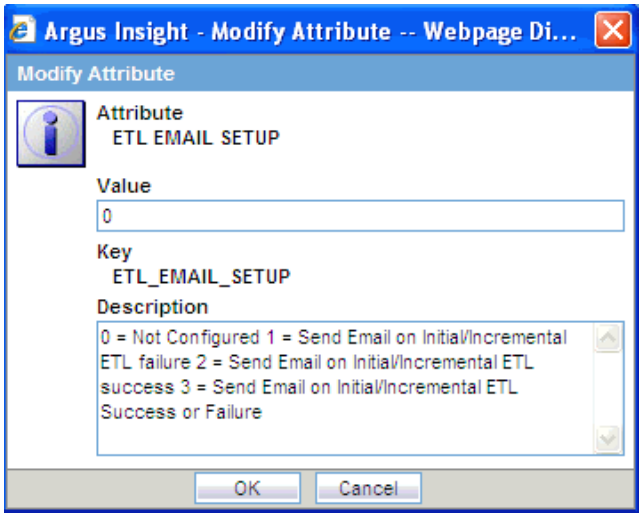
The following attributes relate to sending and receiving email after an extract, transform, and load (ETL) operation has completed, as well as sending email for scheduled reports.

- 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:



   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.

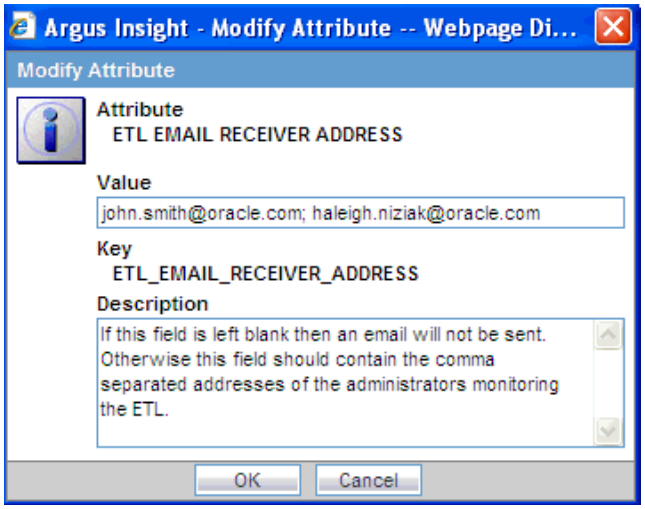
      2 = Send an email message only if an initial or incremental ETL succeeds.

      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:



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.

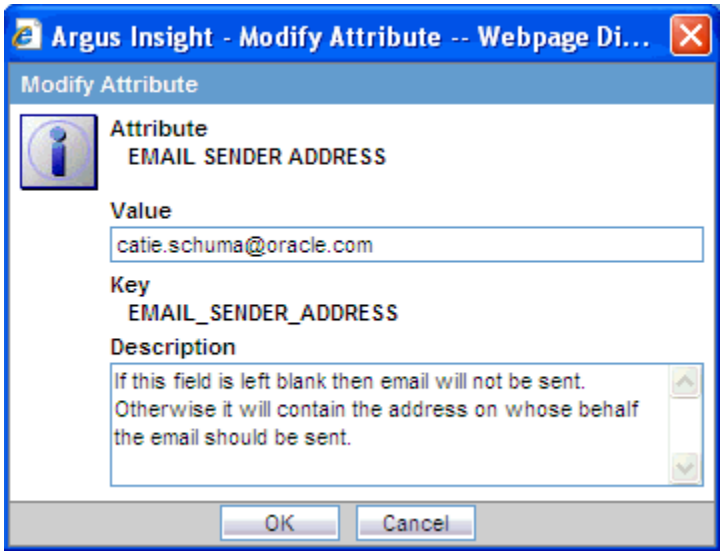
If you leave the Value field blank, then Argus Insight sends no email messages.

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:



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

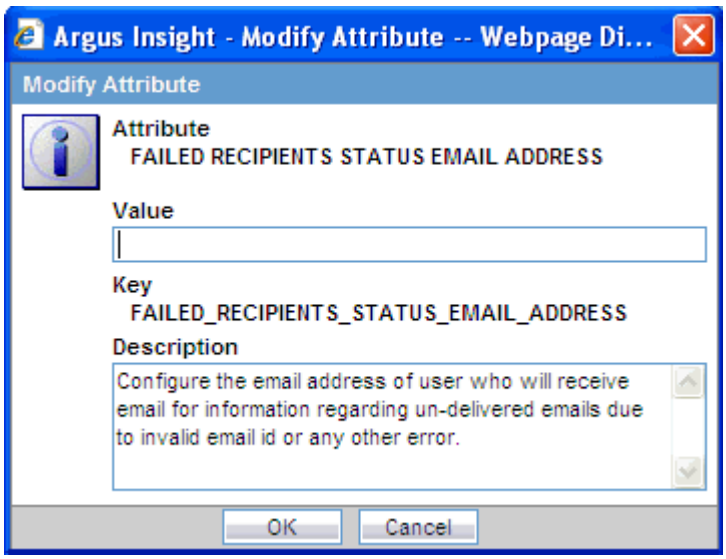
If you leave the Value field blank, then Argus Insight sends no email messages.

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:



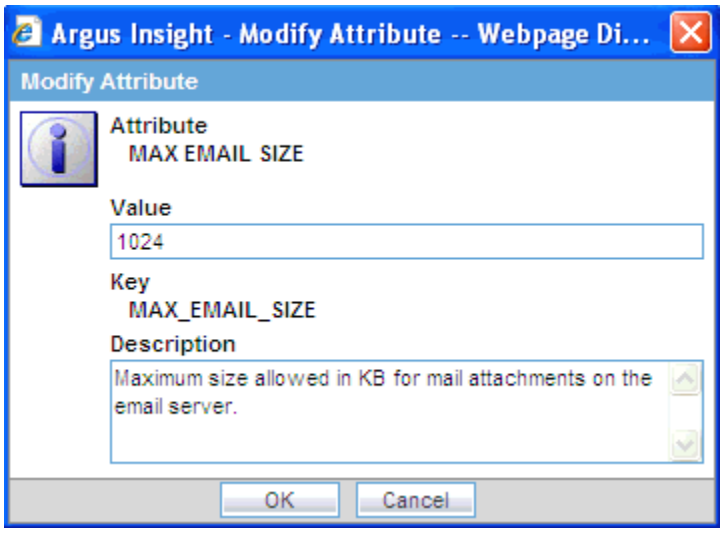
c. Click the **Value** field, and enter the email address of the user who will receive information about undeliverable emails.

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:



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.

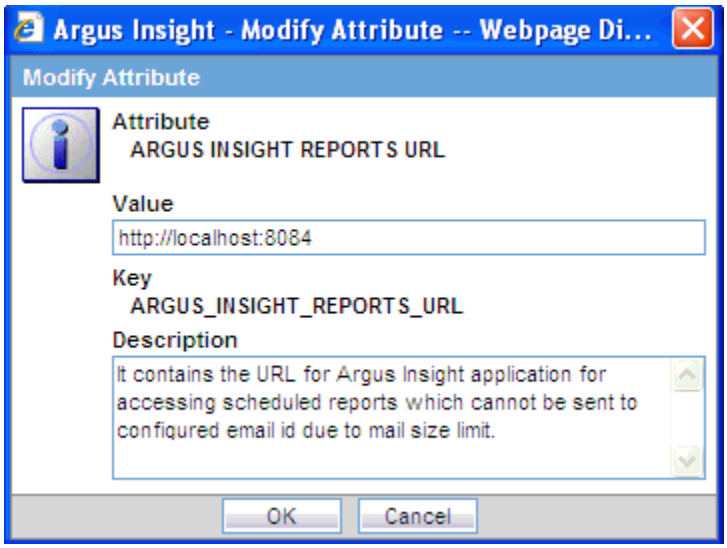
d. Click **OK** to save your changes and return to the List Maintenance tab.

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:



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

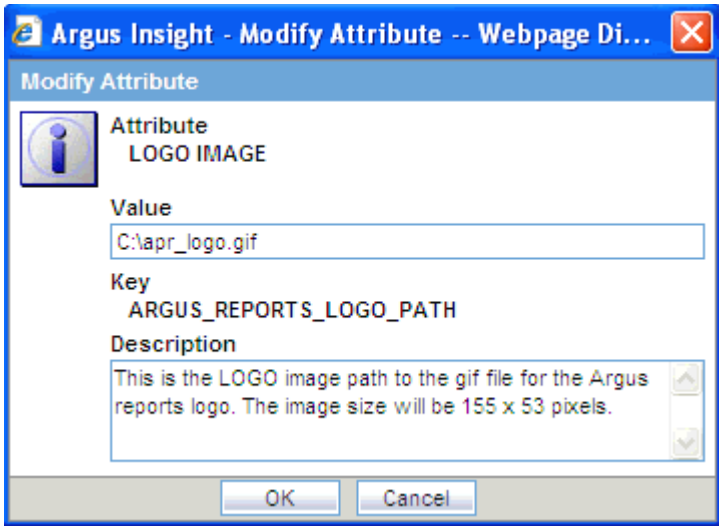
  — US FDA MedWatch 3500A report

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

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:



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.

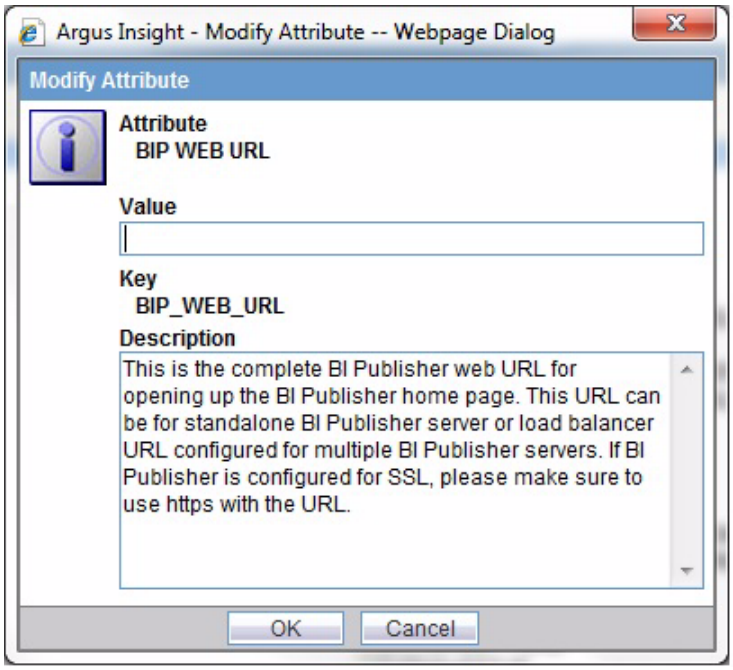
4.2.6 Setting the Attributes Specific ONLY to BIP

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

- BIP WEB URL
- KEEP REPORT DATA

To define the attributes required for BIP, 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 WEB URL** from the Attributes group.
   a. Click **Modify.** The following Modify Attribute dialog box opens:



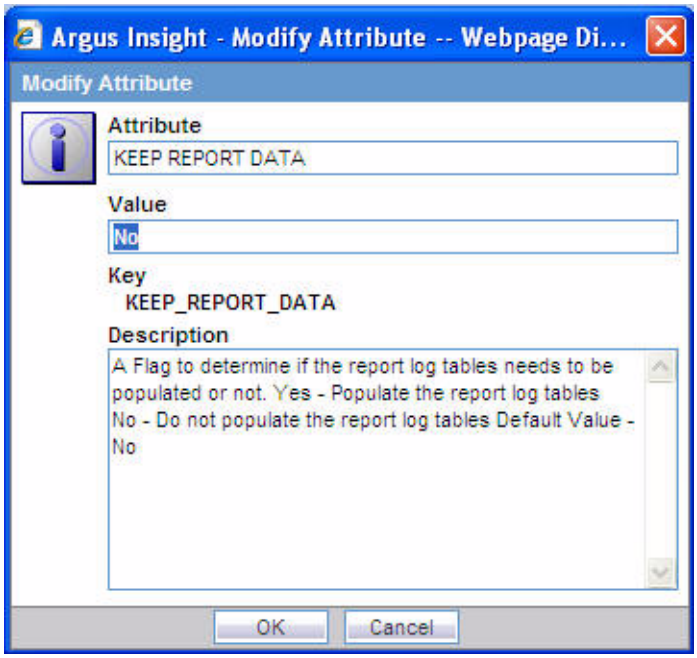
b. Click the **Value** field, and enter the name of the BIP Web URL to open the BIP Home Page. This URL can be the BI Publisher URL for standalone BI Publisher server or the Load Balancer URL configured for multiple BI Publisher servers. If BI Publisher is configured for SSL, you must use https with the URL. For example:

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

c. Click **OK** to save 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:



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.

4.2.7 Setting the Attributes Specific ONLY to BusinessObjects

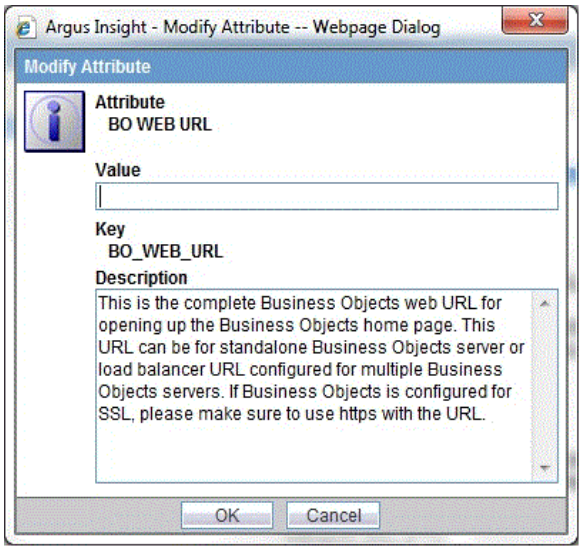
If you are using BusinessObjects as your Business Intelligence tool with Argus Insight, you need to complete the following tasks to define those attributes that are required for **BusinessObjects configurations only**:

- Setting the Attributes for the BusinessObjects Servers

4.2.7.1 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 Web URL that Argus Insight uses:
   a. Select **BO WEB URL** from the Attributes group.
   b. Click **Modify.**



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 BusinessObjects Home page. These problems may be caused due to the session interference of Argus Insight and BusinessObjects web application.

---

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

4.2.8 Setting the Attributes Specific ONLY to Cognos

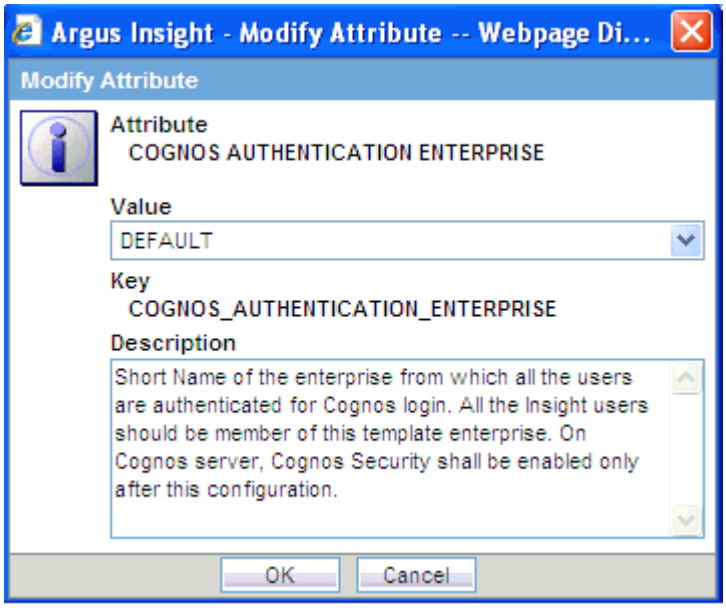
If you are using Cognos as your Business Intelligence tool with Argus Insight, you need to set the following Cognos-specific attributes:

- COGNOS AUTHENTICATION ENTERPRISE
- COGNOS WEB URL
- POPULATE DLL SLL REPORTS TABLE DATA
- COGNOS SINGLE SIGN ON ENABLED

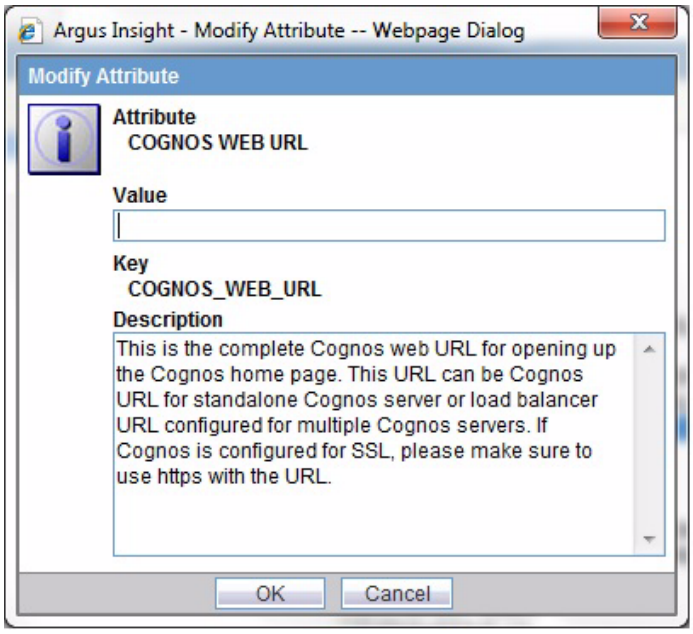
> **Note:** You must configure the COGNOS AUTHENTICATION ENTERPRISE profile switch for Cognos integration. The default value of this switch is Null.

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:



   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 WEB URL** from the Attributes group. Argus Insight uses this attribute to identify which Cognos 10 Web URL to use.
   a. Click **Modify.** The following Modify Attribute dialog box opens:



b. Click the **Value** field, and enter the name of the Cognos Web URL for opening the Cognos Home Page. This URL can be the Cognos URL for standalone Cognos server or the Load Balancer URL configured for multiple Cognos servers. If Cognos is configured for SSL, you must use **https** with the URL.

Example: http://<server name>/Cognos102

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

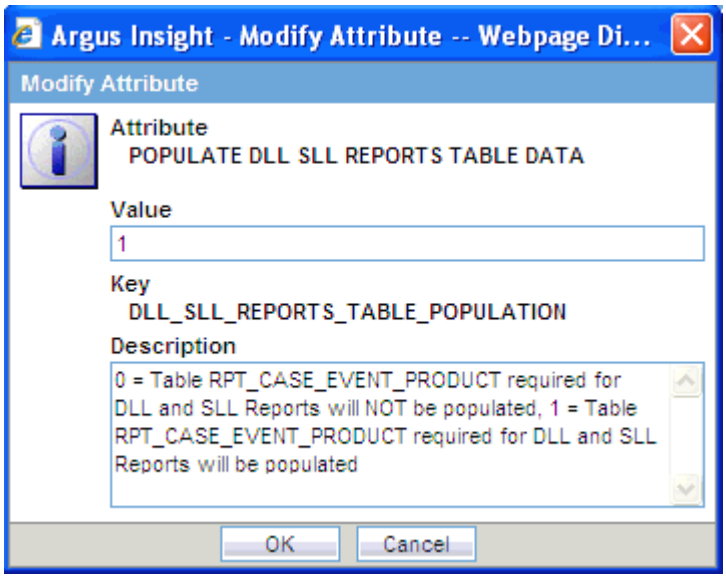
5. Select **POPULATE DLL SLL REPORTS TABLE DATA** from the Attributes group.

Note: The attribute mentioned below is obsolete in case of a fresh installation of Argus Insight 7.0.3.

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:



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

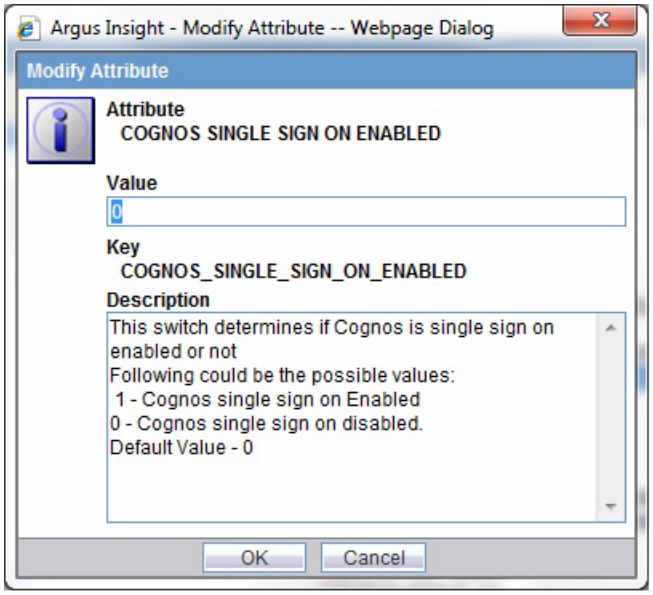
0 = Do not populate the RPT_CASE_EVENT_PRODUCT table, which is required for DLL and SLL reports

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.

6. Select **COGNOS SINGLE SIGN ON ENABLED** from the Attributes group.

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



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

1 = Cognos single sign on enabled

0 = Cognos single sign on disabled

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

4.3 Configuring Duration Value Bands

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

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

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

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

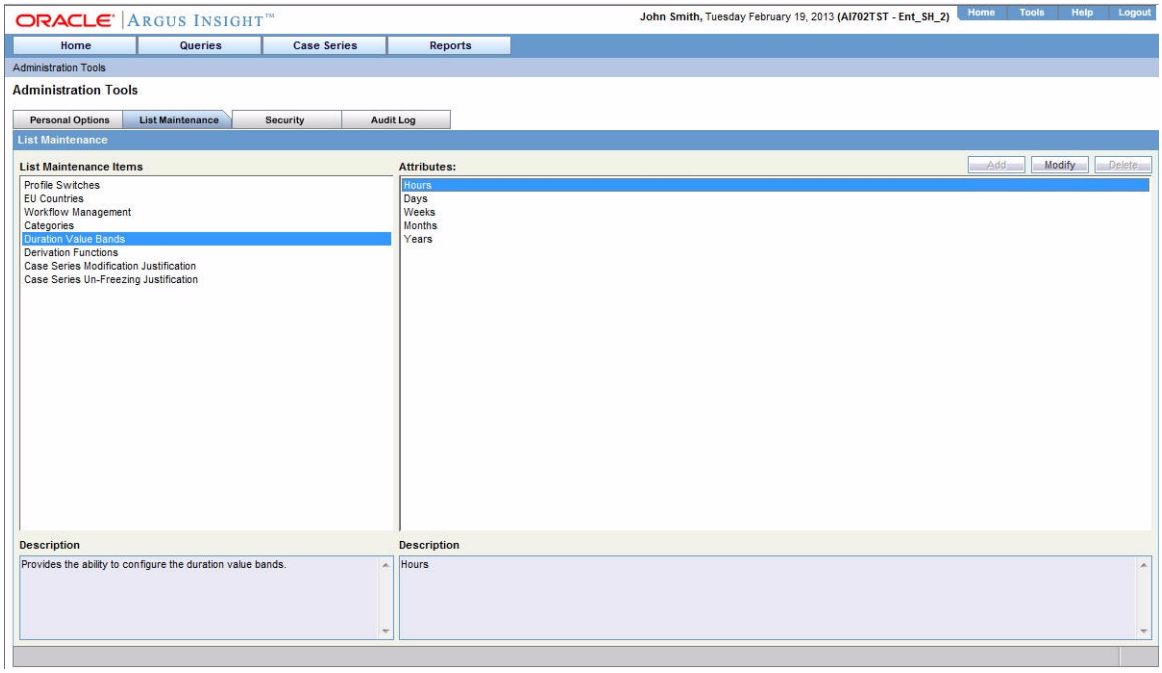
Using the Duration Value Bands item on the List Maintenance tab, you can configure duration value bands in hours, days, weeks, months, and years. For each band, you can specify multiple ranges by entering minimum and maximum values for each range item. Any value that falls within a configured range will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

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

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

To modify a duration value band:

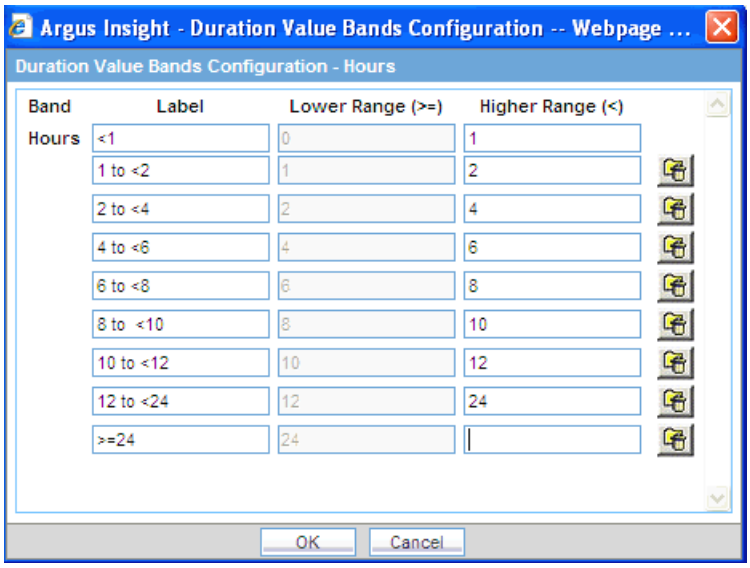
1. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page. The ADMINISTRATION TOOLS page opens.
2. Click the **List Maintenance** tab.
3. Select **Duration Value Bands** from the List Maintenance Items group. The Attributes group displays the valid bands (Hours, Days, Weeks, Months, and Years). You can modify the values of these bands. You cannot, however, add more bands or delete an existing band.



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.



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.

4.4 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.

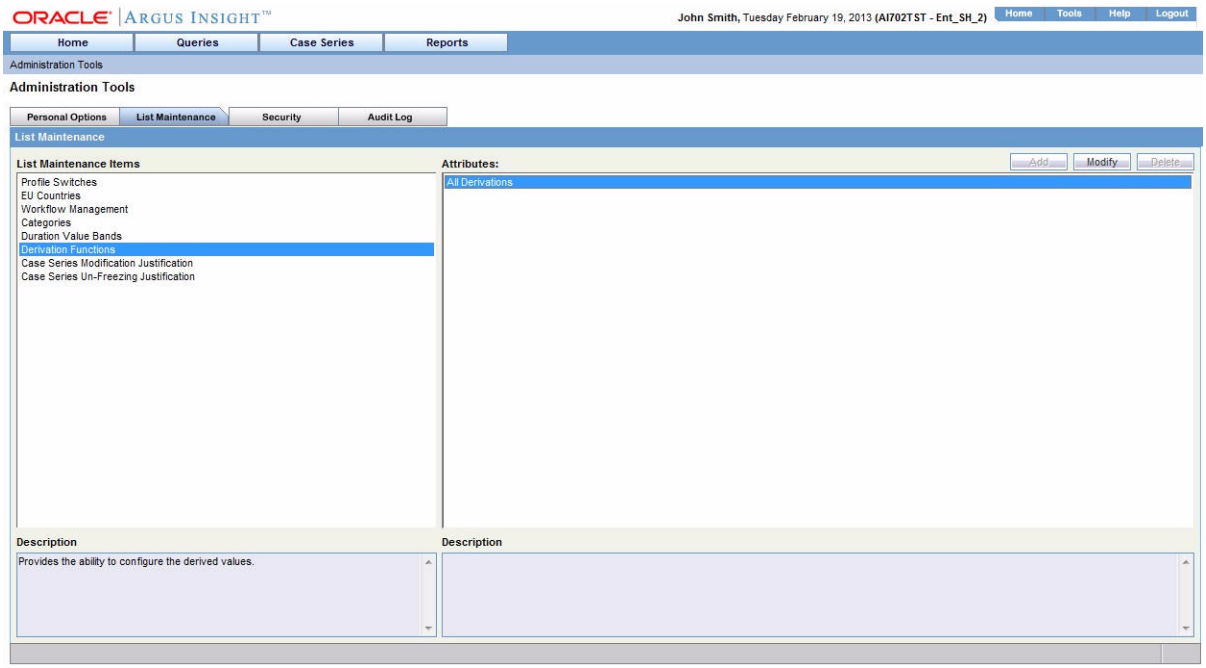
You can specify more than one attribute. For example, you can create a further specialized List Maintenance item called **Report Type 1 US** and derive to this item all the cases that have the **Report Type** attribute defined as **Spontaneous, Literature,** or **Compassionate Use,** *and* the **Country 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.

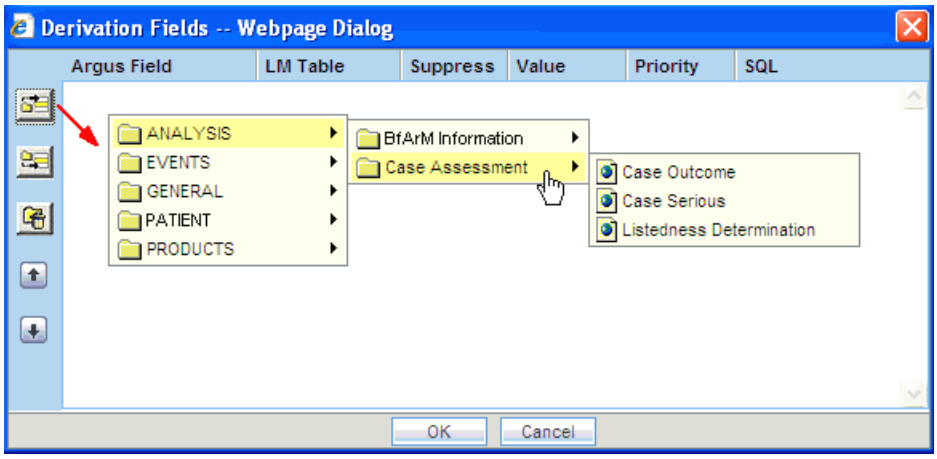
4.4.1 Opening the Derivation Fields Dialog Box

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.



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



4.4.2 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

Table 4–1 (Cont.) Icons in the Derivation Fields Dialog Box

Click…	To…
	Delete the currently selected derivation field element (row)
	Move the selected row up
	Move the selected row down

4.4.3 Field Mapping Derivation Rules

Table 4–2 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 Case Serious Listedness Determination
EVENTS	Event Information	Lack of Efficacy
GENERAL	General Information	Report Type Derived Pregnancy
PATIENT	Patient Information	Age Group Gender Patient weight BMI desc
PRODUCTS	Product Drug	Derived Drug Abuse Derived Drug Interaction Derived Overdose Last daily dose

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

4.4.4 Fields and Check Boxes in the Derivation Fields Dialog Box

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

4.4.4.1 LM Table

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

4.4.4.2 Suppress

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

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

4.4.4.3 Value

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

4.4.4.4 Priority

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

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

4.4.4.5 SQL

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

Note: The SQL statement must follow the correct syntax.

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

Guidelines for correct syntax:

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

  Correct: SELECT CASE_ID FROM RPT_CASE WHERE…

  Incorrect: SELECT RPT_CASE.CASE_ID FROM RPT_CASE WHERE…

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

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

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

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT DISTINCT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

4.5 Configuring the Argus Insight 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.

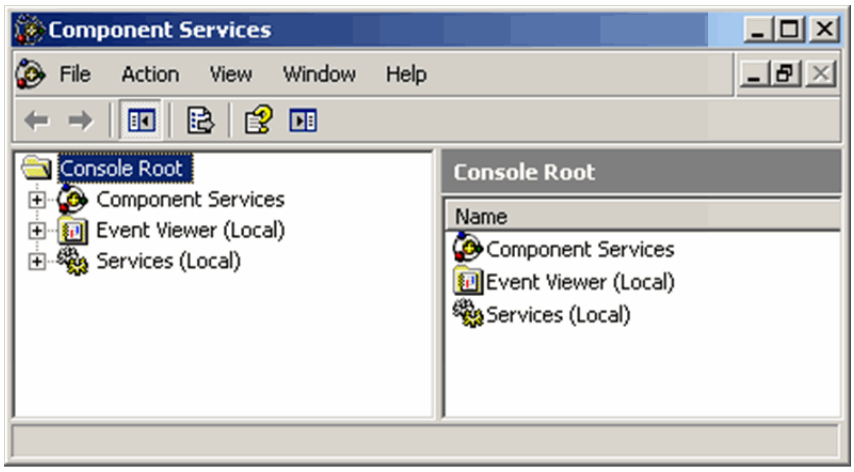
> **Note:** To change the interval of different service tasks, modify the entries in the Service.config file located in the Bin folder of Argus Insight. All the times in the Service.config file are specified in seconds.

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.

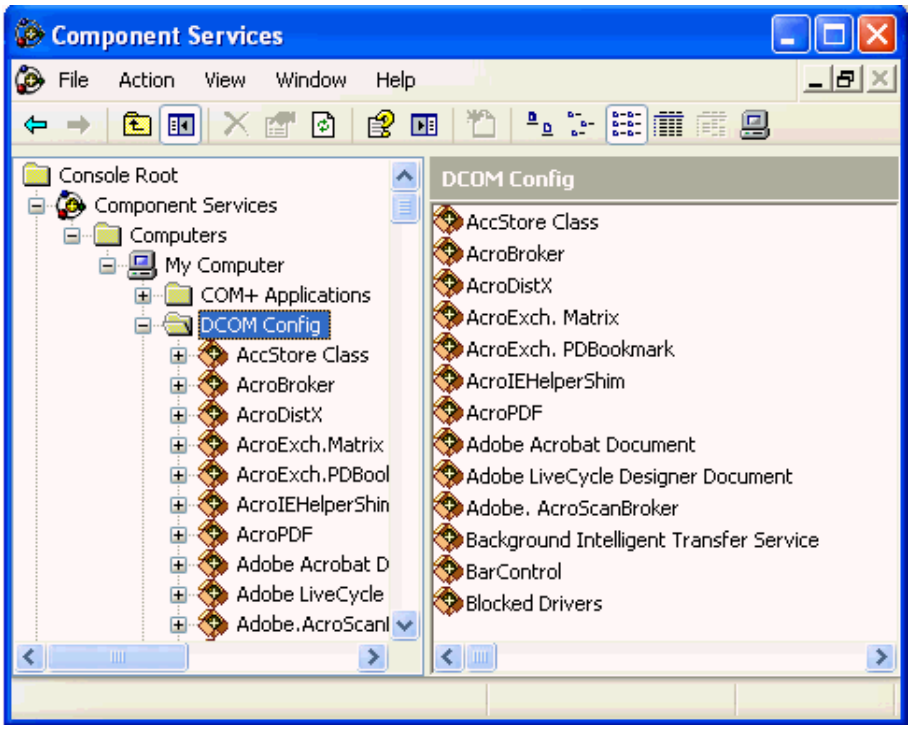
4.6 Configuring the CIOMS and MedWatch Reports

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

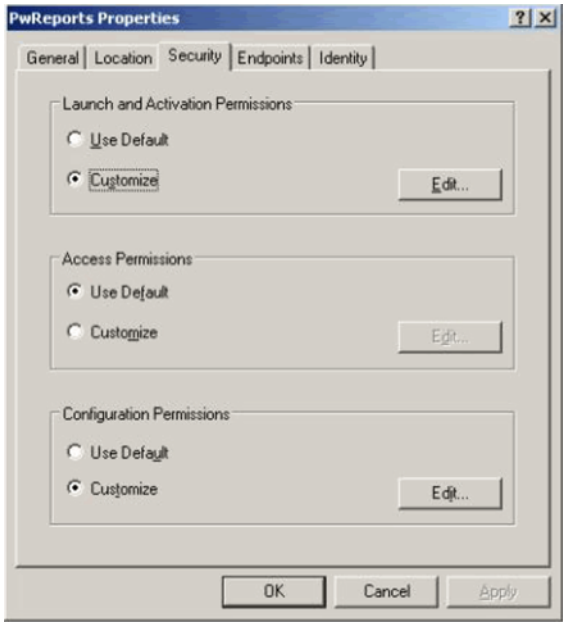
1. Log in to the Argus Insight Web Server.
2. Click **Start** and then select **Run.**
3. Type **dcomcnfg** in the text box and click **OK.** The Component Services window opens.



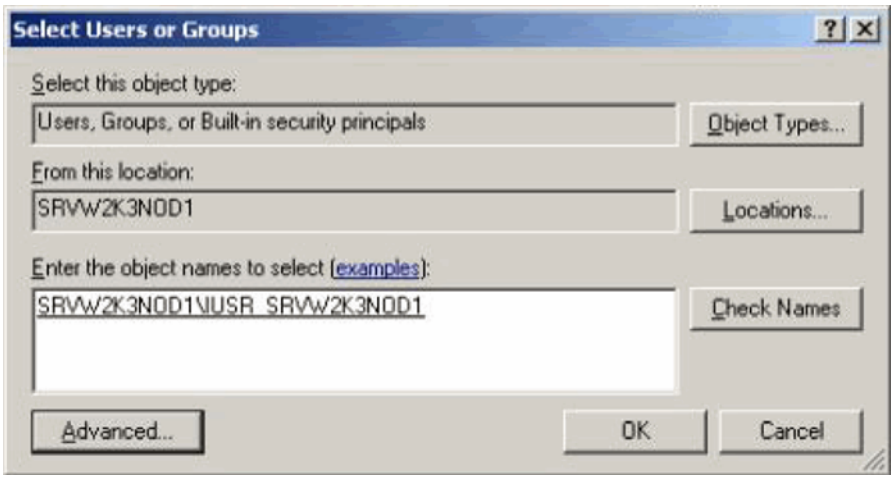
4. Navigate to **Console Root, Component Services, Computers, My Computer,** and then select **DCOM Config.**



5. Right-click **PwReports** and select **Properties.** The PwReports Properties dialog box opens.
6. Click the **Security** tab.



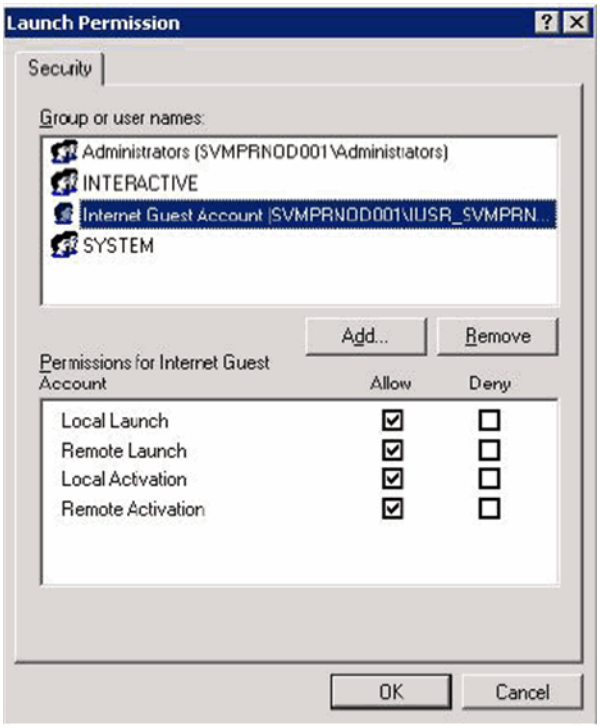
7. Look in the Launch and Activation Permissions group, select **Customize,** and then click **Edit.** The Launch Permission dialog box opens.
8. Click **Add.** The Select Users or Groups dialog box opens.



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:



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.

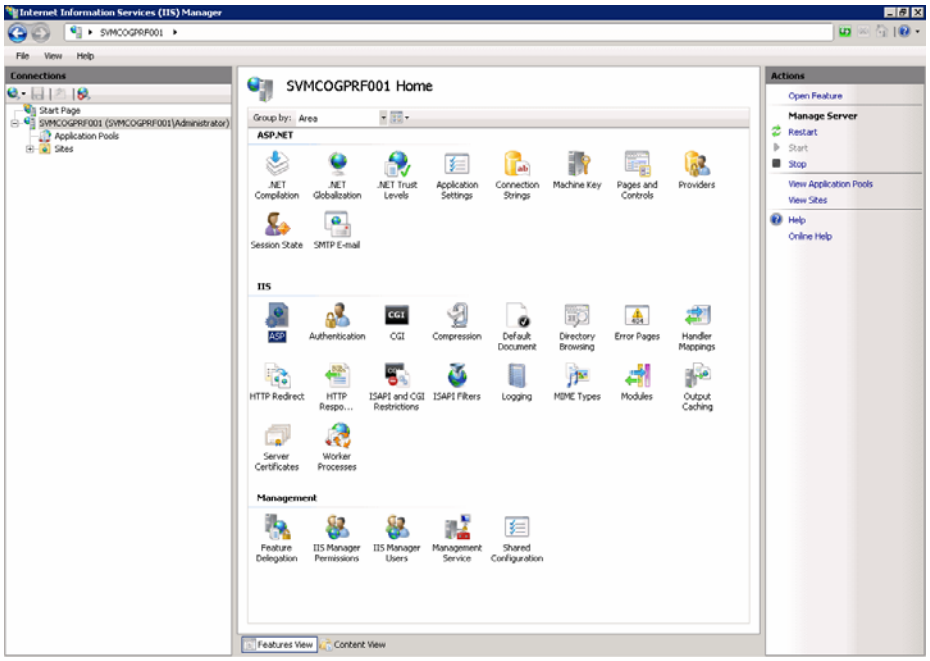
c. Click **OK.**

10. Exit the Component Services program.

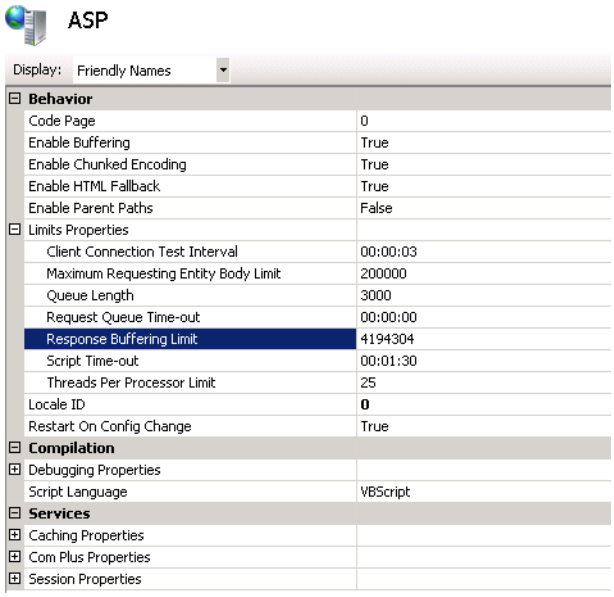
4.7 Configuring the IIS File Download Limit

To configure the IIS file download limit for Windows 2008:

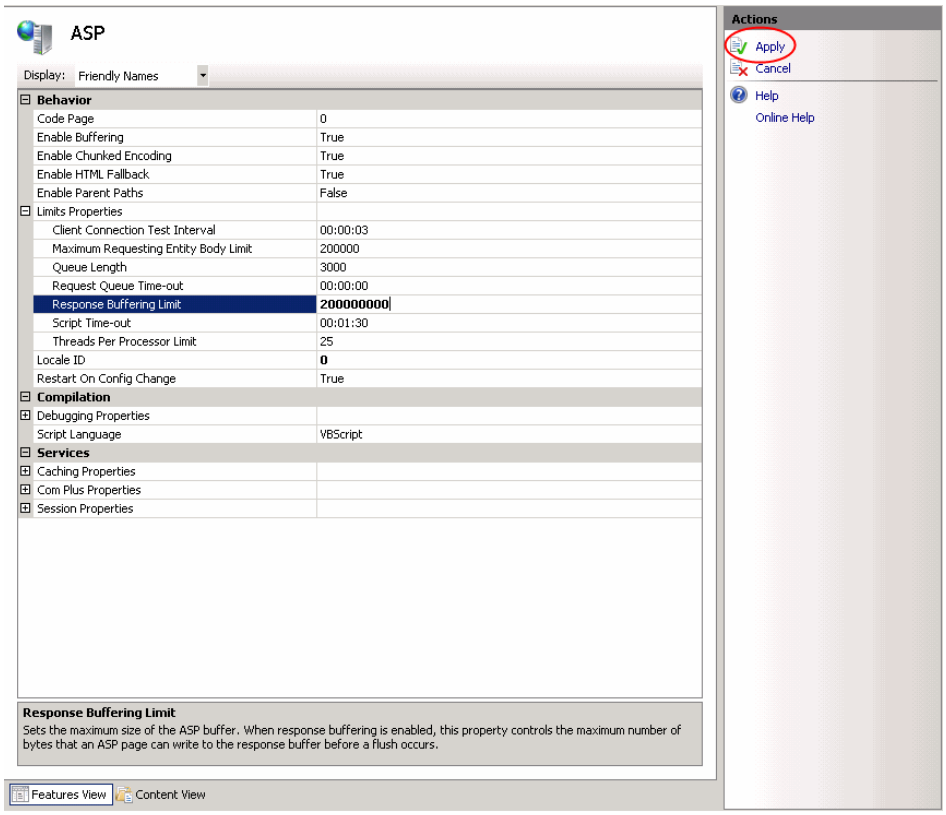
1. Go to the Internet Information Services (IIS) Manager.



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



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).



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.**

4.7.1 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
```

4.8 Using Export and Import to Copy Configuration Data

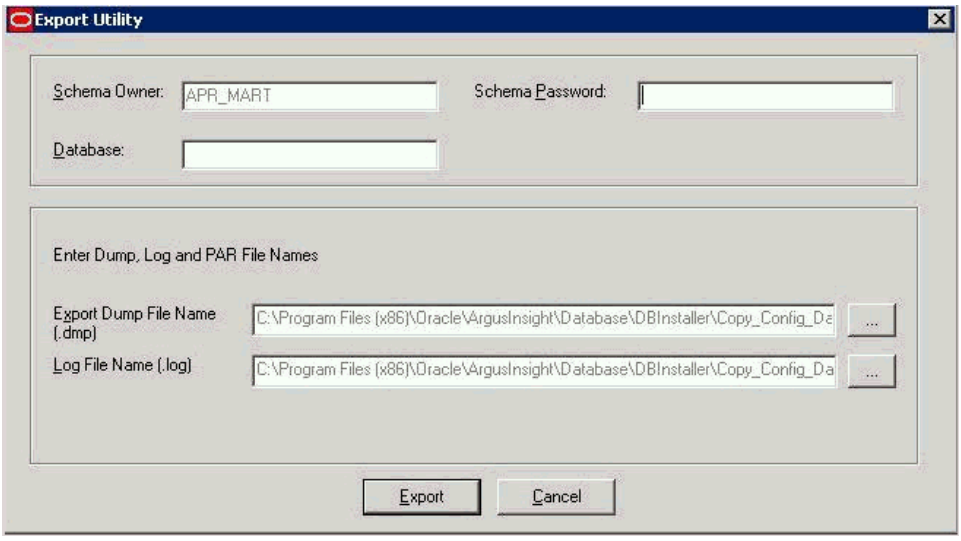
Before configuring export and import functions, be aware of the following:

- 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.

4.8.1 Exporting Data

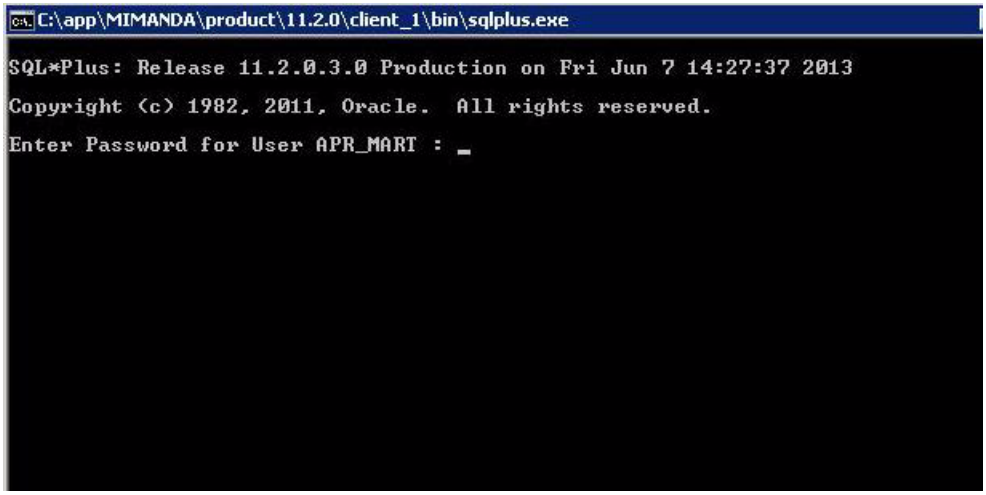
To export data:

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

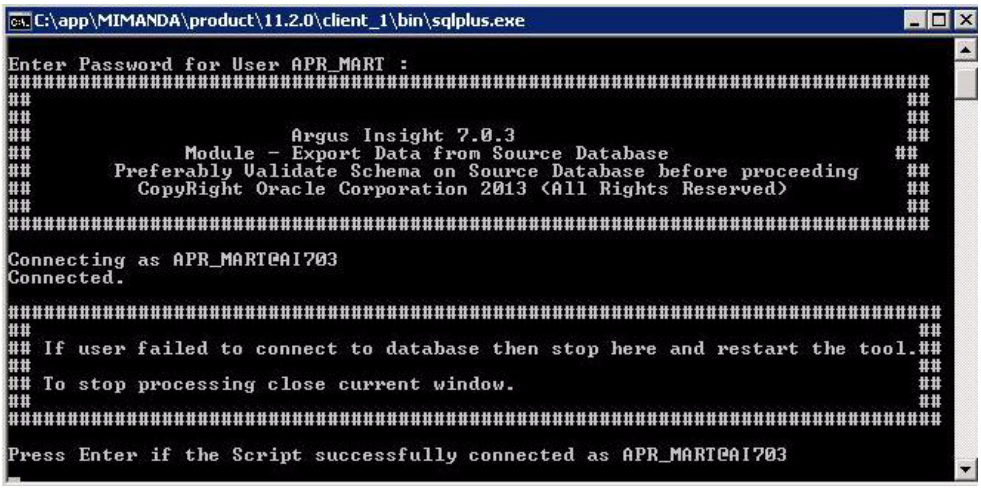


3. Enter the name of the schema owner, the schema password, and the name of database.
4. Enter the complete directory path and file name for the export dump file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Export Dump File 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:

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

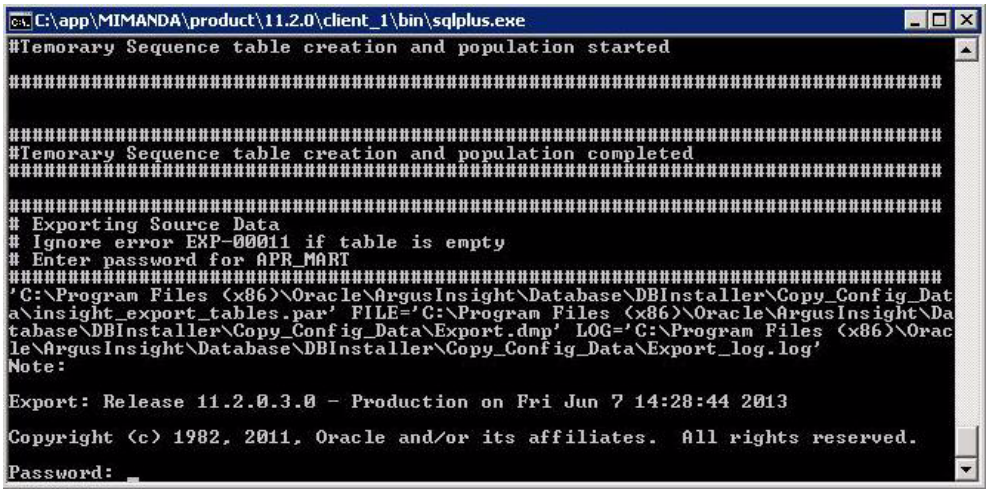


8. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



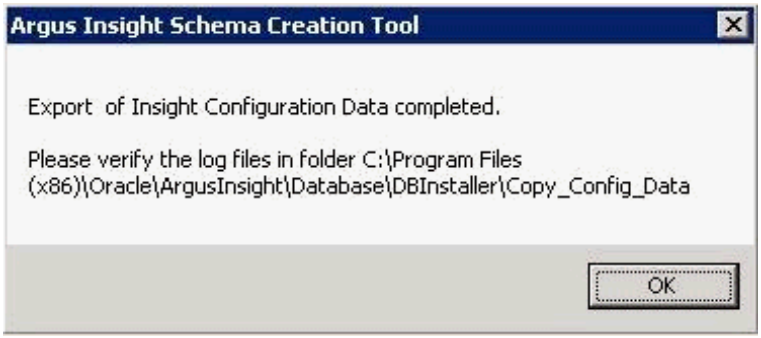
9. Verify that the script is successfully connected as <APR_MART User Name>@<Argus Insight Database Name> and press **Enter**. This displays the screen, with the Argus Insight Mart details.

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



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:



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.

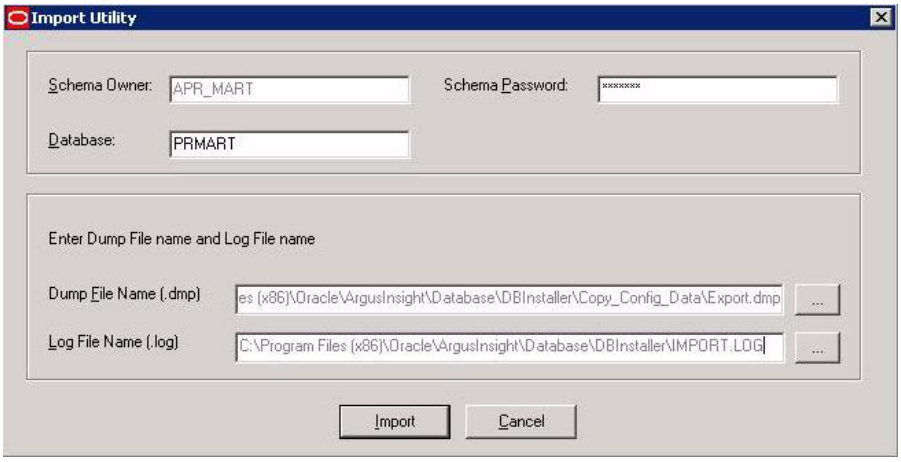
    Log files are in the following folder:

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

4.8.2 Importing Data

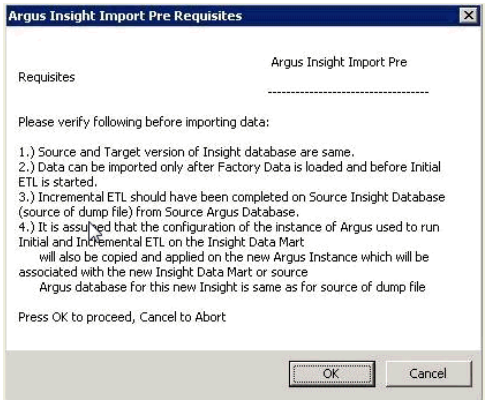
To import data:

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

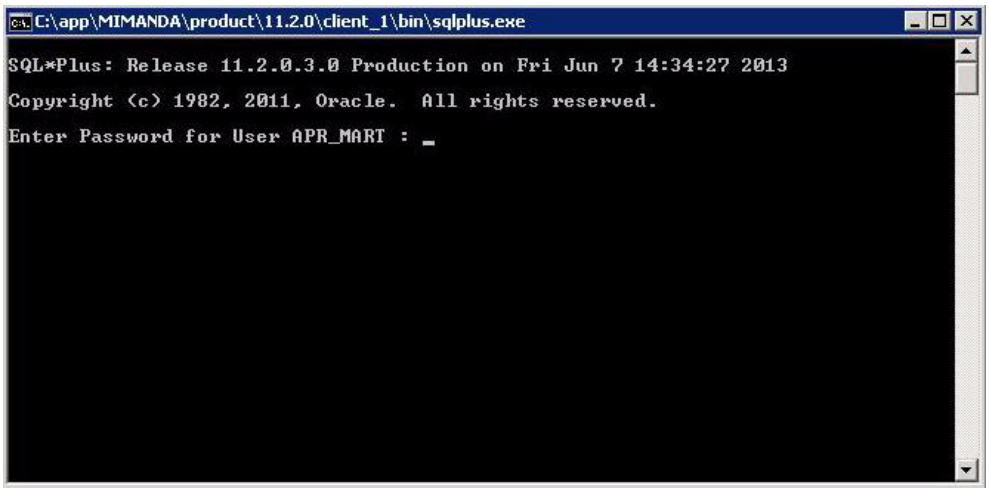


3. Enter the name of the schema owner, the schema password, and the name of database.
4. Enter the complete directory path and file name for the dump file. You can choose to:
   - Keep the default file location and name as specified.
   - Click the **...** button next to the **Dump File Name** field. 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.

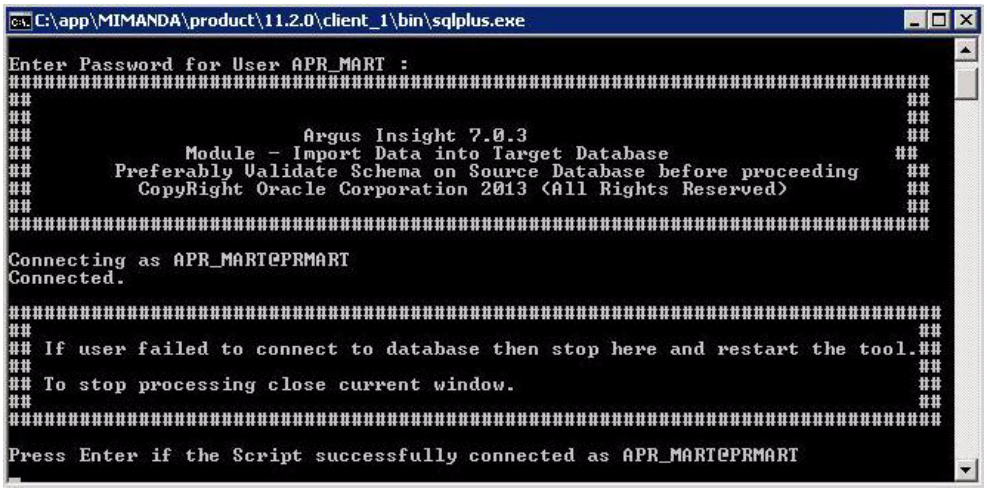
   The system opens a dialog box that lists the prerequisites to importing data.



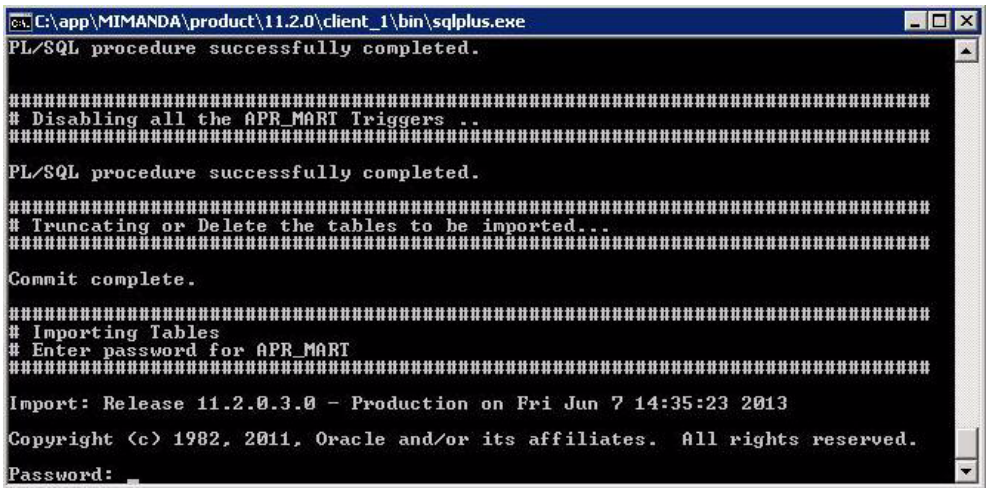
7. Review the prerequisites and verify that your system complies with the requirements.
   - If you have not met all the prerequisites, click **Cancel** to stop the data import. Complete all prerequisites before restarting the data import process.
   - If you have met all the prerequisites, click **OK.**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



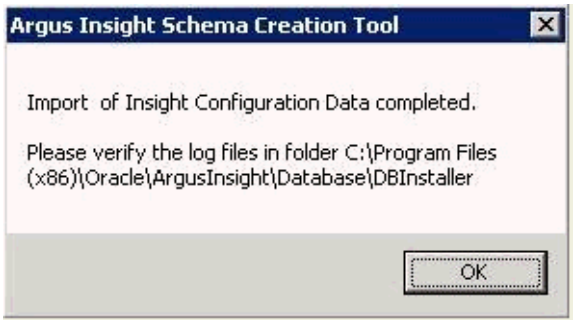
8. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



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



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:



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

4.9 Using Argus Safety to Configure Enterprises for Argus Insight

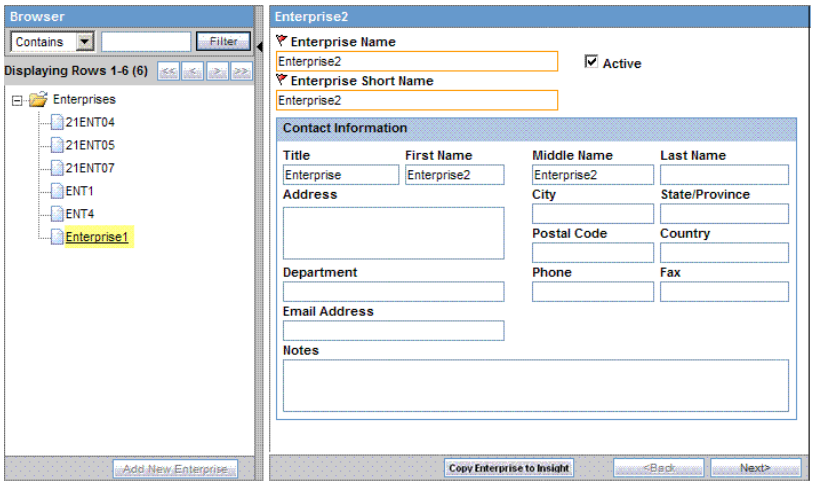
Using Argus Safety to configure enterprises for Argus Insight is supported in multi-tenant installations only.

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:

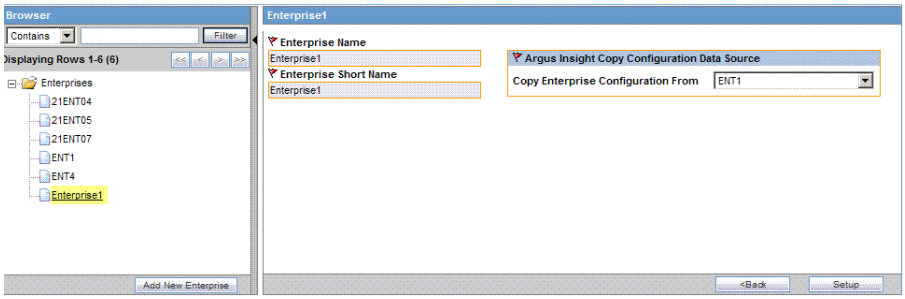


3. Click **Copy Enterprise to Insight** to initiate the creation of the selected enterprise in Argus Insight.

   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:

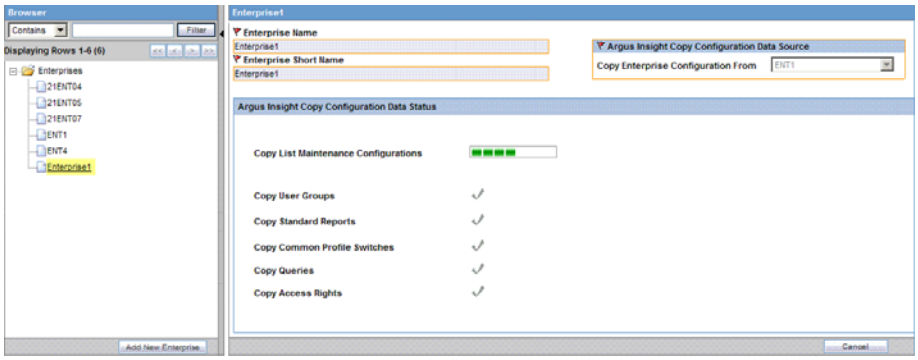


4. Use the **Copy Enterprise Configuration From** field to select the source enterprise from which the information will be copied.

   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:



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

4.10 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:

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.
  ```

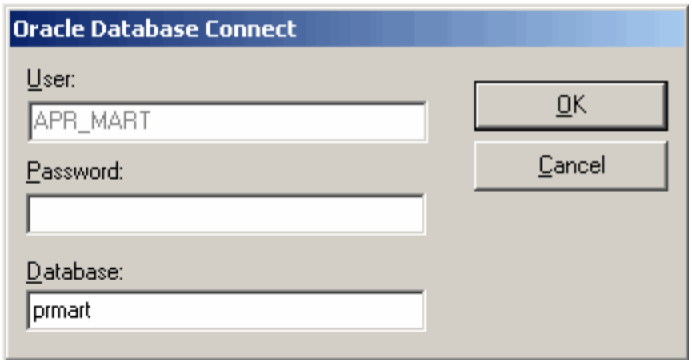
  Ignore this warning for all MedDRA tables.
- **Do not** run incremental ETL for more than 50,000 cases. Run the Initial ETL again if the number of cases exceeds 50,000.

5.2 Running the Initial ETL

To run the initial ETL:

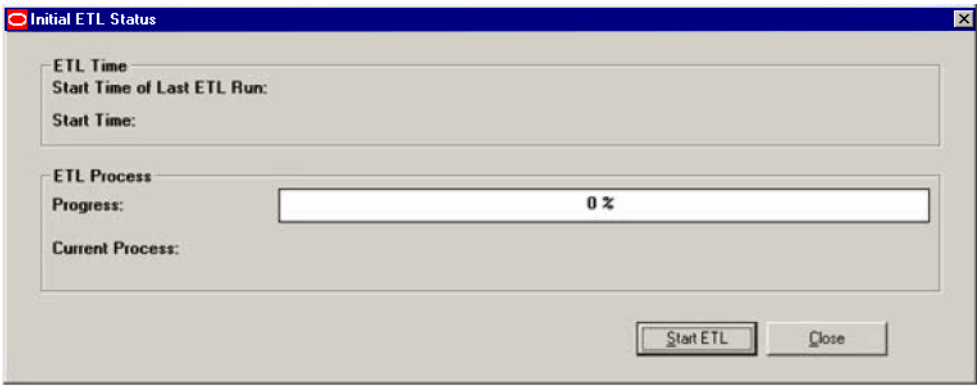
1. Log in to the Argus Insight Web Server as a user with administrator privileges.
2. Click **Start.**
3. Navigate to **Programs, Oracle, Argus Insight,** and then select **Schema Creation Tool.**

4. Click **Initial ETL.** The Oracle Database Connect dialog box opens.

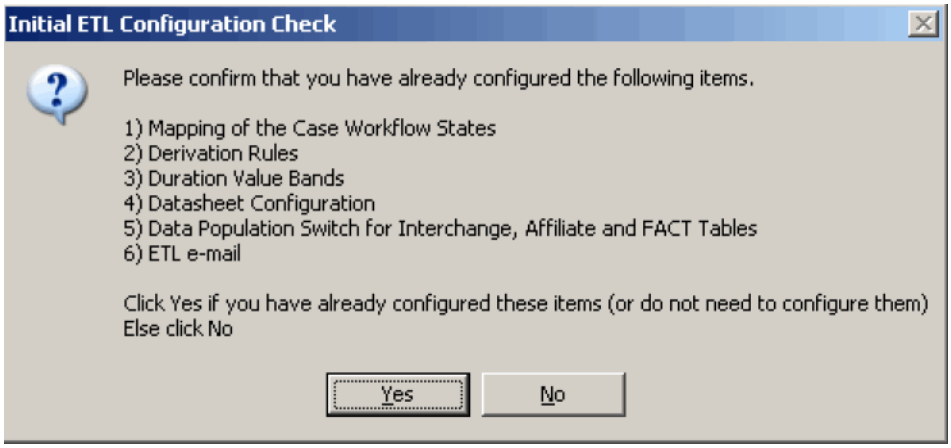


5. Connect to the Oracle Database:
   a. In the **Password** field, type the password for the APR_MART user.
   b. In the **Database** field, type the name of your Argus Insight database.
   c. Click **OK.**

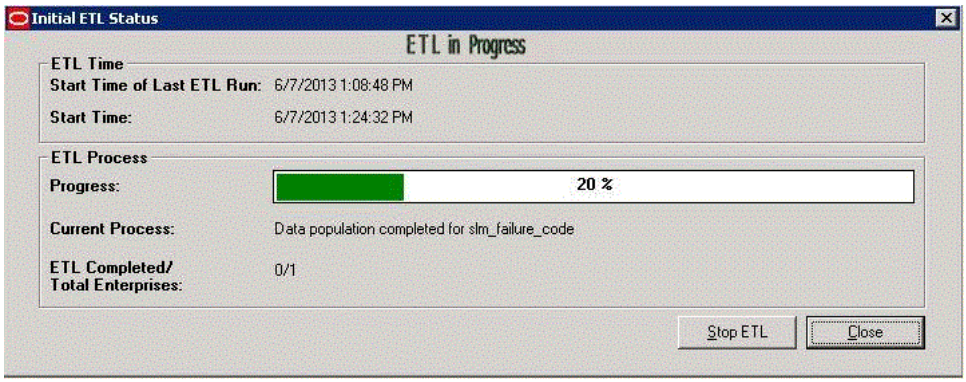
   The Initial ETL Status dialog box opens.



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.



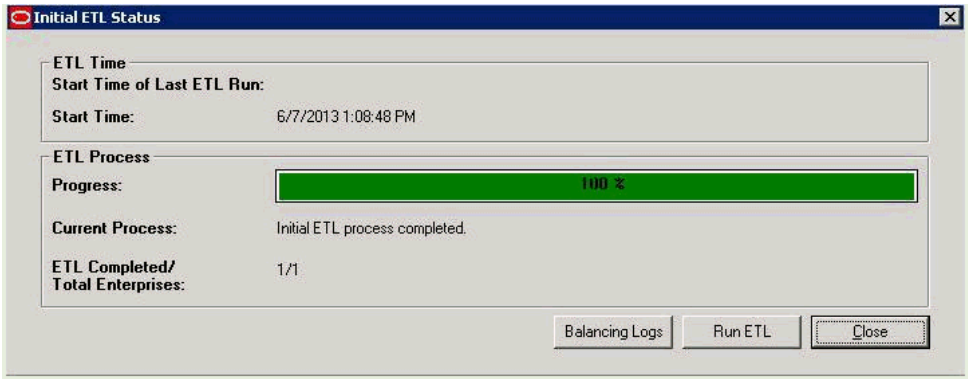
7. Click **Yes** if these items have already been configured. The system displays a status dialog box showing the start time of the ETL, the progress bar, and the current process in execution.



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.

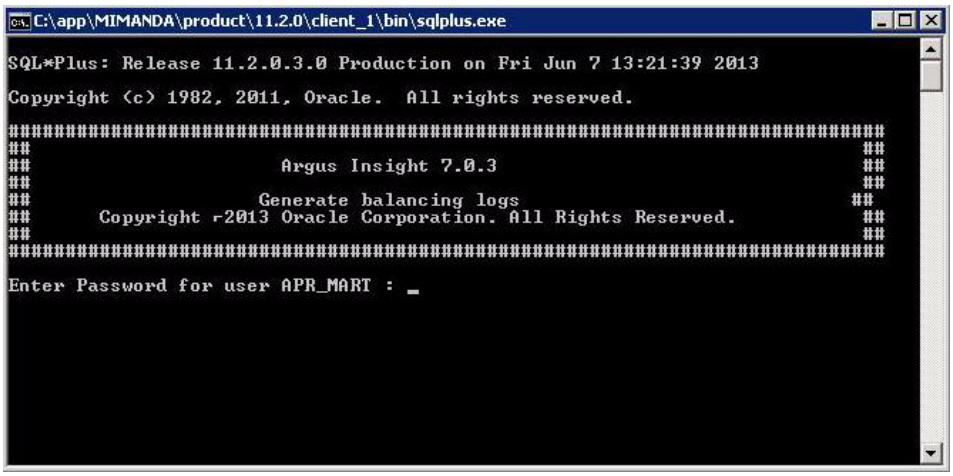


5.2.1 Generating the Balance Logs

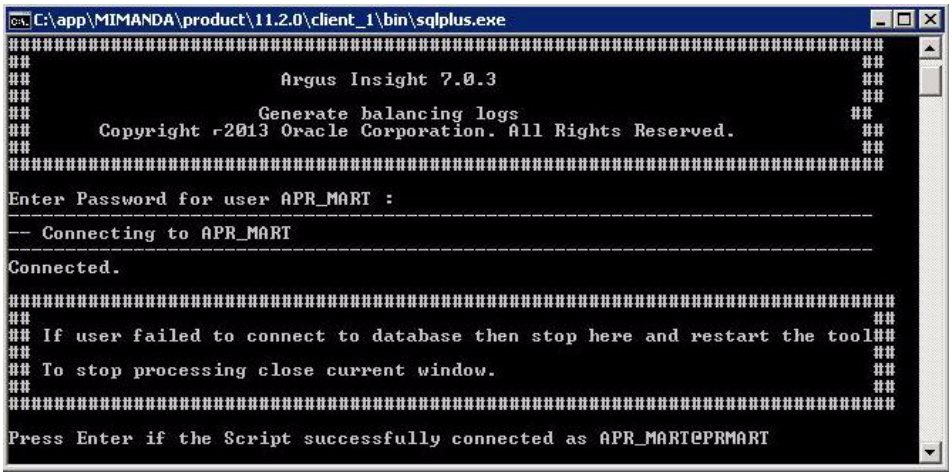
When the system successfully completes the Initial ETL process, you should generate and check the logs.

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:

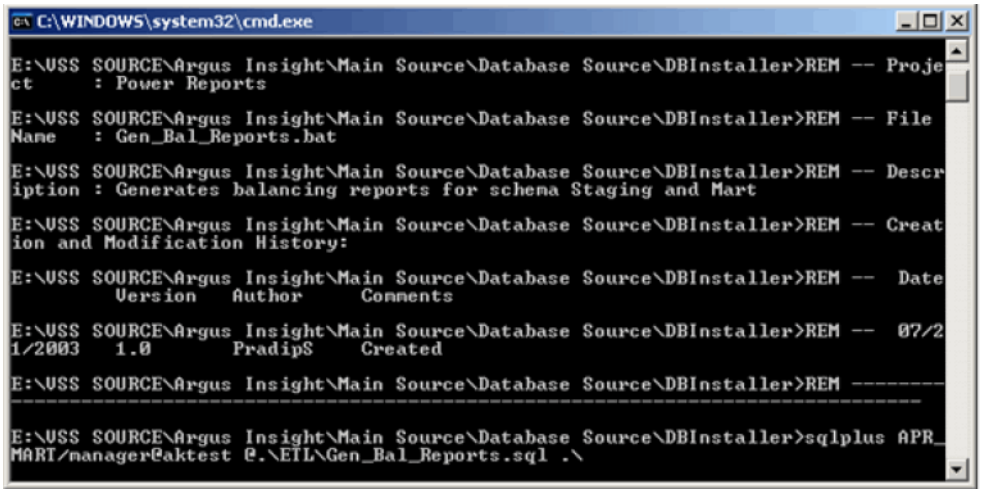


4. Enter the password for the **APR_MART** user and press **Enter**. This displays the following command screen:



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.



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

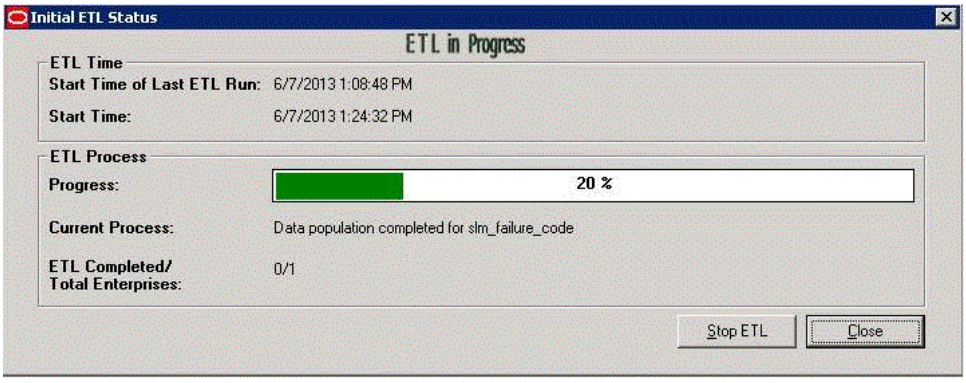
5.2.2 Closing the Initial ETL Status Dialog Box

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.**

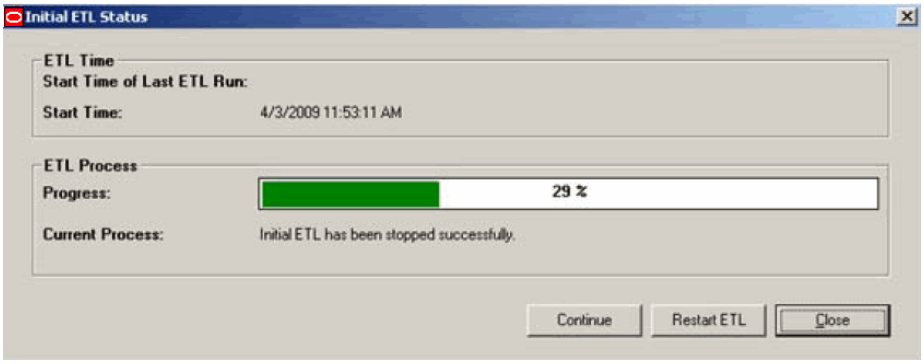
5.2.3 Stopping the Execution of ETL

You can choose to stop an ETL in progress.



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:



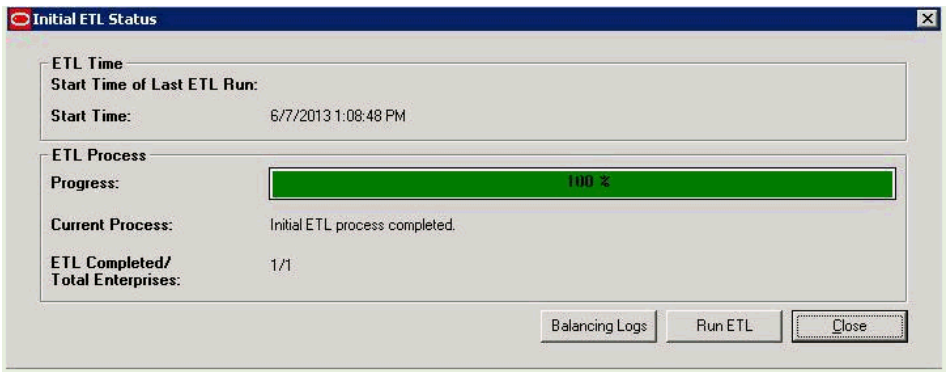
At this point, you can select one of the following options:

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

5.3 Running the Initial ETL Again

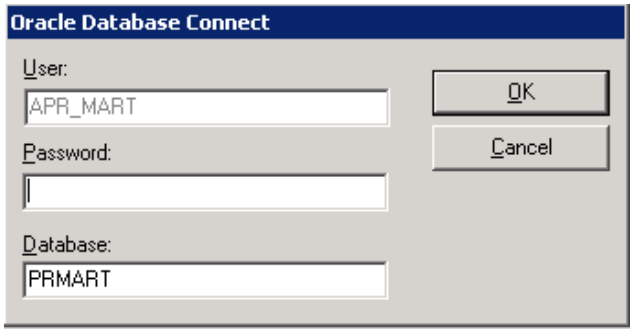
To start the ETL process from the beginning:

1. Click **Run ETL.**



The system prompts for confirmation on whether you want to start the initial ETL from the beginning.

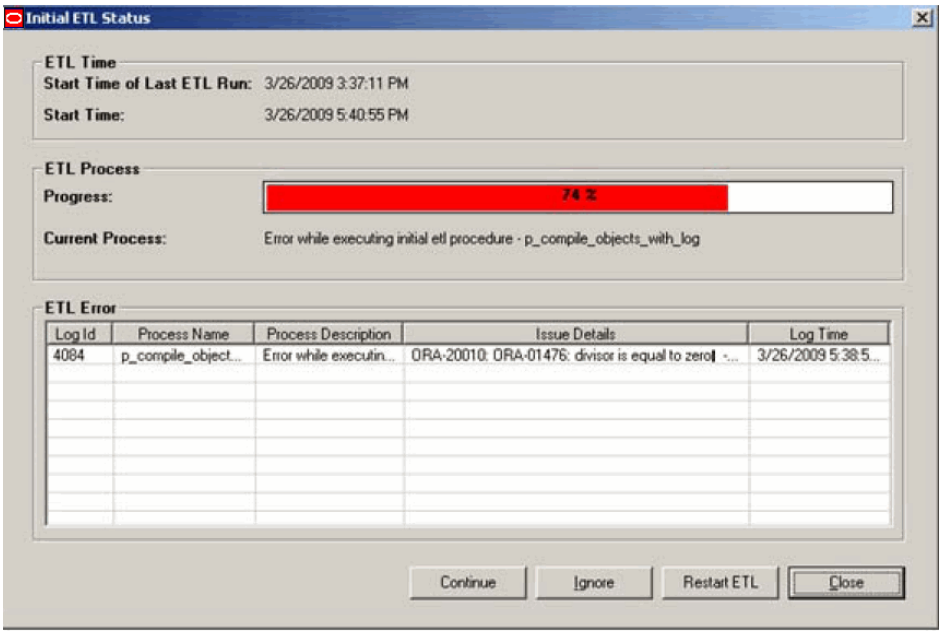
2. Click **OK.** The Oracle Database Connect dialog box opens.



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:



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

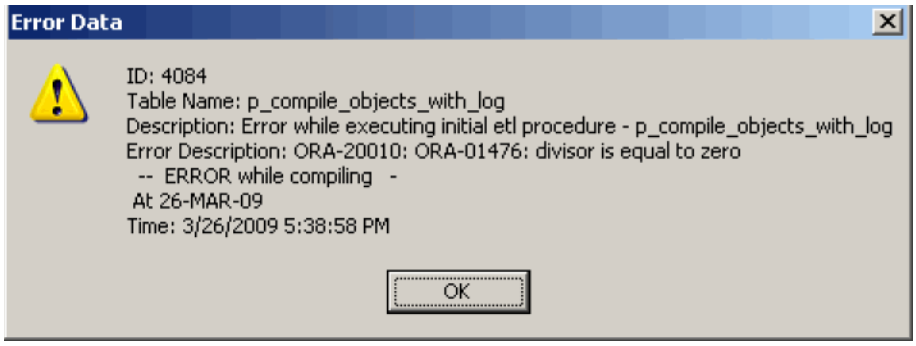
- Click **Continue** to continue the failed Initial ETL process.
- Click **Ignore** to ignore the failed Initial ETL process.
- Click **Modify Attributes** of ETL Data Exclusion if PRE_REQ_CHECK_FLAG switch is set to ABORT.

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

5.4.1 Continuing the Failed Initial ETL Process

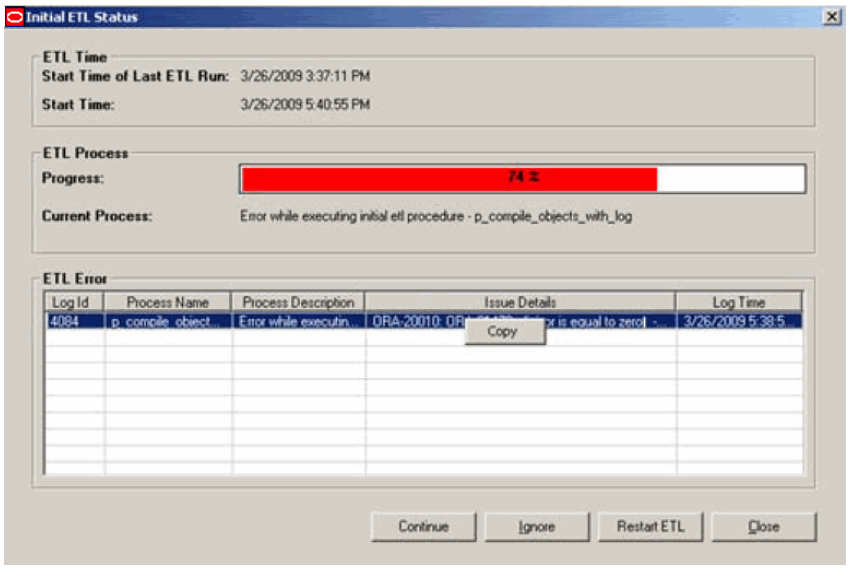
To continue the Initial ETL process from the failed ETL procedure:

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

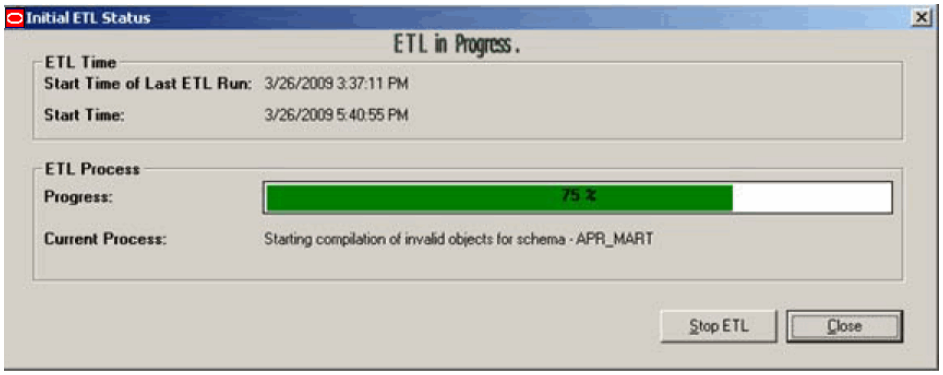


2. Review the error information, and then click **OK.**

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



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).



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).

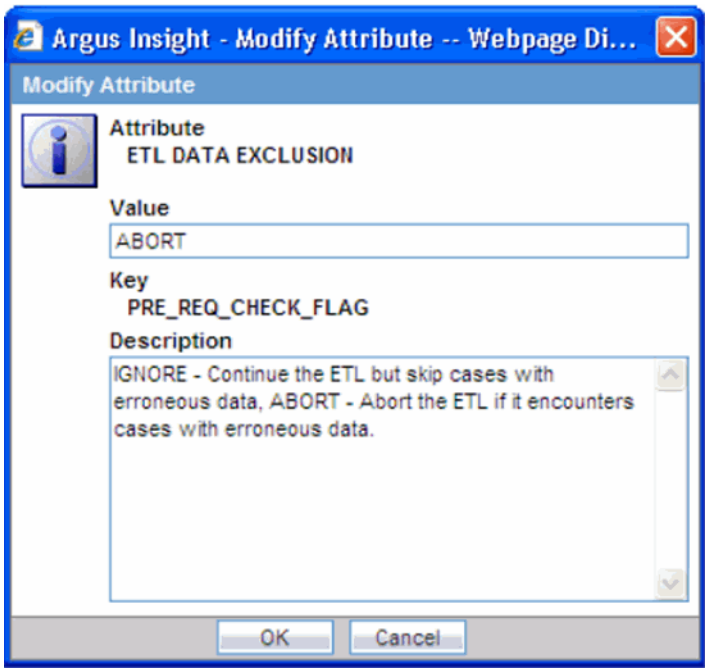
5.4.3 Modifying the Attributes of ETL Data Exclusion

You must modify these attributes before ETL execution.

To modify ETL Data Exclusion attributes:

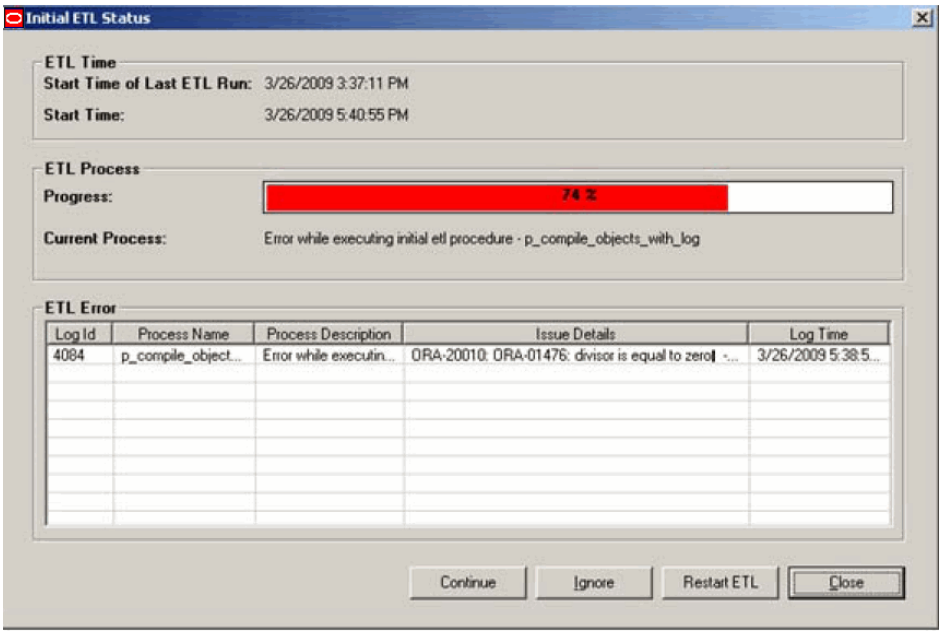
1. Log in to the Argus Insight application as a user with administrator privileges.
2. Click the **Tools** tab in the upper-right corner of the Argus Insight Home page to open the ADMINISTRATION TOOLS page.

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:



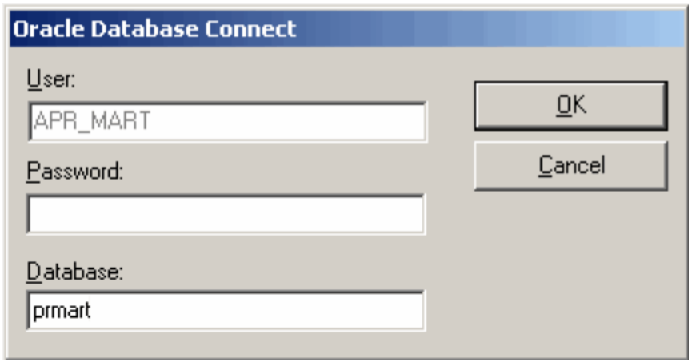
6. Click the **Value** field and enter one of the following values:
   - If you want the ETL process to skip cases with erroneous data and continue processing all other cases, enter **IGNORE.**
   - If you want the ETL process to abort when it encounters cases with erroneous data, enter **ABORT.**
7. Click **OK** to save your changes and return to the List Maintenance tab.

5.5 Restarting the Initial ETL Process

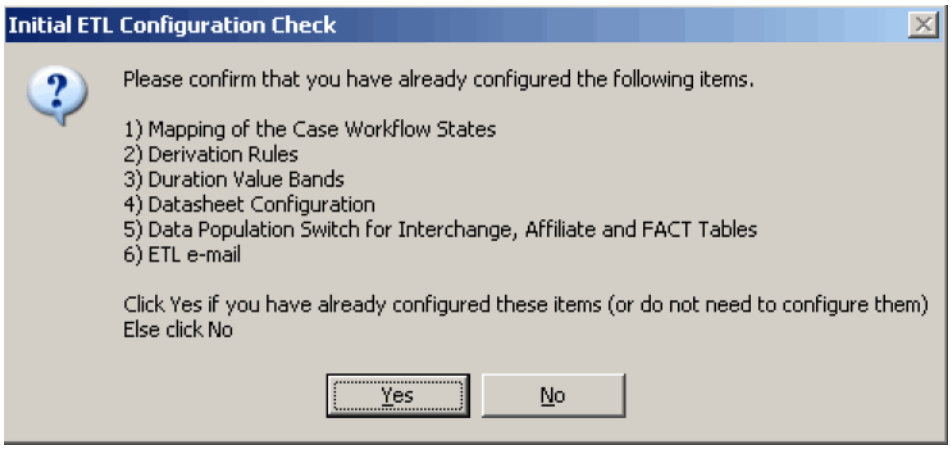


To restart the Initial ETL process starting from after the confirmation message and APR_MART password input:

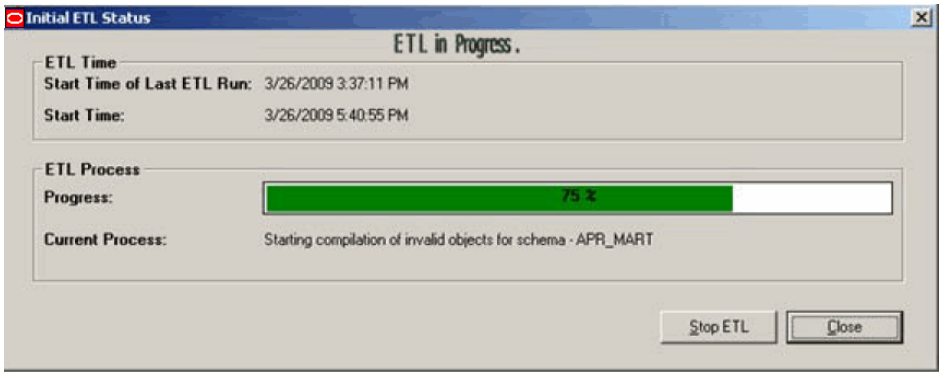
1. Click **Restart ETL.** The system prompts for confirmation that you want to start the initial ETL from the beginning.
2. Click **OK.** The Oracle Database Connect dialog box opens.



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.



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:



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

6

Configuring the BIP Environment

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

This chapter 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

6.1 Uploading the Argus Insight.xdrz file to BIP

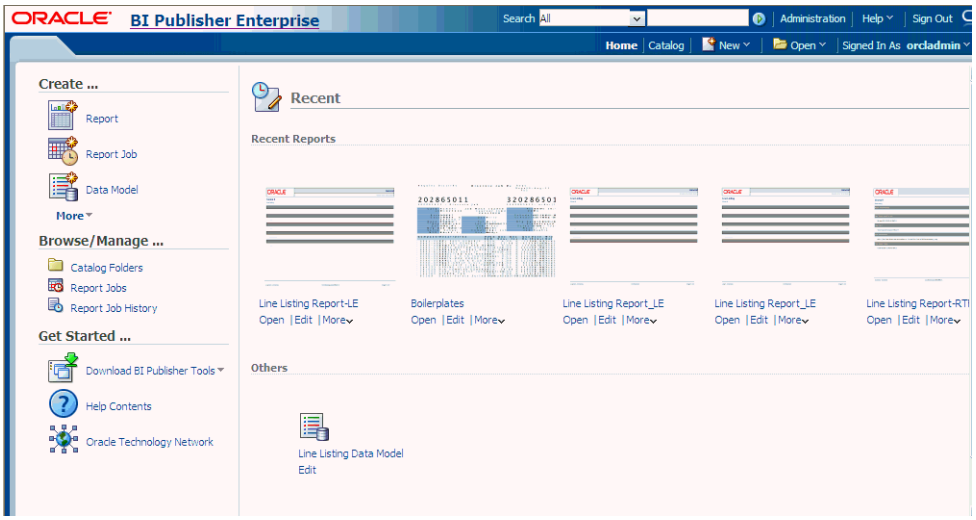
> **Note:** You must be logged in to BIP with the BI Admin User credentials to be able to upload the **Argus Insight.xdrz** file. You can refer to Table 6–3 for more information on the BI Admin User.

To upload the **Argus Insight.xdrz** file to BIP, execute the following steps:

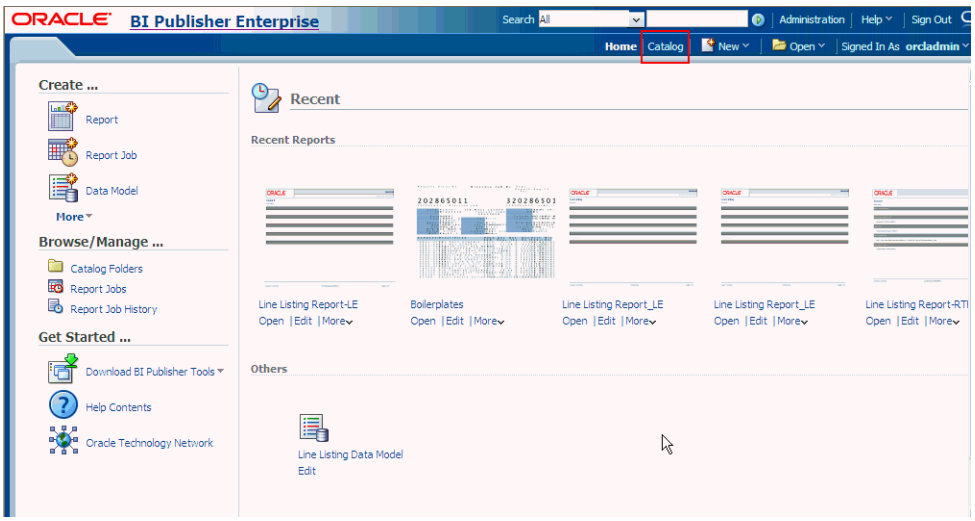
1. Copy the **Argus Insight.xdrz** file from the following location on the Argus Insight Web Server to the local file system:

   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:

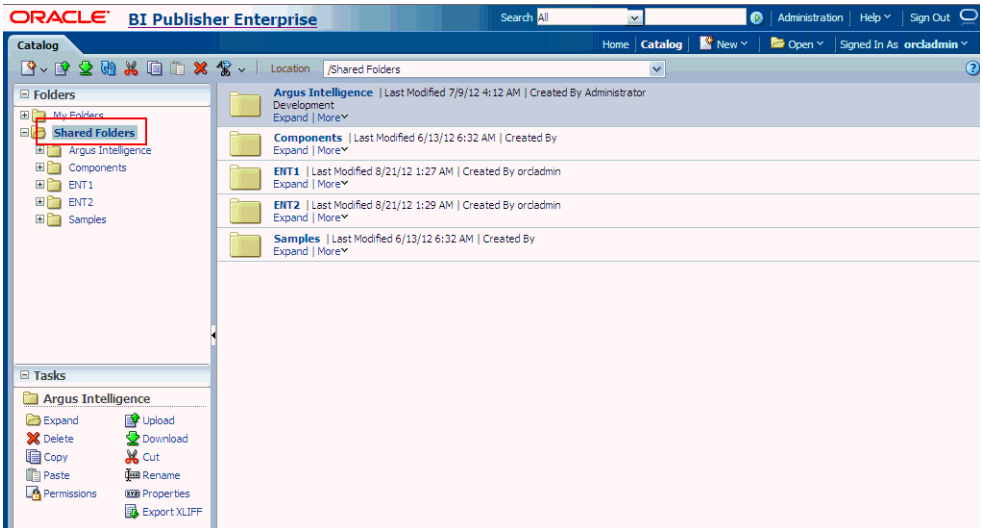


3. Click **Catalog** as highlighted in the following figure:

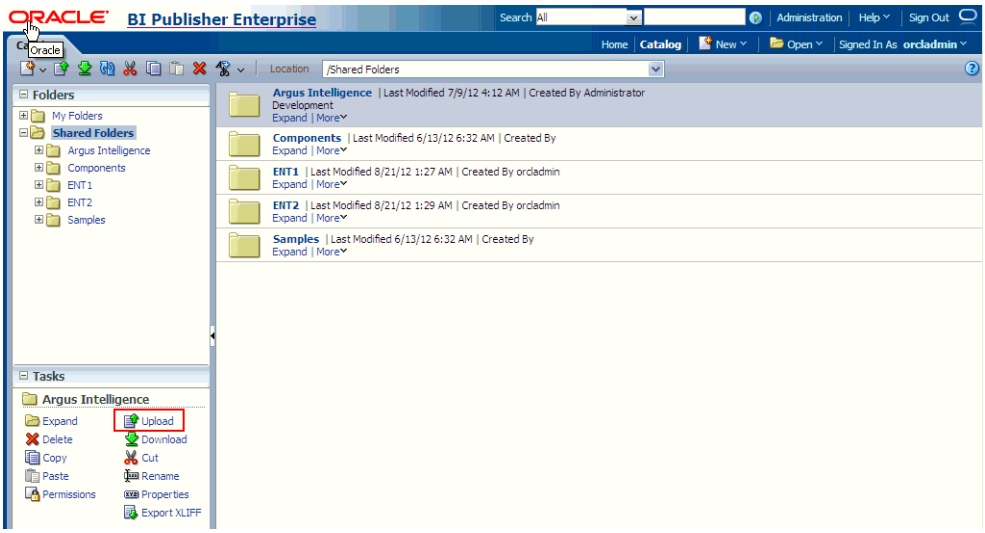


This displays the **Catalog** screen with the **Folders** and **Tasks** sections.

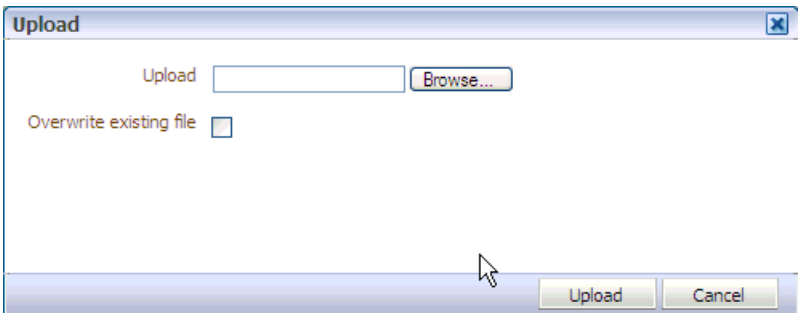
4. Click **Shared Folders** in the **Folders** section as shown in the following figure:



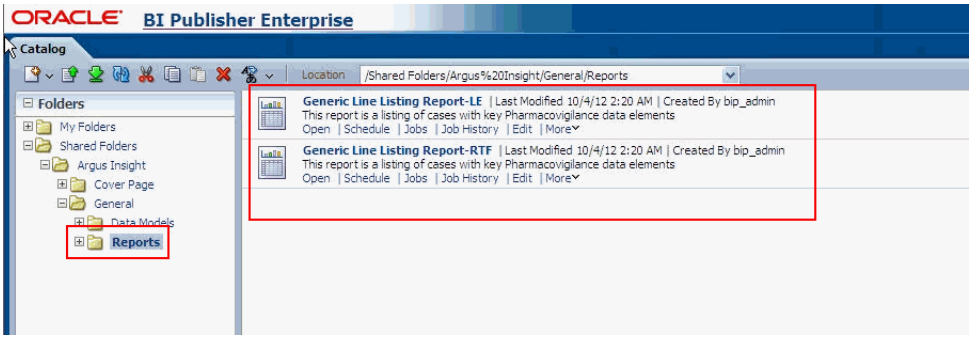
5. Click **Upload** in the **Tasks** section as highlighted in the following figure:



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:



6.2 Creating PRMART JDBC Connection

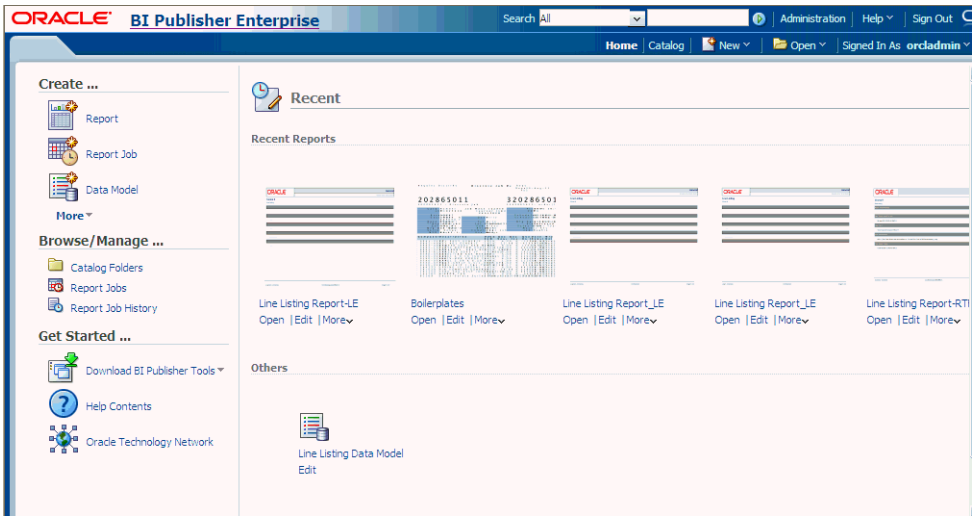
If you are installing BIP on a Windows machine, the TNS entry of Argus Insight must be added in **TNSNAMES.ora** file of the BIP Web Server.

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

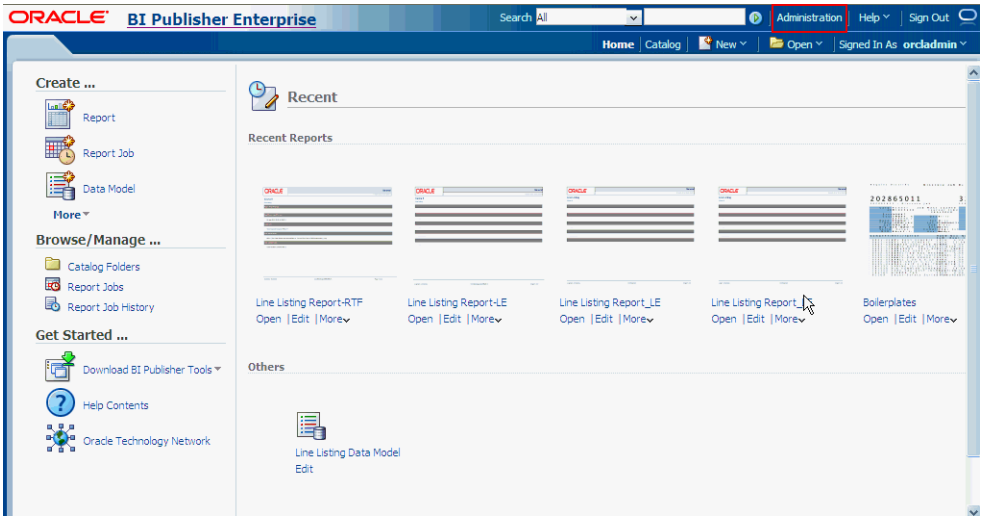
Once you have uploaded the **Argus Insight.xdrz** file to BIP, you also need to create a connection between the BIP and the database.

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:



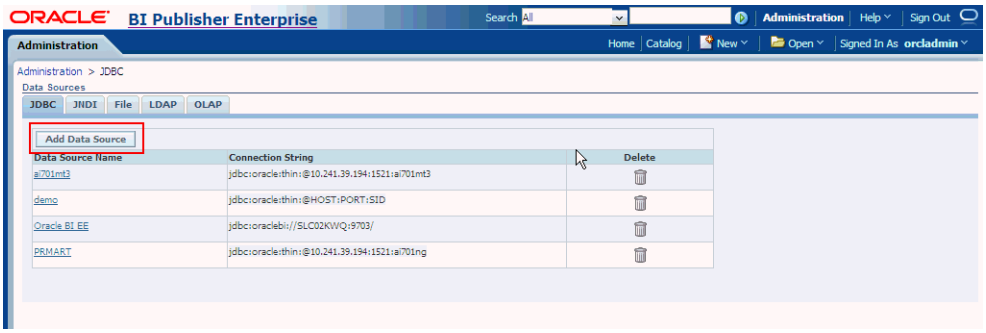
2. Click **Administration** as highlighted in the following figure:



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:



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

   a. Enter **PRMART** in the **Data Source Name** field.

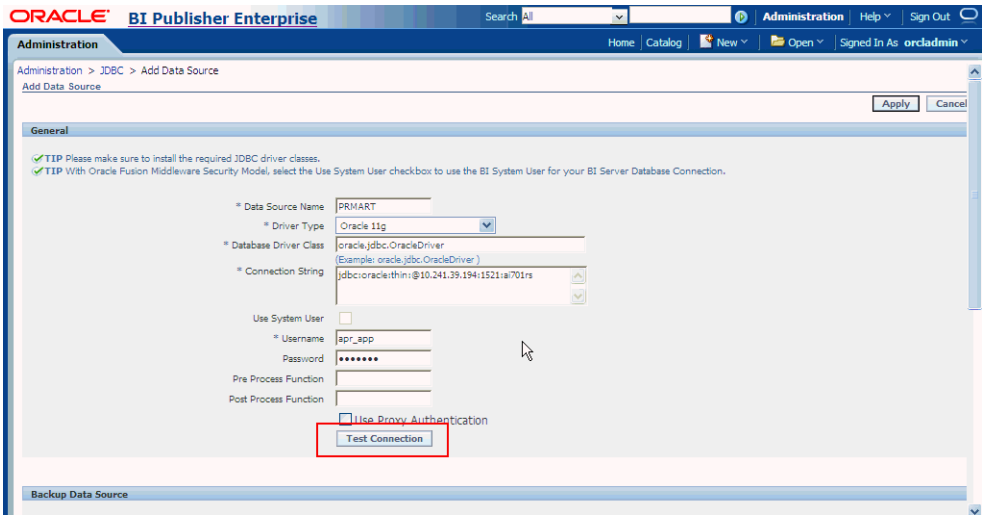
   b. Select the database from the **Driver Type** drop-down list. This auto-populates the **Database Driver Class** field.

   c. Enter the connection string in the **Connection String** field. You must enter all the details in lower case in this field.

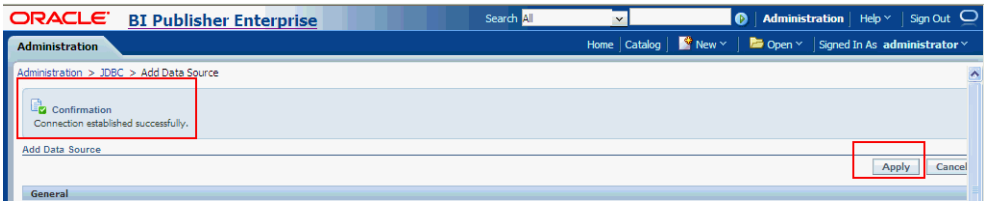
   d. Enter the username (Argus Insight application DB user, for example, apr_app) to connect to the database in the **Username** field.

   e. Enter the password for the user in the **Password** field.

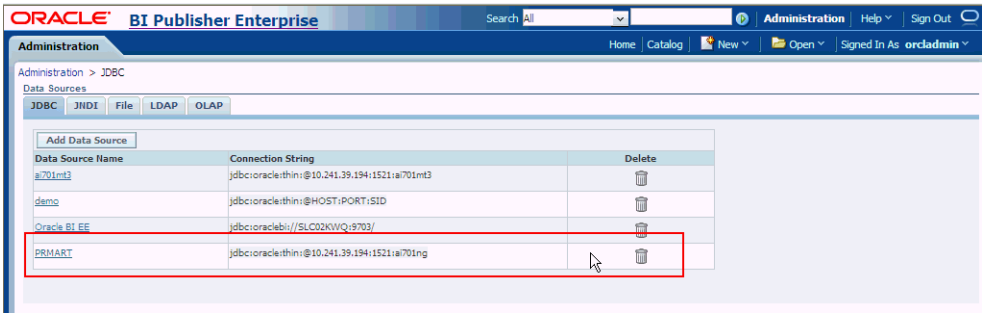
   f. Click **Test Connection** as shown in the following figure:



If successful, this displays a confirmation message, as shown in the following figure:



6. Click **Apply**. This displays the **PRMART** Data Source in the list of already existing data source names as shown in the following figure:



This successfully creates a connection between BIP and the database.

6.3 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

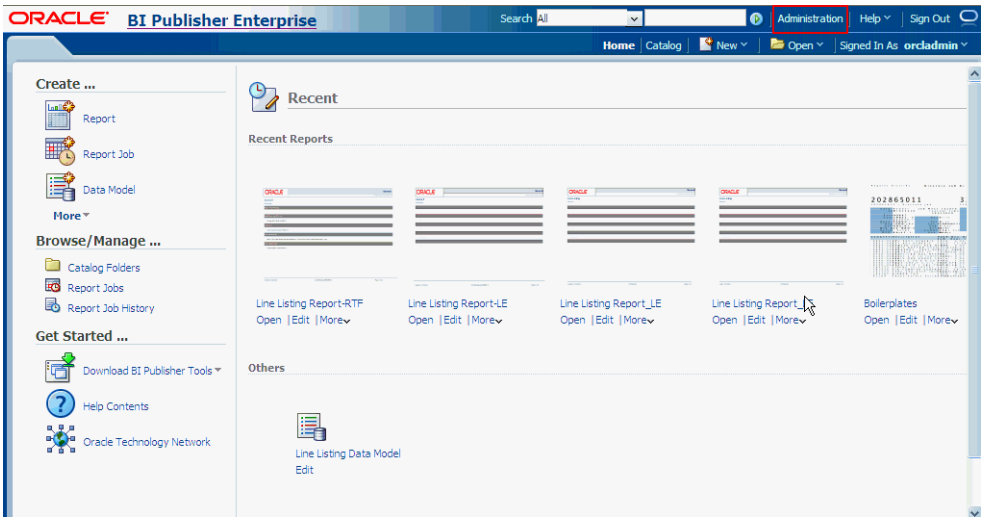
- Creating Roles, Adding Data Sources, and Assigning Roles

6.3.1 Configuring Server Settings

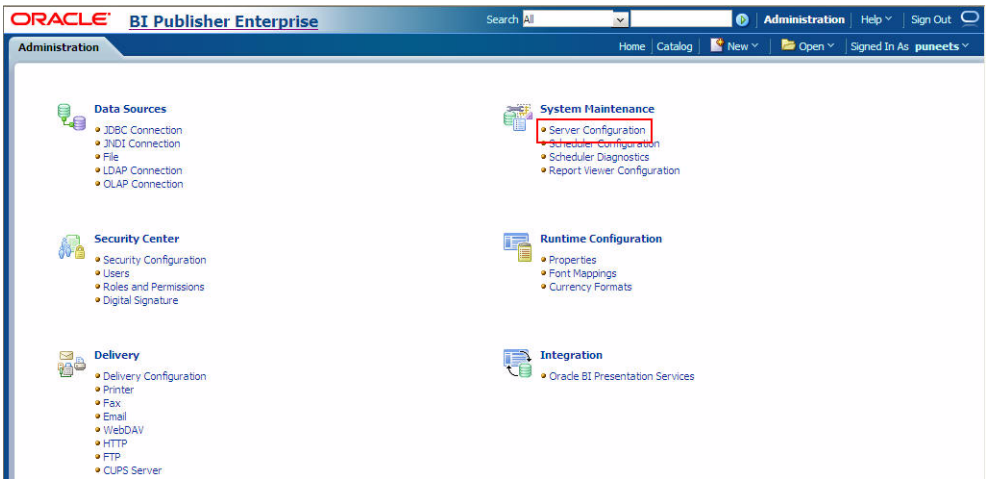
> **Note:** When using file systems such as NFS, Windows, or NAS for the repository, ensure that the file system is secured.

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:



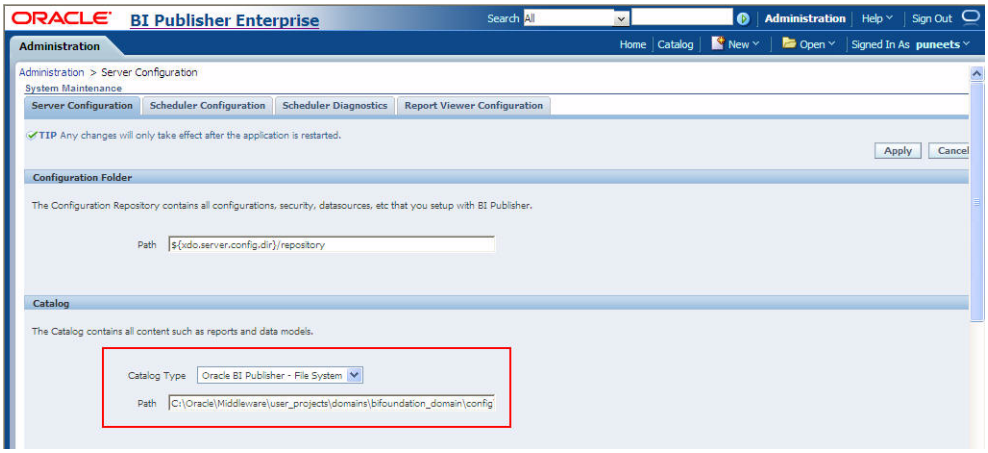
This displays the **Server Configuration** Screen.

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:



6. Click **Apply** to save the changes.
7. Restart the BI server.

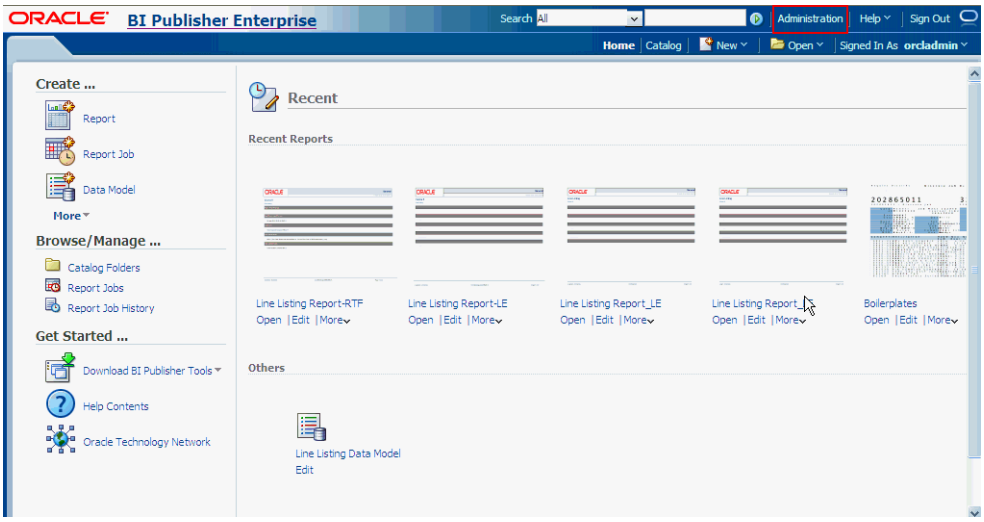
Note: Because the repository is in the file system, the case sensitivity of folder and Report Names is determined by the platform on which you run BI Publisher. For Windows-based environments, the repository object names are not case-sensitive. For UNIX-based environments, the Repository Object Names are case-sensitive.

For more information, refer to the Configuring Server Properties section of the Administrator's guide for Oracle BIP.

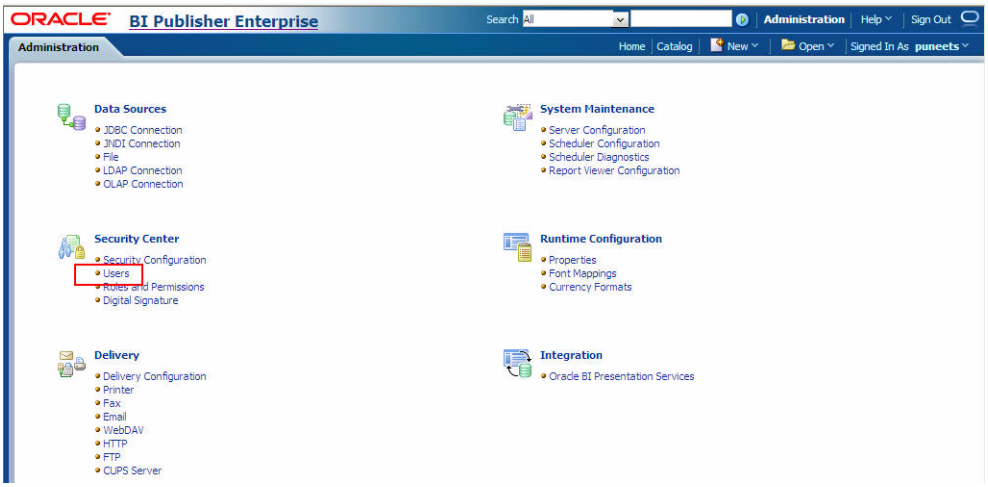
6.3.2 Creating Users and Assigning Roles to Users

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:

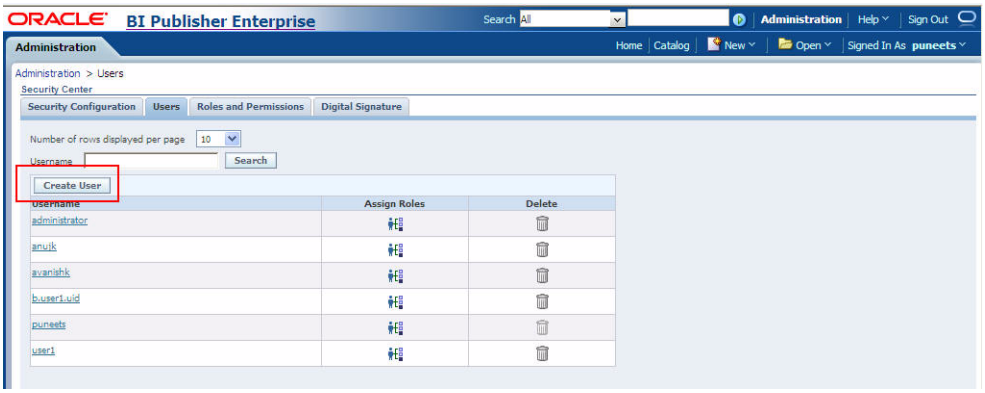


3. Click **Users** in the **Security Center** section as highlighted in the following figure:

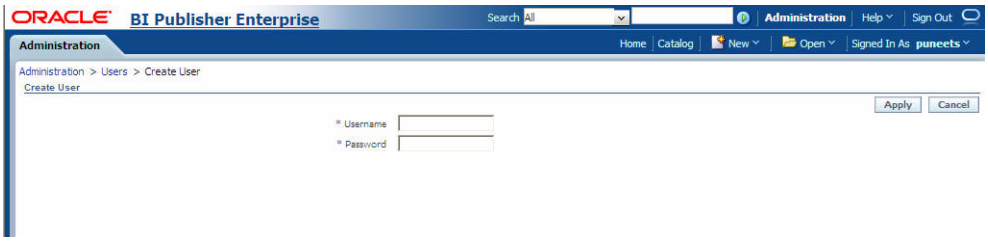


This displays the **Users** screen.

4. Click **Create User** as highlighted in the following figure:

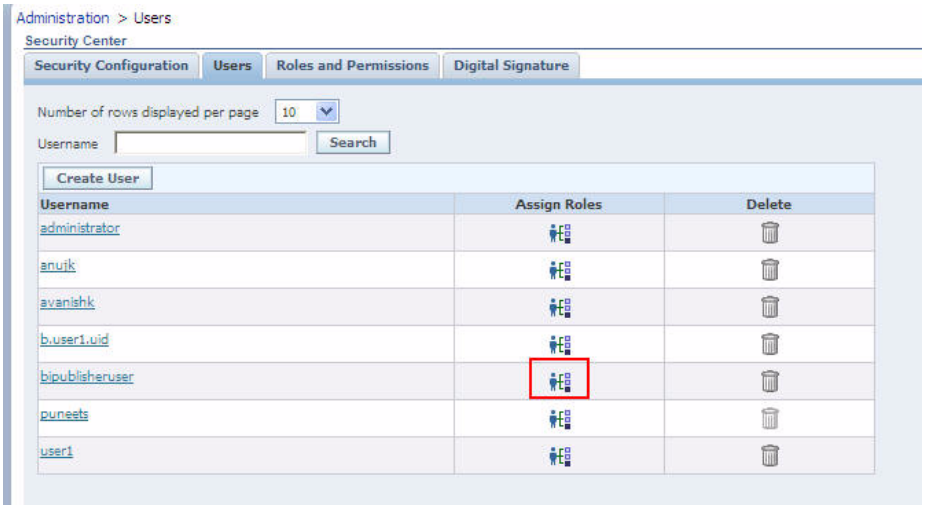


This displays the **Create User** Screen as shown in the following figure:

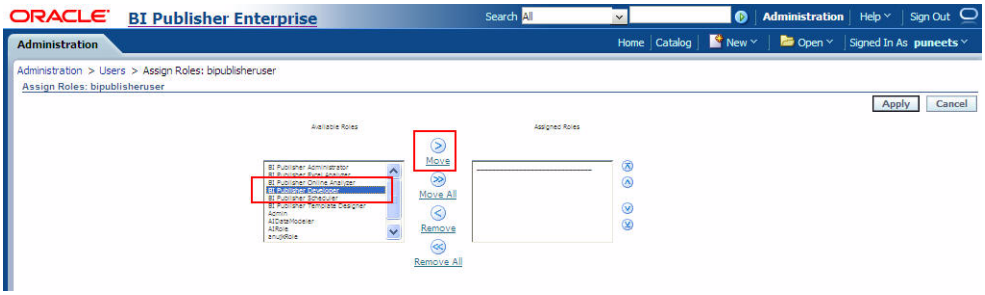


5. Enter the name of the user in the **Username** field.
6. Enter the password in the **Password** field.
7. Click **Apply**. The name of the user is displayed in the list of existing users.

   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:



   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:



10. Click **Apply**. This assigns the selected roles to the user.

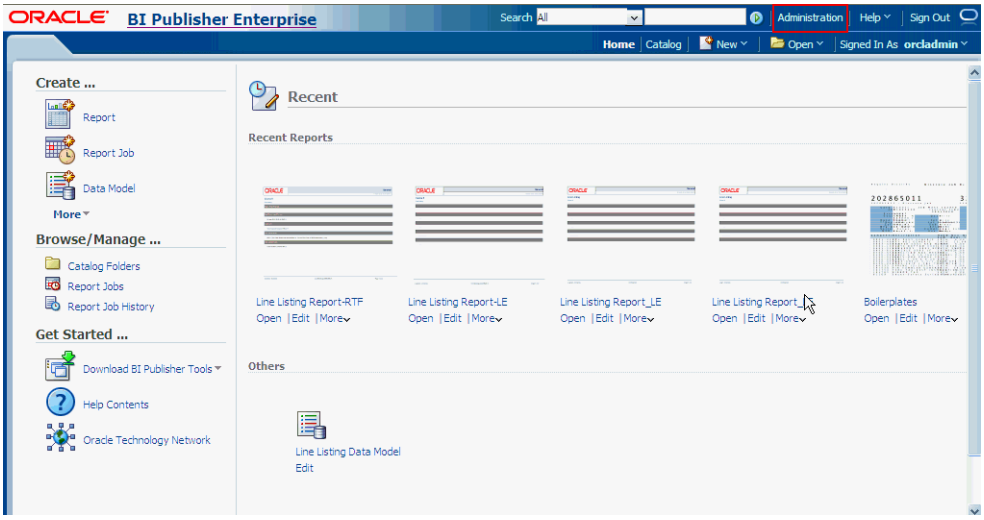
    For the list of users that you need to configure using BIP, refer to the Configuring BIP Users and Roles: Oracle Fusion Middleware Security Model section of this chapter.

6.3.3 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:

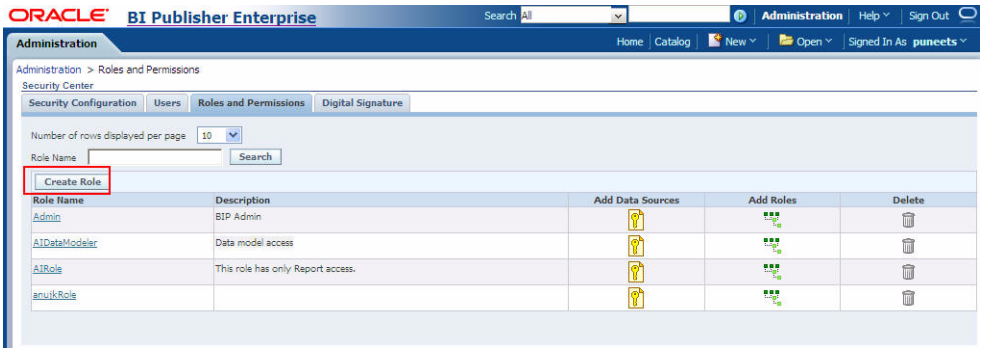
1. Log on to BIP using the administrator credentials. This displays the BIP Home Page.
2. Click **Administration** as highlighted in the following figure:



3. Click **Roles and Permissions** in the **Security Center** section as highlighted in the following figure:

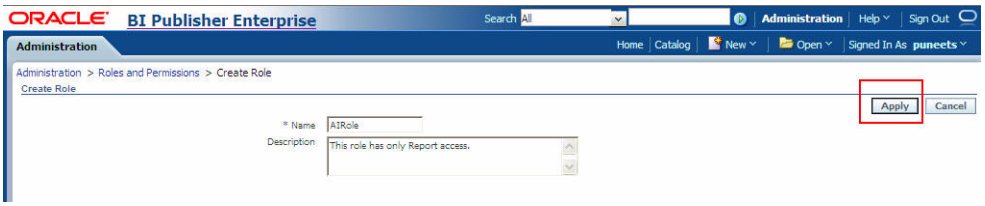
   This displays the **Roles and Permissions** Screen.

4. Click **Create Role** as shown in the following figure:



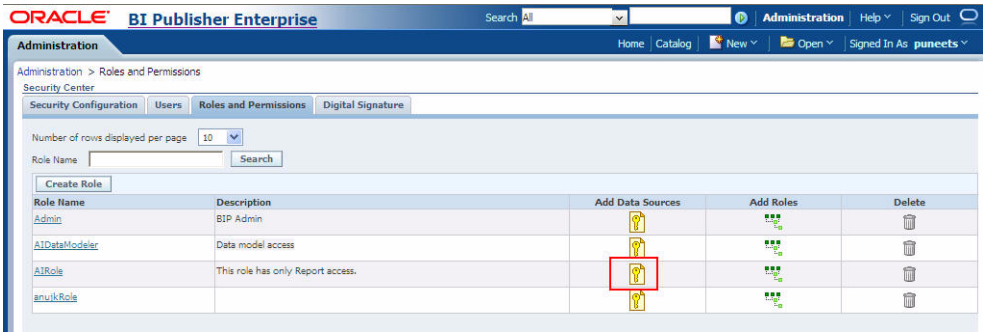
This displays the **Create Role** Screen.

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:



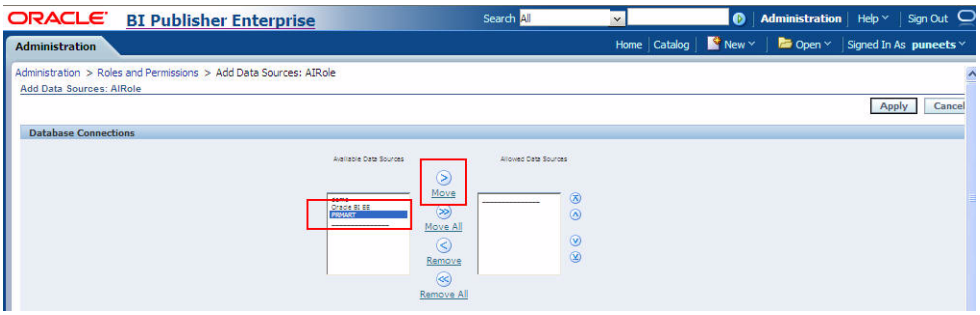
This displays the role in the list of existing roles on the **Roles and Permissions** Screen.

8. Click Add Data Sources Icon, corresponding to the role which you have just created, as depicted in the following figure:



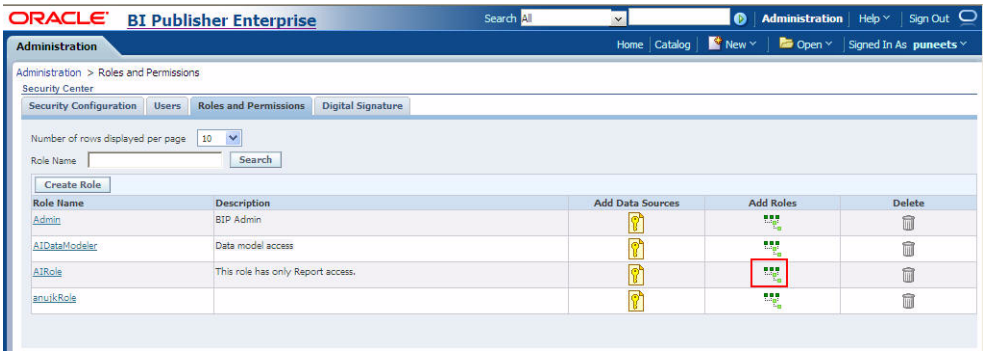
This displays the **Add Data Sources** Screen.

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:



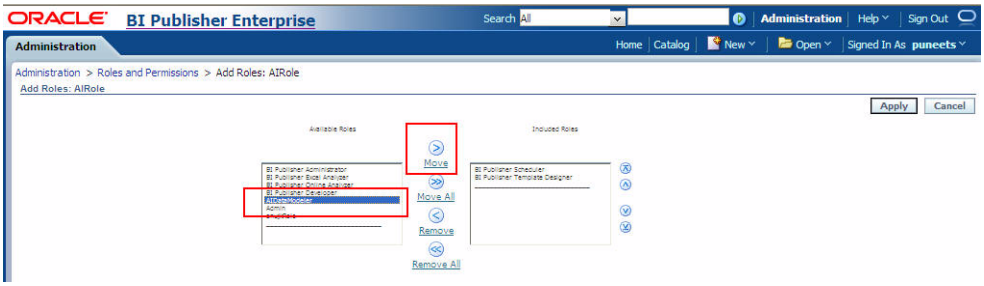
10. Click **Apply** to save the changes. This again displays the **Roles and Permissions** Screen. See Creating PRMART JDBC Connection section for the steps to create the JDBC connection.

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:



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.

6.4 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

6.4.1 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.

6.4.2 Creating Users and Assigning Roles to Users

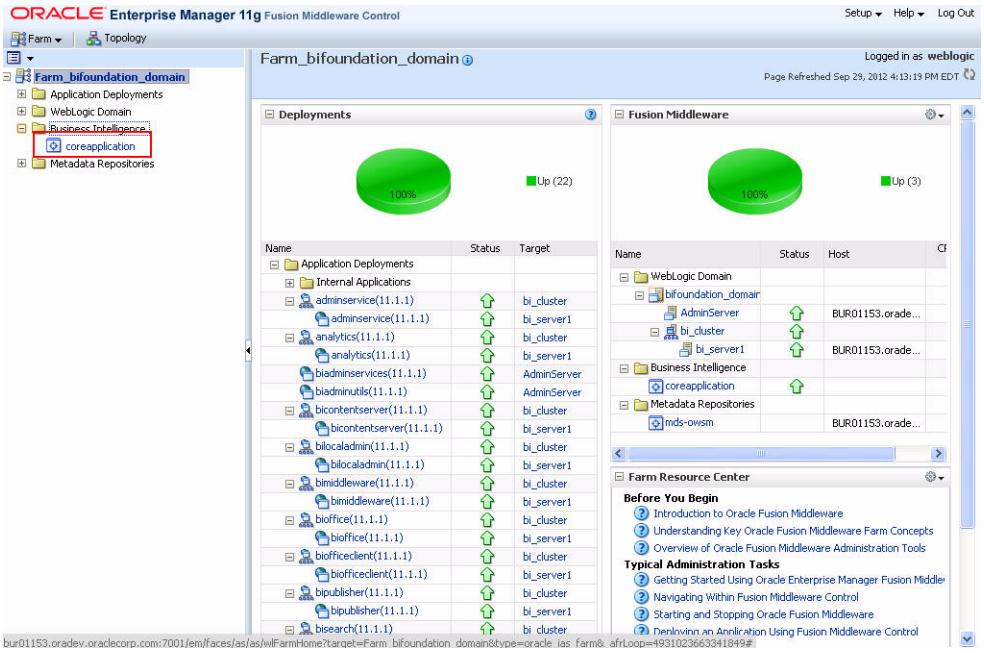
Creating users for LDAP or SSO users is done using the LDAP servers which is beyond the scope of this manual.

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.

6.4.3 Creating Roles, Adding Data Sources, and Assigning Roles in WebLogic Enterprise Manager

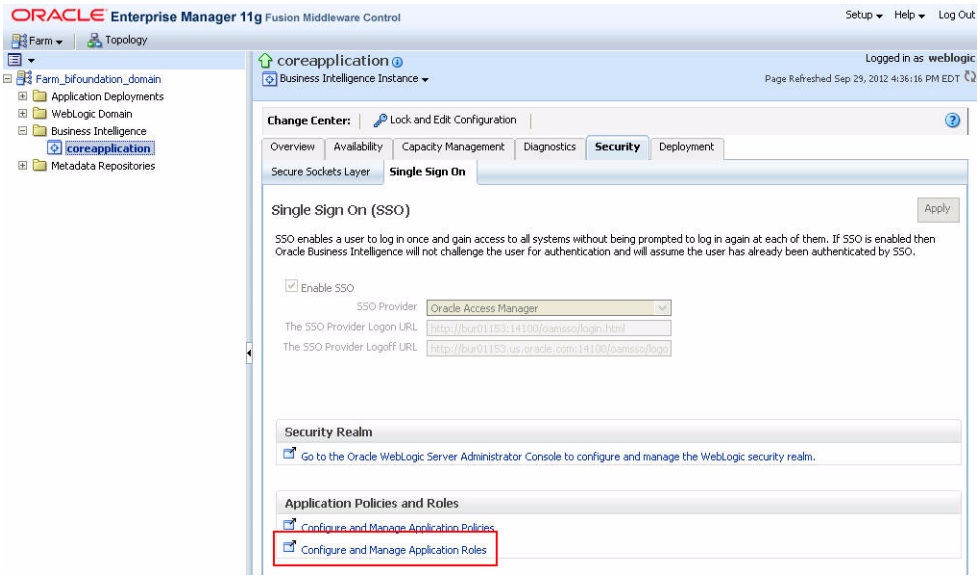
To create roles, add data sources, and assign roles in WebLogic Enterprise Manager, execute the following procedure:

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:



This displays the **coreapplication** Screen in the right pane.

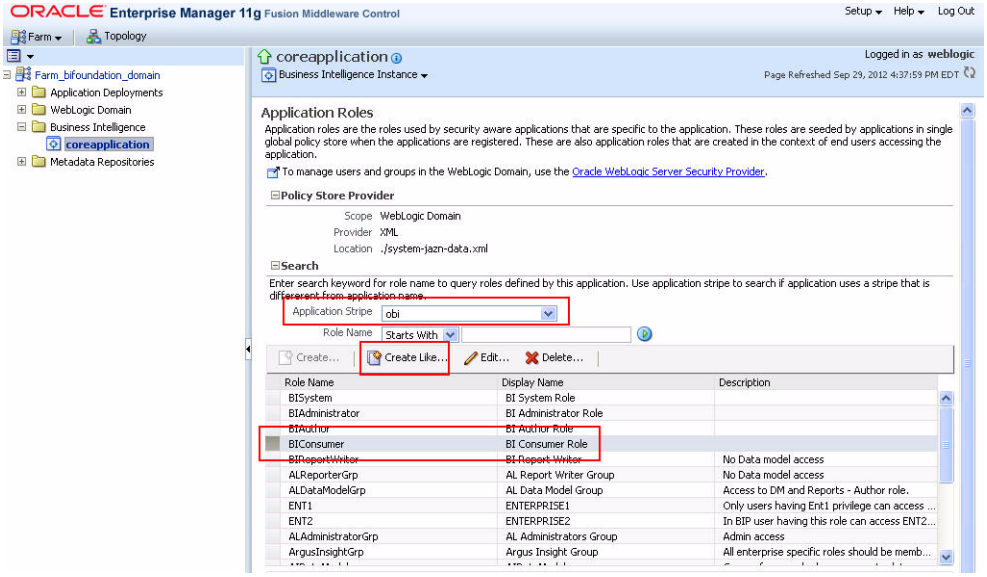
3. Click **Configure and Manage Application Roles** in the **Application Policies and Roles** section, as shown in the following figure:



This displays the **Application Roles** Screen.

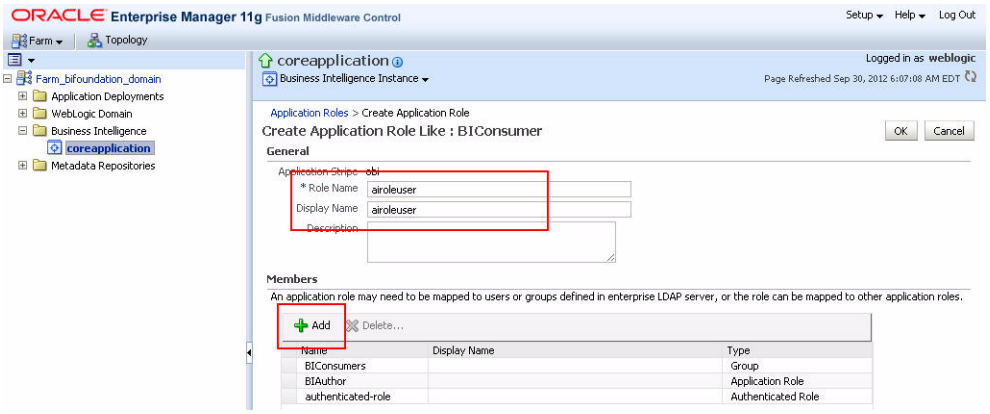
4. Select the required application stripe from the **Application Stripe** drop-down list.

5. Select any existing role (for example, **BIConsumer**) and click **Create Like**, as shown in the following figure:



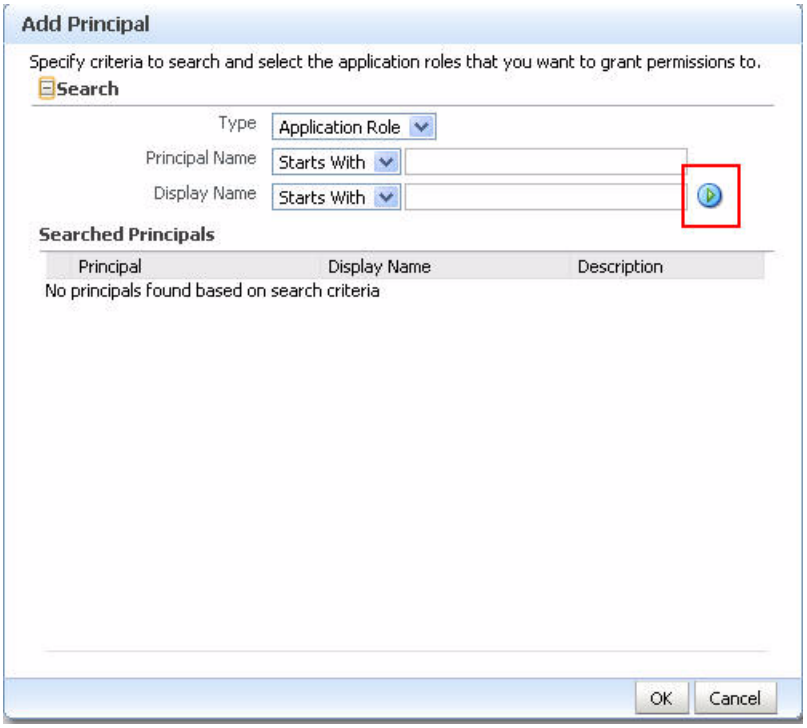
This displays the **Create Application Role** Screen.

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:

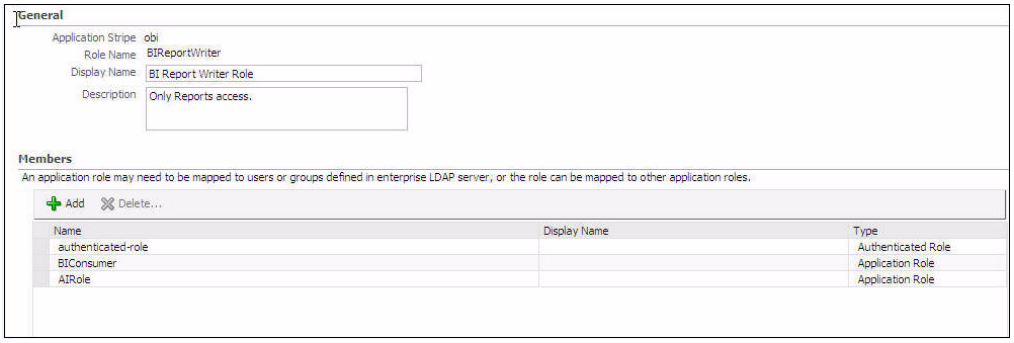


This displays the **Add Principal** Screen.

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:



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:

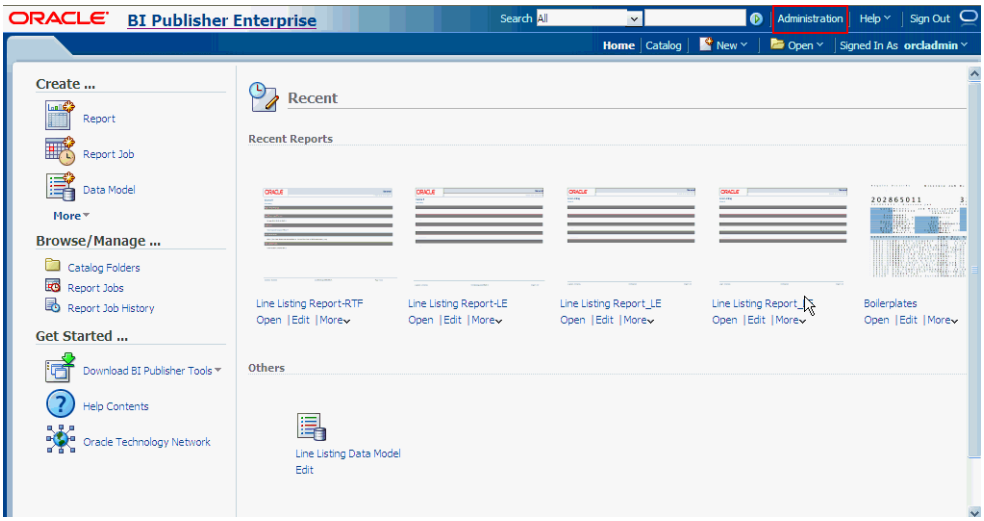


> **Note:** The **BIReportWriter** role must be added to the **BIReportWriter** application policy. You can refer to the Creating Application Policy section for the steps to create the application policy for the **BIReportWriter** role.

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.

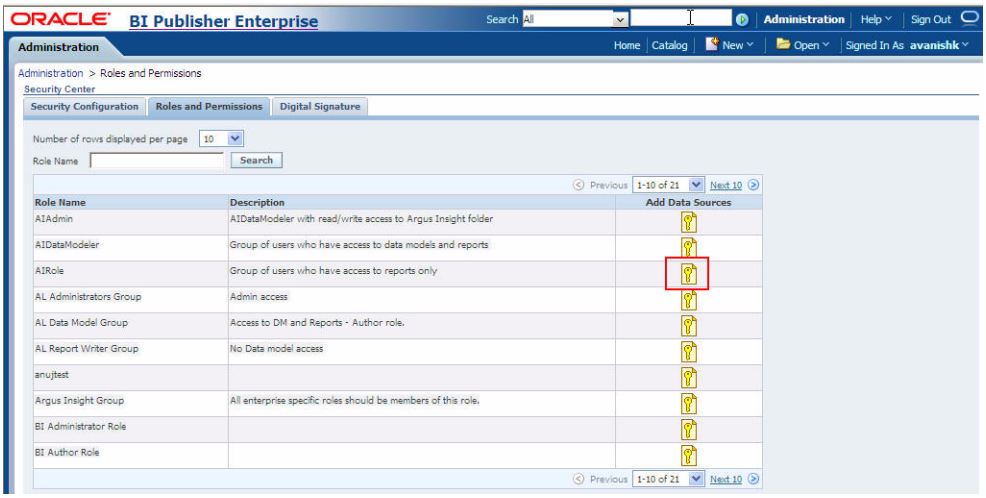
14. Click **Administration** as highlighted in the following figure:



15. Click **Roles and Permissions** in the **Security Center** section as highlighted in the following figure:

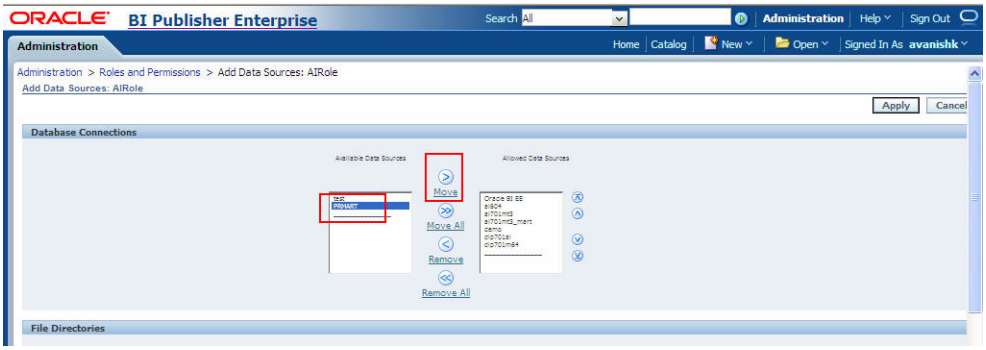
This displays the **Roles and Permissions** Screen. You can view the name of the new role which you have just created in the list of role names.

16. Click the Add Data Sources icon corresponding to the name of the new role, as depicted in the following figure:



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.

6.4.4 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.

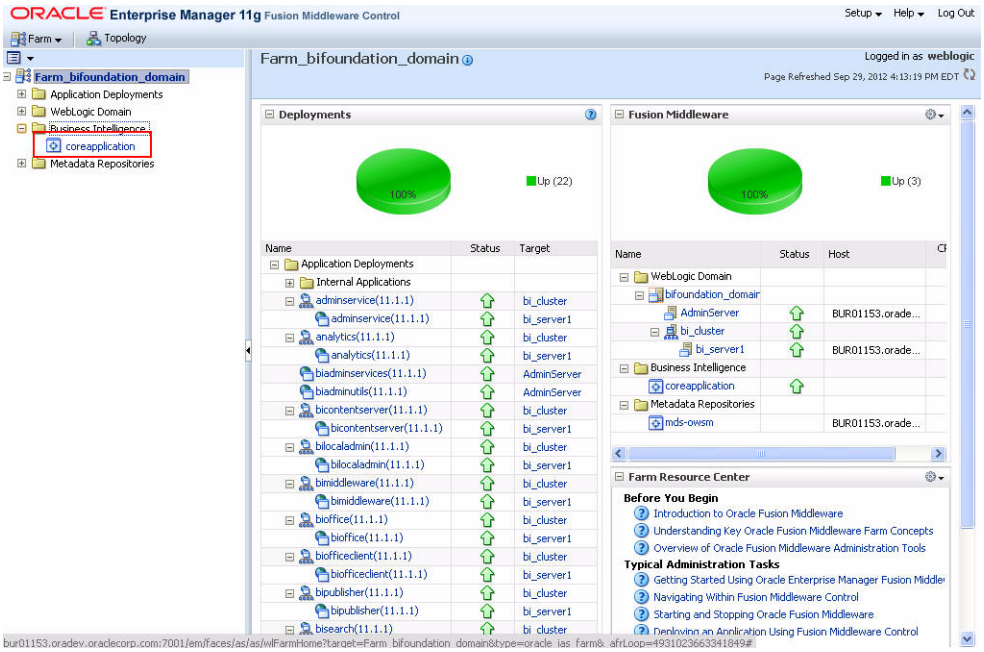
Before creating a BI Publisher policy, you must have created an empty role in the Enterprise Manager.

> **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:

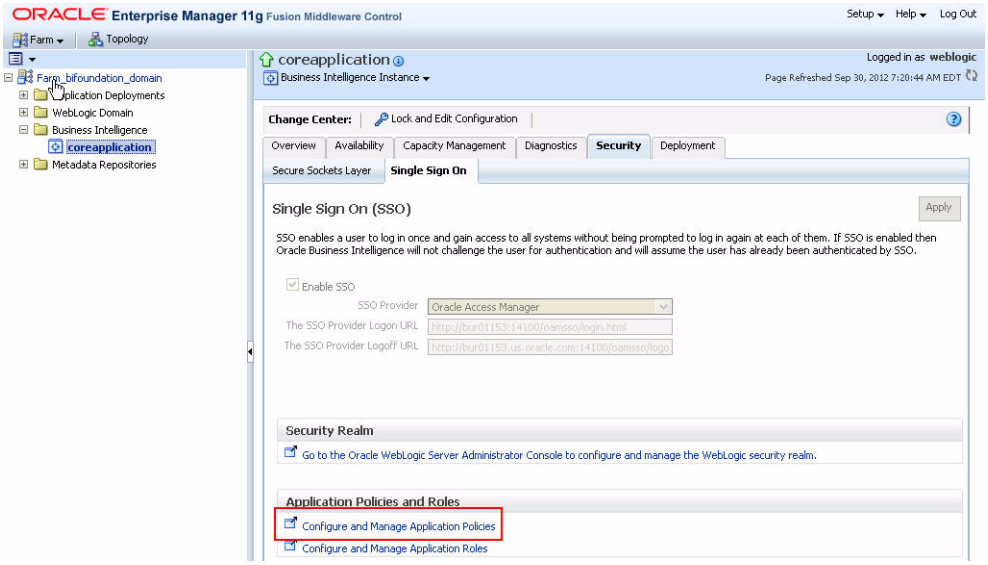
1. Log on to the Enterprise Manager. This displays the Enterprise Manager home page with a list of folders in the left pane.

2. Expand the **Business Intelligence** folder in the left pane and click **coreapplication**, as shown in the following figure:



This displays the **coreapplication** Screen in the right pane.

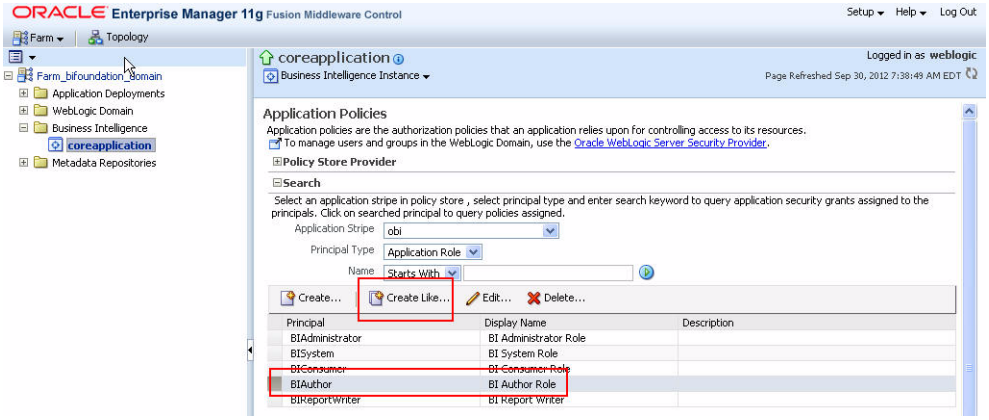
3. Click **Configure and Manage Application Policies** in the **Application Policies and Roles** section, as shown in the following figure:



This displays the **Application Policies** Screen.

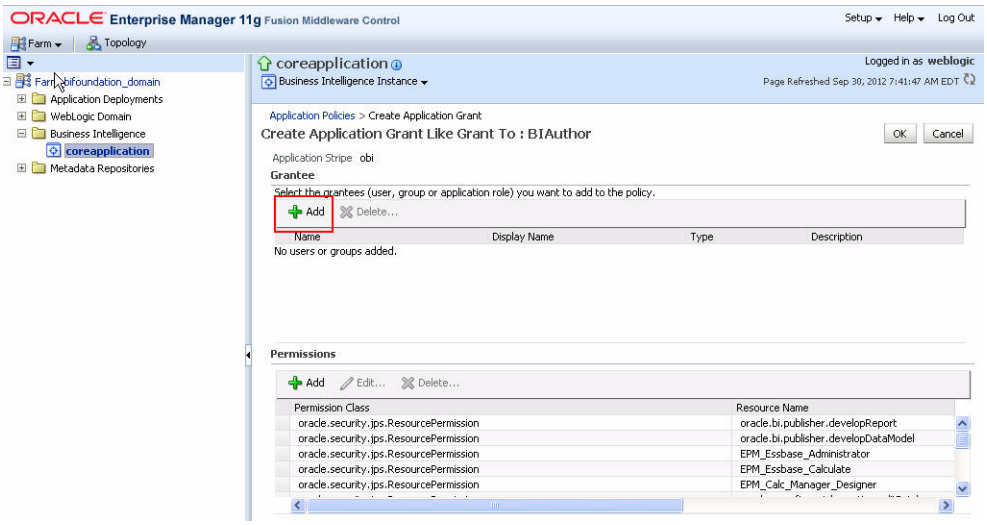
4. Select **obi** from the **Application Stripe** drop-down list.

5. Select the **BIAuthor** policy and click **Create Like** as shown in the following figure:



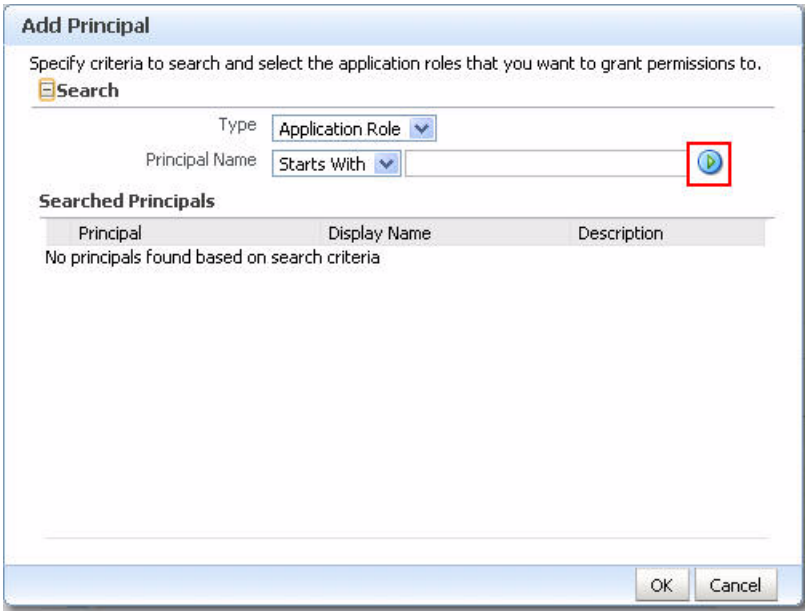
This displays the **Create Application Grant Like** Screen with the **Grantee** and **Permissions** sections.

6. Click **Add** in the **Grantee** section, as highlighted in the following figure:



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:



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.

6.5 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.

6.5.1 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.

6.5.2 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.

6.5.3 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.

6.5.4 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).

6.5.5 Configuring BIP Roles

The following table illustrates the Roles that you need to configure using BIP:

Table 6–1 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**

6.5.6 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 6–2 Folder Level Permissions

Folder	Roles to be added	Permissions
Argus Insight	AIAdminRole	Full access
Argus Insight > **General** > **Data Model**	AIDataModelerRole, AIRole	AIDataModelerRole - Full access 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 Enterprise Report Role -Read, Run, Schedule, and View report
Enterprise Specific Folder - Reports	Enterprise Report Role	Full access

6.6 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

6.6.1 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 6–3 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 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.

6.6.2 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 6–4 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. 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. In addition, this user has full access to the Argus Insight folder.
Enterprise Modeler Role	AIDataModelerRole (Created in 8.6.1 section) Enterprise Report Role	The user belonging to this role has access to: Argus Insight **Data Models** folder (Full access) Argus Insight **Reports** folder (Read, Run, Schedule, View report) Enterprise specific **Data Models** folder (Full access) Enterprise specific **Reports** folder (Read, Run, Schedule, View report)
Enterprise Modeler Role Users	Enterprise Modeler Role	This user has access to: Argus Insight **Data Models** folder (Full access) Argus Insight **Reports** folder (Read, Run, Schedule, View report) Enterprise specific **Data Models** folder (Full access) 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: Argus Insight **Data Models** folder (Read only) Argus Insight **Reports** folder (Full access) Enterprise specific **Data Models** folder (Read only) Enterprise specific **Reports** folder (Full access)
Enterprise Report Role Users	Enterprise Report Role	This user has access to: Argus Insight **Data Models** folder (Read only) Argus Insight **Reports** folder (Full access) Enterprise specific **Data Models** folder (Read only) 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.

7

Configuring the BusinessObjects XI Environment

This chapter describes how to configure the BusinessObjects XI (BOXI) environment. You must configure the BusinessObjects XI environment in the order specified in this guide.

This chapter includes the following topics:

- Checking Requirements
- Configuring the BusinessObjects Server
- Configuring the Argus Insight Web Server

If you are using Cognos 10 instead of BusinessObjects XI, see Chapter 8 for information about configuring the Cognos 10 environment for Argus Insight.

7.1 Checking Requirements

Before 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.

> **Note:** Argus Insight 7.0.3 does not support multi-tenancy with its reporting framework for BusinessObjects. There are no restrictions in the multi-tenant Argus Insight database for the functioning of BusinessObjects. The users can enhance the Argus Insight Reporting framework or tweak BusinessObjects to support multi-tenancy in BO reports.

7.2 Configuring the BusinessObjects Server

The sections describes the following tasks that you must complete to configure the BusinessObjects Server:

- Copying the PRMART TNS Entry

7.2.1 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.

> **Note:** PRMART TNS entry must be mentioned in the TNSNAMES.ora file for both 32-bit and 64-bit Oracle Client.

If both applications use the same server and Oracle client, no modifications to the TNSNAMES.ora file are required.

7.3 Configuring the Argus Insight Web Server

The following profile switches are available only when the BO WEB URL profile switch is configured and Legacy Report profile switch is set to 1:

- Holiday Schedule Management
- Product Designated Medical Event Configuration
- Measurable Suppliers
- Site Configuration
- Acceptable Delay Justification Configuration

To configure these profile switches, refer to Argus Insight 7.0.2 Installation Guide.

8

Configuring the Cognos 10 Environment

This chapter describes how to configure the Cognos 10 environment. You must configure the Cognos 10 environment in the order specified in this guide.

This chapter includes the following topic:

- Setting Up Cognos Server and Configuration for New Installation

Before 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."

8.1 Setting Up Cognos Server and Configuration for New Installation

This section describes how to set up Cognos Server and configure your environment for a new installation of Argus Insight.

This section comprises the following sub-section:

- Configuring IIS 7.0 on the Cognos 10 Server
- Configuring the Java Database Components
- Configuring Custom Java Authentication
- Configuring the Cognos 10 Environment
- Creating Cognos Data Source (PRMART)
- Configuring Cognos Security
- Configuring Roles and Permissions

8.1.1 Configuring IIS 7.0 on the Cognos 10 Server

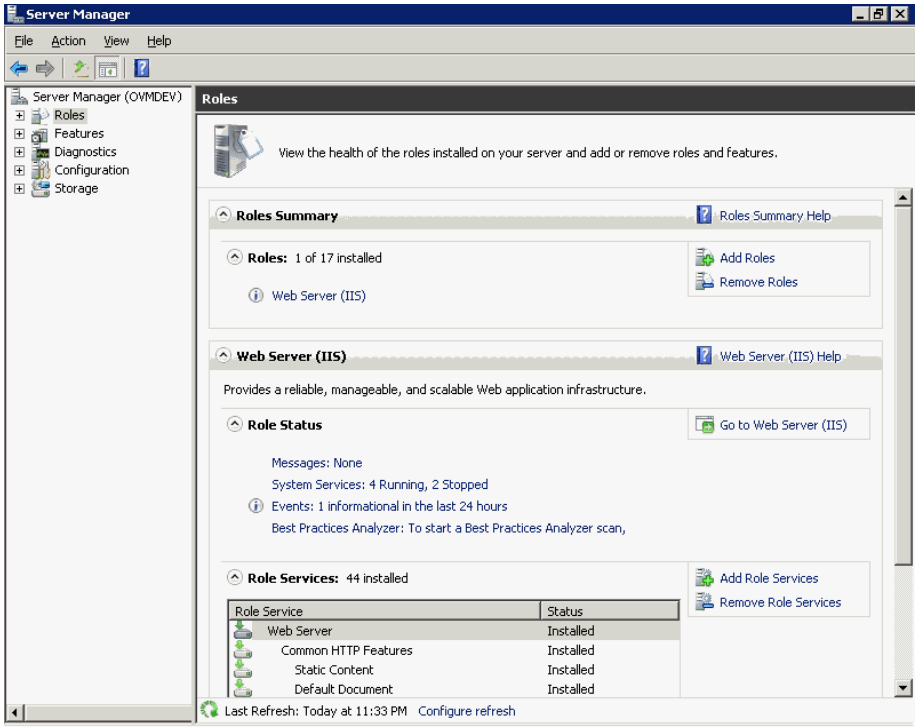
This section describes the following tasks that you must complete to configure Internet Information Services 7.0 (IIS 7.0) on the Cognos 10 Server:

- Checking that CGI or ISAPI Is Enabled in IIS
- Creating the Cognos 10 Virtual Directories
- Editing ISAPI or CGI Extensions
- Adding the Module Mapping
- Editing the Module Mapping
- Allowing CGI Application to Use Execute

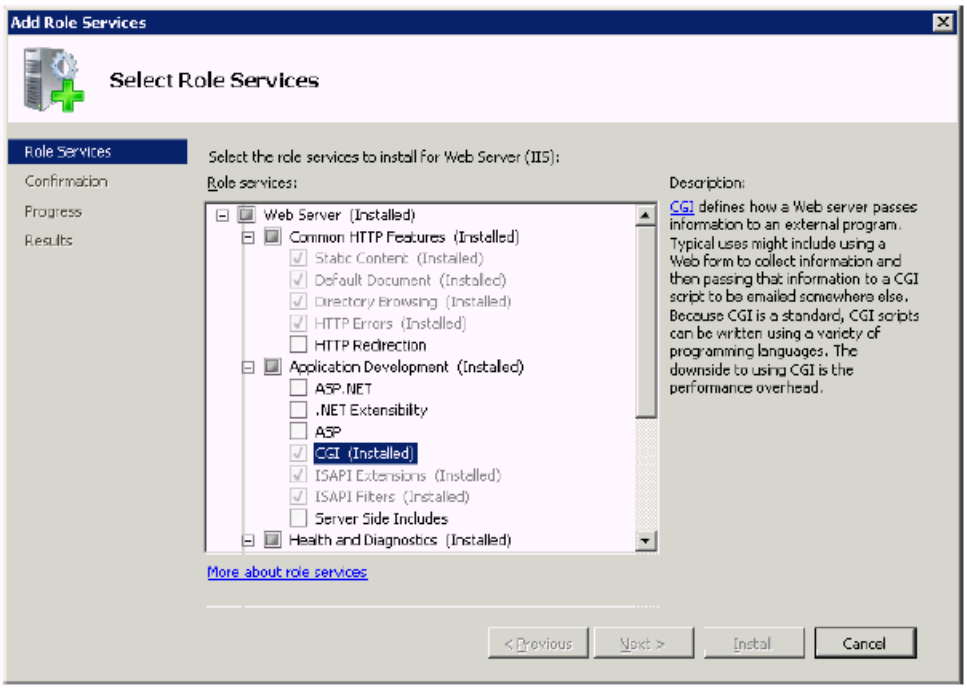
8.1.1.1 Checking that CGI or ISAPI Is Enabled in IIS

To check that CGI or ISAPI is enabled in IIS:

1. Click **Start.**
2. Navigate to **Administrative Tools** and select **Server Manager.** The Server Manager window opens.



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

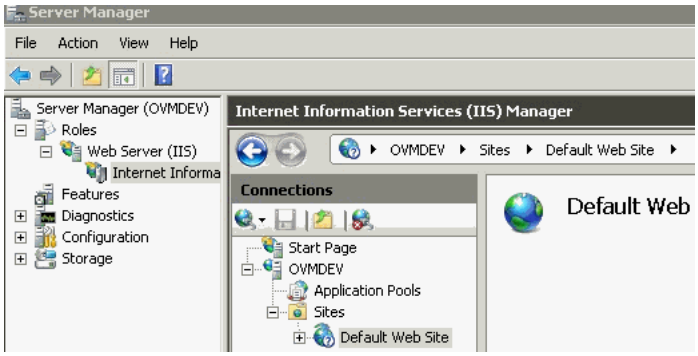


4. Expand **Application Development (Installed).**
5. Verify that the CGI and ISAPI Extensions are listed as **(Installed).**
   - If these role services are not installed, select the appropriate check box and then click **Install.** Follow the instructions on the screen to complete the installation.
   - If these role services are already installed, click **Cancel.** The system returns to the Server Manager window.

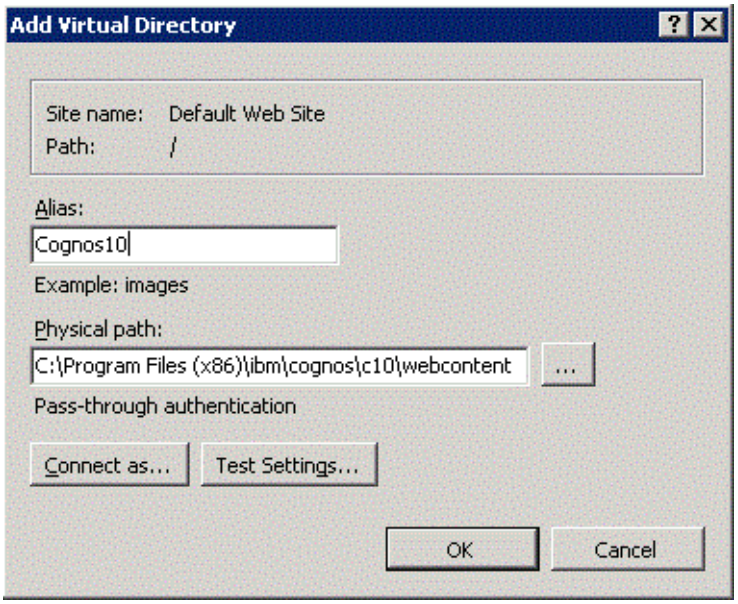
8.1.1.2 Creating the Cognos 10 Virtual Directories

To create the Cognos 10 virtual directories:

1. Navigate to **Roles, Web Server (IIS),** and select **Internet Information Services (IIS) Manager.**
2. 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.



   a. In the **Alias** field, enter **Cognos 10.**

b. In the **Physical path** field, enter the complete path to the Cognos 10 Web content directory. The default path is:

drive:\Program Files\ibm\cognos\c10\webcontent

c. Click **OK.**

5. Right-click your newly-created Cognos 10 virtual directory and select **Add Virtual Directory.** The Add Virtual Directory dialog box opens.

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

b. In the **Physical path** field, enter the complete path to the Cognos 10 cgi-bin directory. The default path is:

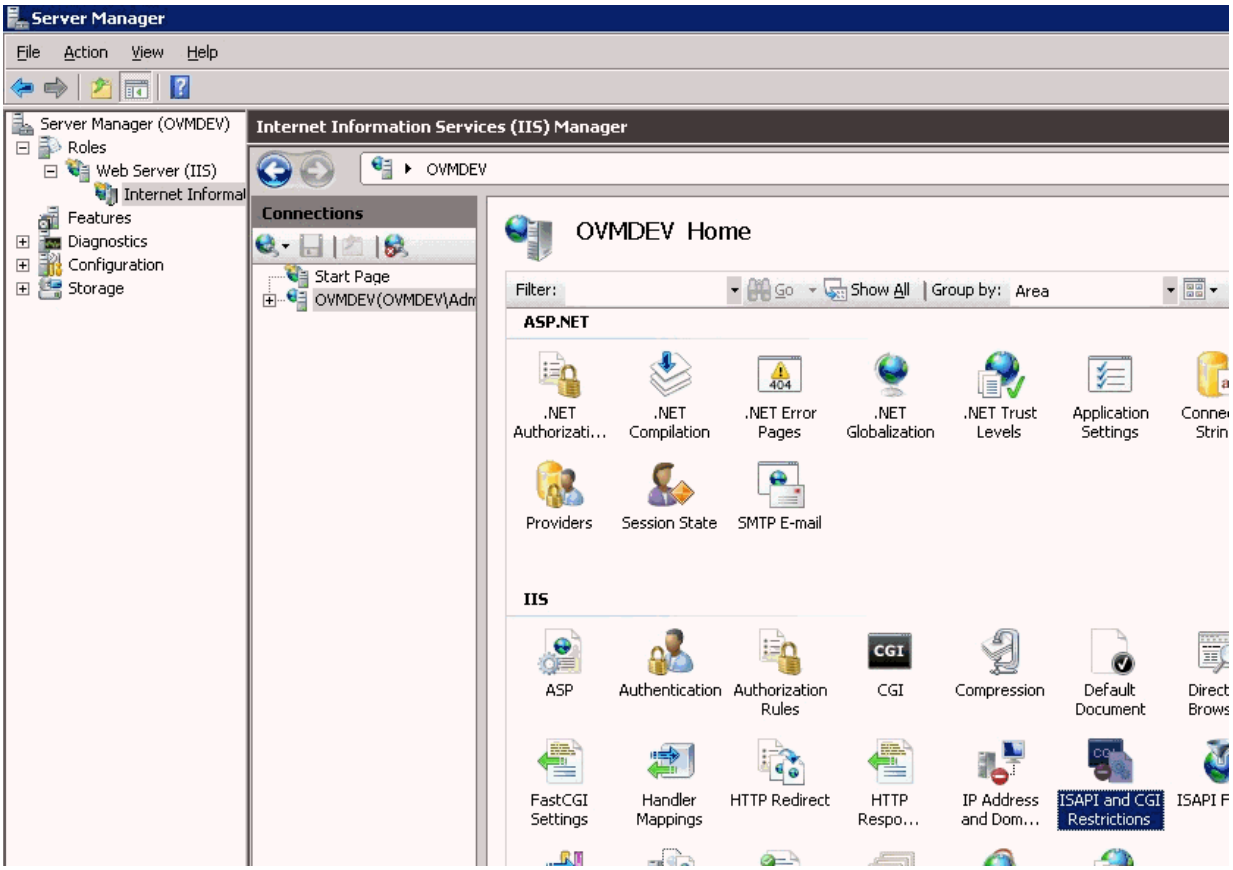
drive:\Program Files\ibm\cognos\c10\cgi-bin

c. Click **OK.**

8.1.1.3 Editing ISAPI or CGI Extensions

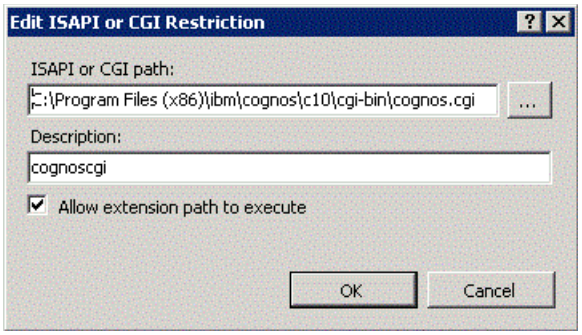
To edit the ISAPI or CGI extensions:

1. 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.



a. In the **ISAPI or CGI path** field, enter the path to either the cognos.cgi file or the cognosisapi.dll file depending on which one you will use.

Note: For Argus Insight, Oracle recommends that you use cognos.cgi. In addition, you may need to surround the path in double quotes if it contains any spaces.

The default path for each file is as follows:

drive:\Program Files\ibm\cognos\c10\cgi-bin\cognosisapi.dll

drive:\Program Files\ibm\cognos\c10\cgi-bin\cognos.cgi

b. Select 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.

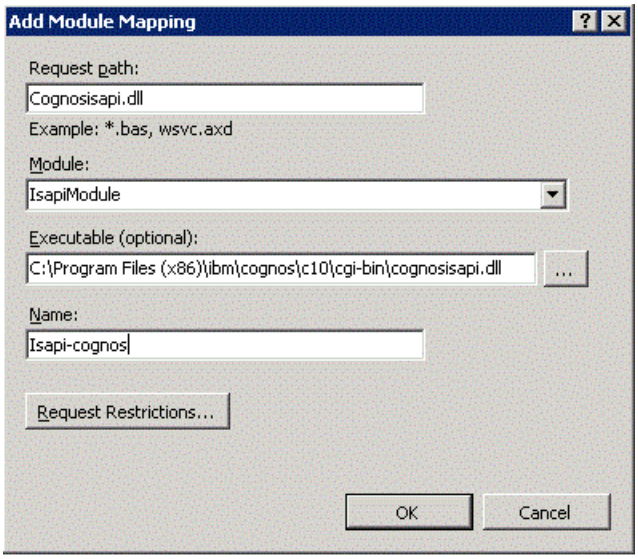
4. Select the **Allow unspecified CGI Modules** check box.
5. Click **OK.**

8.1.1.4 Adding the Module Mapping

To add the module mapping:

1. Open the Internet Information Services (IIS) Manager.
2. Expand the virtual directory folder and click 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.



   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.

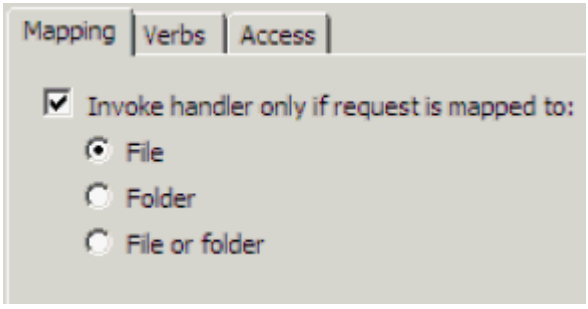
      If you are using an ISAPI Module, you must enter the complete path to the cognosisapi.dll. You can click the ellipsis icon to browse to the file location.

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

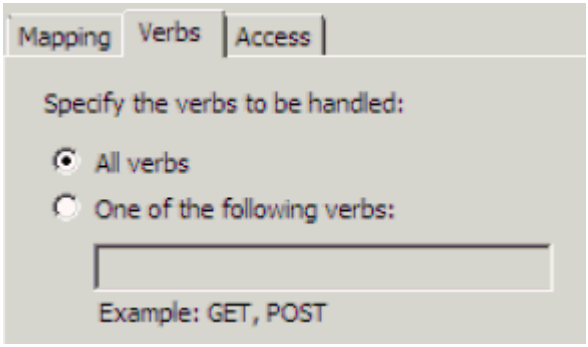
   d. In the **Name** field, enter a realistic name for this mapping. For example, ISAPI-Cognos.

5. Click **Request Restrictions.**

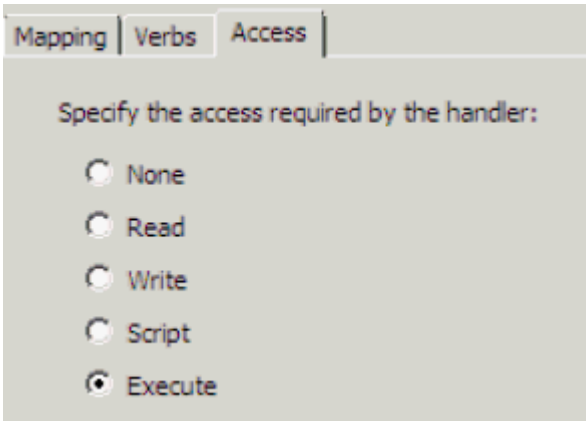
   a. Click the **Mapping** tab, and select **Invoke handler only if request is mapped to: File.**



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



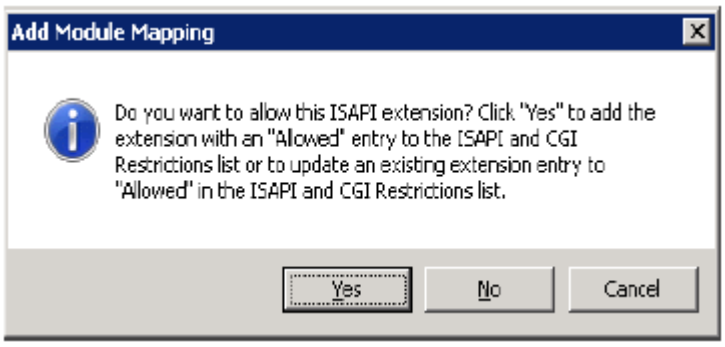
c. Click the **Access** tab, and select **Specify the access required by the handler: Execute.**



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 8.1.1.3, "Editing ISAPI or CGI Extensions," the system may display the following message:



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

8.1.1.5 Editing the Module Mapping

For Cognos Administration to function properly, you must manually edit the directive that you added to the IIS configuration file in the previous step (see Section 8.1.1.4, "Adding the Module Mapping").

To edit the module mapping:

1. Navigate to the following folder:

   COGNOS_HOME/c10/cgi-bin

   Note: Ensure that you have access permissions on the cgi-bin folder so you can save the changes you make to the web.config file.

2. Open the **web.config** file for editing.
3. Locate the appropriate **add name** statement in the web.config file 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\ibm\Cognos\C10\
   cgi-bin\cognosisapi.dll" resourceType="Unspecified"
   requireAccess="Execute" preCondition="bitness32" />
   ```

4. Add **allowPathInfo="true"** to the end of the statement.

   For CGI:

   ```
   <add name="CGI-cognos" path="*.cgi" verb="*" modules="CgiModule"
   resourceType="Unspecified" allowPathInfo="true" />
   ```

   For ISAPI:

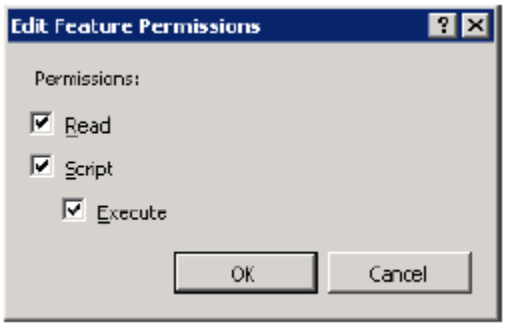
   ```
   <add name="ISAPI-Cognos" path="cognosisapi.dll" verb="*"
   modules="IsapiModule" scriptProcessor="E:\Program Files\ibm\Cognos\C10\
   cgi-bin\cognosisapi.dll" resourceType="Unspecified"
   requireAccess="Execute" preCondition="bitness32" allowPathInfo="true"/>
   ```

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

8.1.1.6 Allowing CGI Application to Use Execute

To allow the CGI application to use execute:

1. Open the Internet Information Services (IIS) Manager.
2. Expand the virtual directory folder and click the **cgi-bin** 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.



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

8.1.2 Configuring the Java Database Components

To configure the Java Database Components (JDBC) in the Cognos 10 environment:

1. Navigate to the following Oracle installation path:

   Oracle_Installation_Path\product*Oracle_Version*\client_1\sqldeveloper\jdbc\lib
2. Copy the **ojdbc5.jar** file to the following location on the Cognos 10 environment:

   Cognos_Installation_Path\c10\webapps\p2pd\web-inf\lib

8.1.3 Configuring Custom Java Authentication

This section comprises the following sub-sections:

- Configuring Custom Java Authentication for Windows
- Configuring Custom Java Authentication for Linux

8.1.3.1 Configuring Custom Java Authentication for Windows

1. Go to IBM Cognos Administration and stop the Cognos services.
2. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\ JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\webapps\p2pd\WEB-INF\lib
3. Copy the **JDBC_Config_PowerReports.properties** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\ JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\Configuration
4. Define the configuration parameters:
   a. Navigate to the following folder:

      Cognos_10_Install_Path\ c10\Configuration
   b. Open the **JDBC_Config_PowerReports.properties** file for editing.

c. Modify the existing values of the following parameters only if the database changed from the 7.0 database:

Parameter	Value to Enter
Server	Enter the IP address or the name of the Database Server.
SID	Enter the instance/service name of the Argus Insight data mart.
Port	Enter the database port number.

d. Save and close the file.

5. Copy **AI.ini** and **ArgusSecureKey.ini** from the following location:

   \\<Argus_Insight_Server>\Windows

   To the following location:

   \\Cognos_10_Install_Path\C10\configuration

6. Navigate to the following folder:

   Program Files\ibm\cognos\c10\bin\jre\6.0\lib\security

7. Backup the following two JAR files:
   - local_policy.jar
   - US_export_policy.jar

8. 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.

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

    Program Files\ibm\cognos\c10\bin\jre\6.0\lib\security

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

8.1.3.2 Configuring Custom Java Authentication for Linux

To configure custom Java authentication:

1. Go to IBM Cognos Administration and stop the Cognos services.
2. Copy the **CAM_AAA_JDBC_PowerReports.jar** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\ JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\webapps\p2pd\WEB-INF\lib
3. Copy the **JDBC_Config_PowerReports.properties** file from the following location:

   \\Argus_Insight_Server\Argus_Insight_Install_Path\java Autherntication\ JDBC_PowerReport

   To the following location on the Cognos 10 Server:

   \\Cognos_10_Install_Path\ c10\Configuration
4. Define the configuration parameters:
   a. Navigate to the following folder:

      Cognos_10_Install_Path\ c10\Configuration
   b. Open the **JDBC_Config_PowerReports.properties** file for editing.
   c. Modify the existing values of the following parameters only if the database changed from the 7.0 database:

Parameter	Value to Enter
Server	Enter the IP address or the name of the Database Server.
SID	Enter the instance/service name of the Argus Insight data mart.
Port	Enter the database port number.

   d. Save and close the file.
5. Copy **AI.ini** and **ArgusSecureKey.ini** from the following location:

   \\<Argus_Insight_Server>\Windows

   To the following location:

   \\Cognos_10_Install_Path\C10\configuration
6. Navigate to the following folder:

   JAVA_HOME\jre\6.0\lib\security
7. Backup the following two JAR files:
   - local_policy.jar
   - US_export_policy.jar
8. Go to the following URL:

   http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html
9. Download the following two JAR files in the extract folder:
   - local_policy.jar
   - US_export_policy.jar

10. Copy those jar files into the following folder:

    JAVA_HOME\jre\6.0\lib\security

11. Click **Yes**, if the **Replace Files** dialog box is displayed.

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

8.1.4 Configuring the Cognos 10 Environment

This section describes the following tasks that you must complete to configure the Cognos 10 environment:

- Opening the IBM Cognos 10 Configuration Window
- Setting the Security Properties for Cognos 10
- Setting the Data Access Properties for Cognos 10
- Creating the Namespace for Argus Insight Authentication
- Saving Your Configuration and Starting the Cognos 10 Service

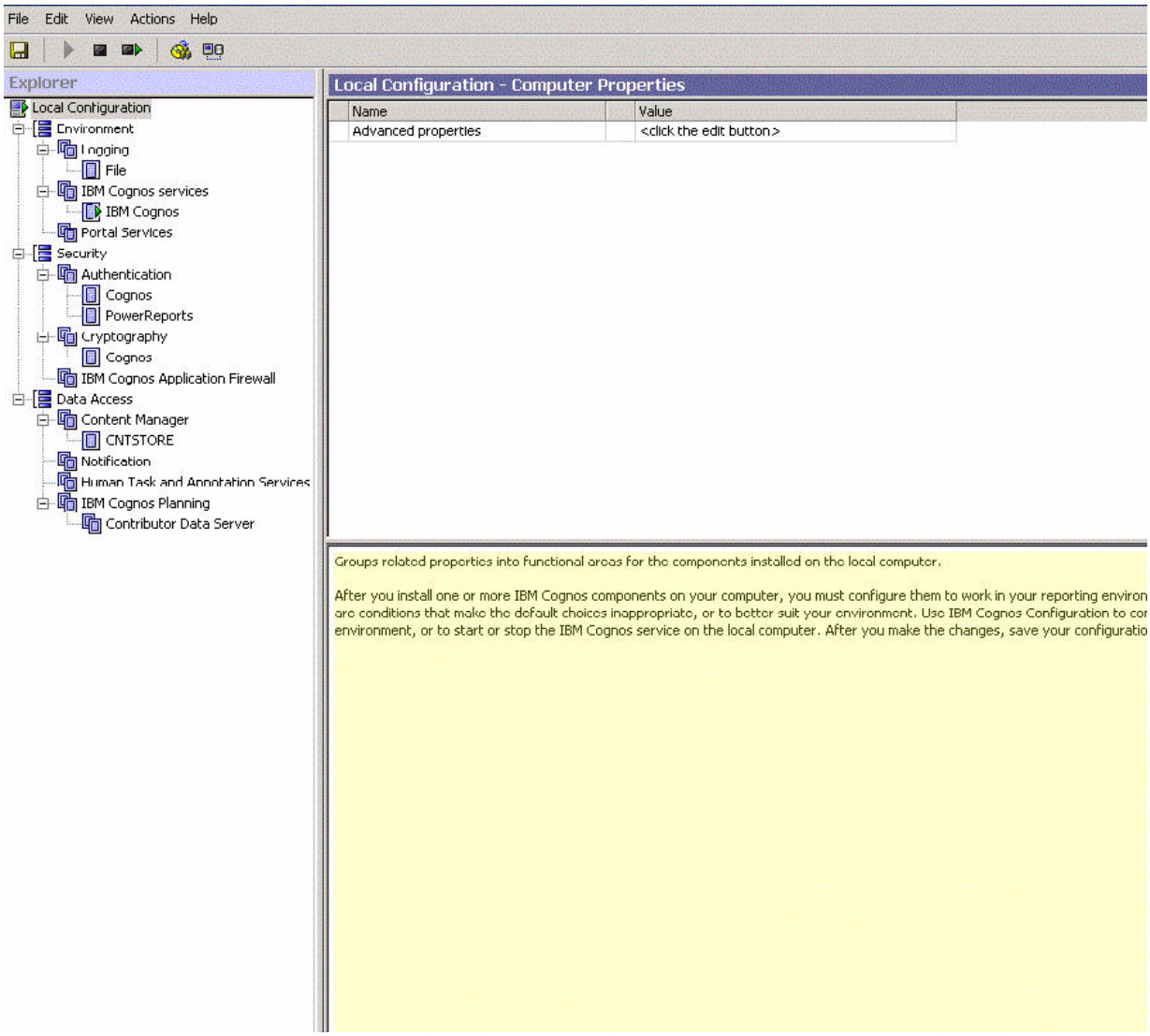
8.1.4.1 Opening the IBM Cognos 10 Configuration Window

You use the options in the IBM Cognos 10 Configuration window to define environment group and logging properties, security properties, and data access properties.

To open the IBM Cognos 10 Configuration window:

1. Click **Start.**

2. Navigate to **All Programs, IBM Cognos 10,** and then select **IBM Cognos Configuration.** The IBM Cognos Configuration window opens.

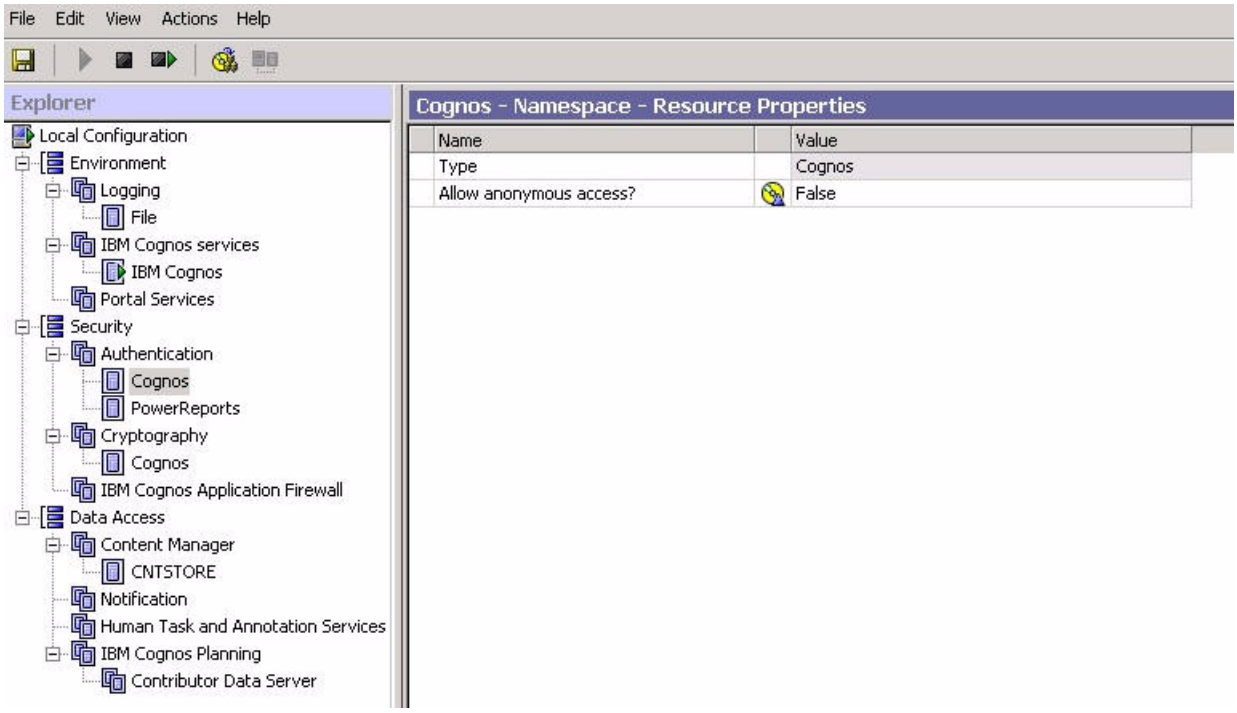


Note: The windows displayed during the Cognos 10 configuration are labeled either IBM Cognos 10 or Cognos 10. Both labels refer to the same Cognos configuration.

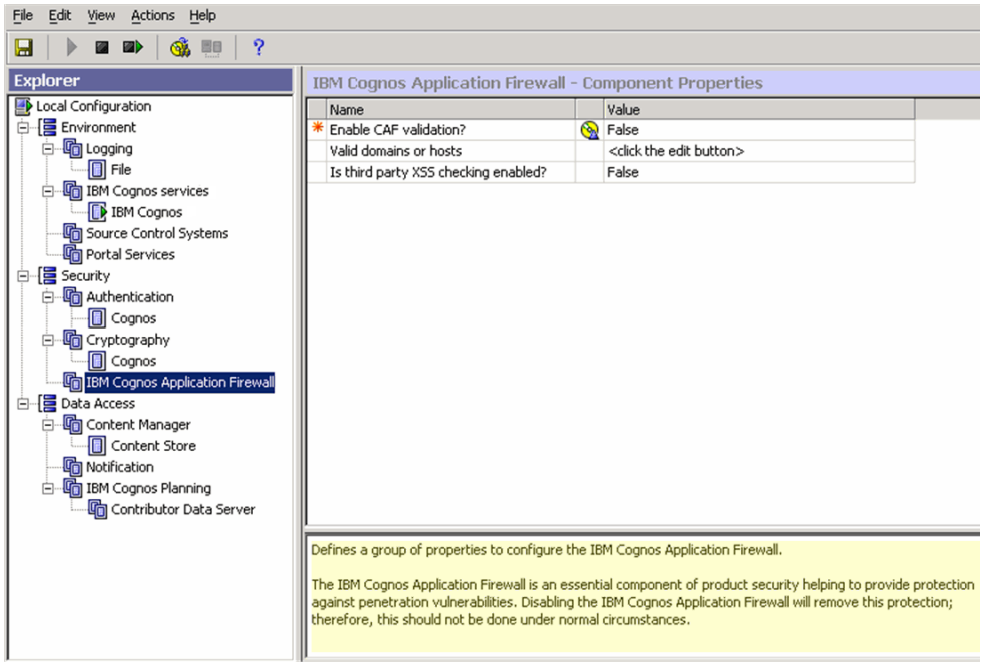
8.1.4.2 Setting the Security Properties for Cognos 10

To define the security properties:

1. Open the IBM Cognos 10 Configuration window.
2. Navigate to **Security, Authentication,** and select **Cognos.**



3. Set the **Allow anonymous access?** property to **True.**
4. Navigate to **Security** and select **IBM Cognos Application Firewall.**



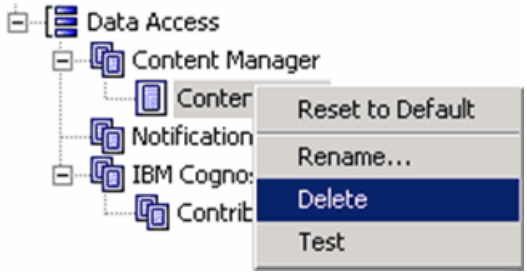
5. Set the **Enable CAF validation?** property to **False.**

8.1.4.3 Setting the Data Access Properties for Cognos 10

To define the data access properties:

1. Open the IBM Cognos 10 Configuration window.

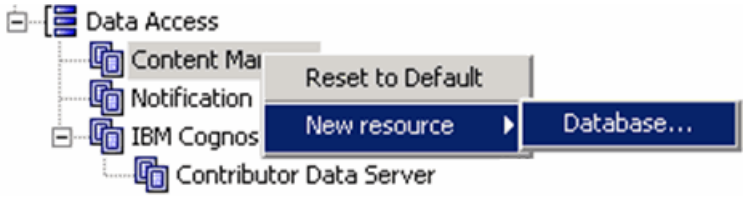
2. Navigate to **Data Access, Content Manager,** right-click **Content Store,** and then select **Delete** from the menu.



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

3. Click **Yes.**

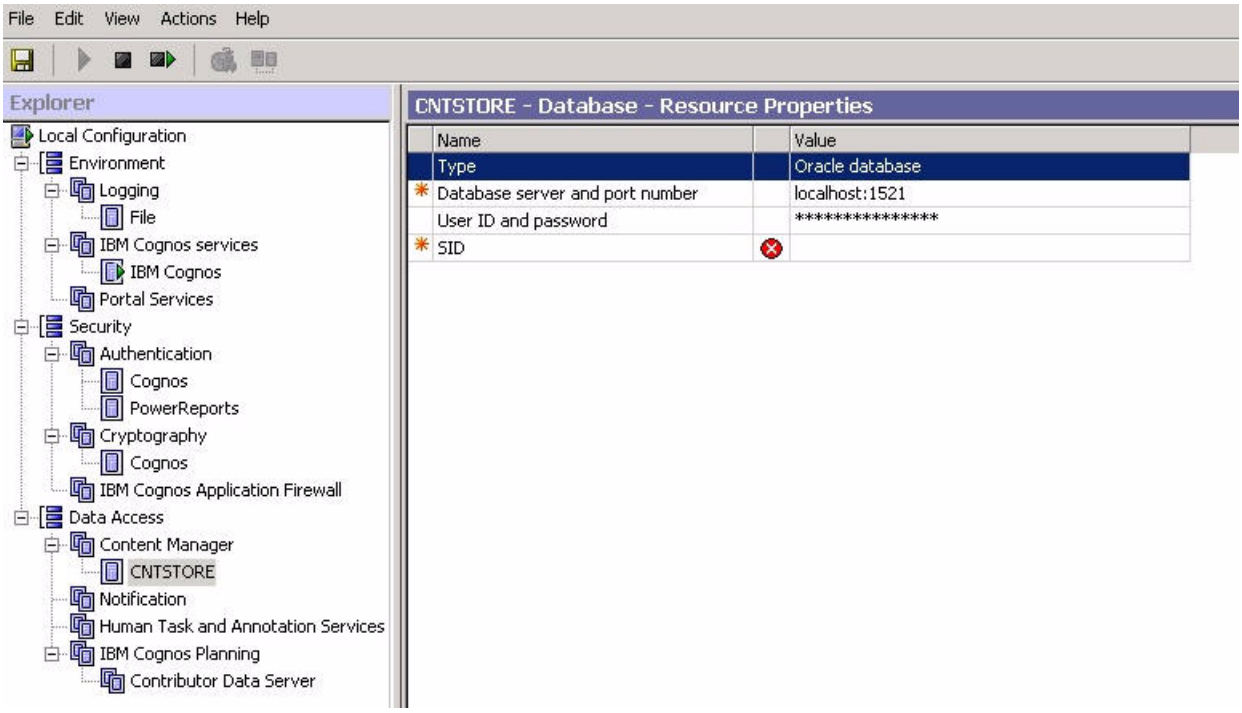
4. Navigate to **Data Access,** right-click **Content Manager,** select **New resource,** and then select **Database.**



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.



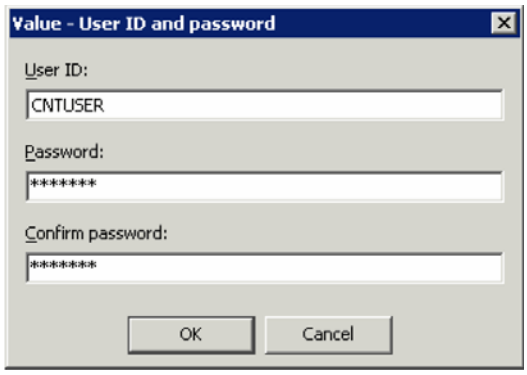
6. Enter the value for the **Database server and port number** as:

   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.



   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.

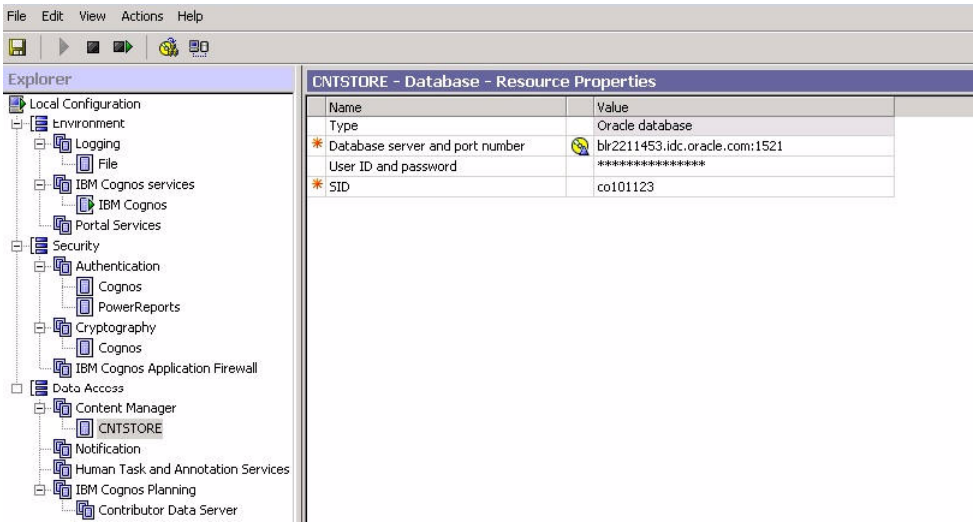
   d. Click **OK.**

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 10 server.

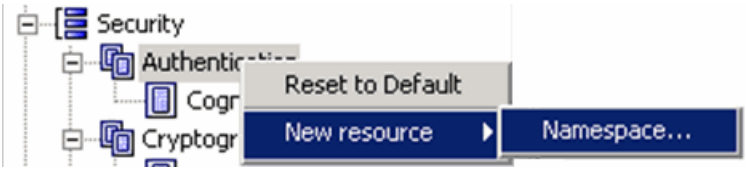
8. Enter the database instance name for the Cognos 10 repository in the **Service name** field.



8.1.4.4 Creating the Namespace for Argus Insight Authentication

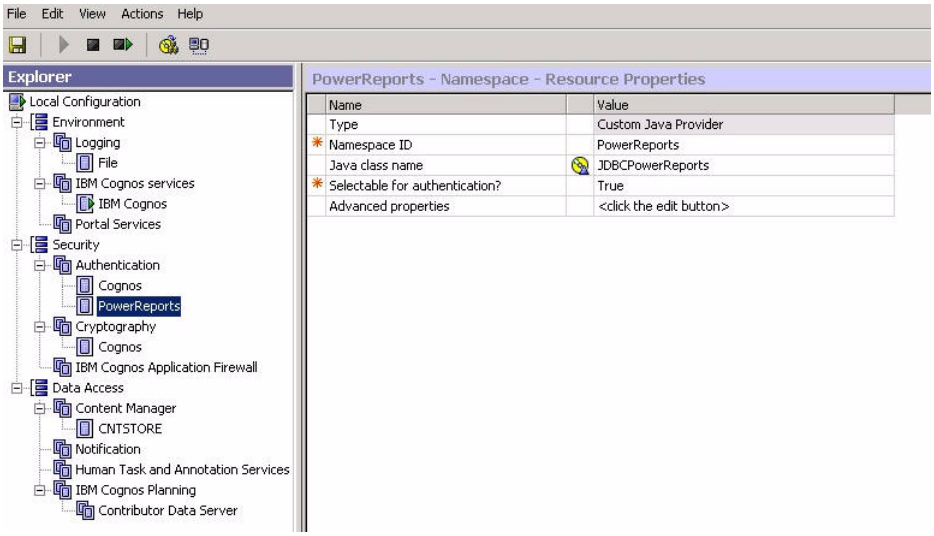
To create the namespace for Argus Insight authentication:

1. Open the IBM Cognos 10 Configuration 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.

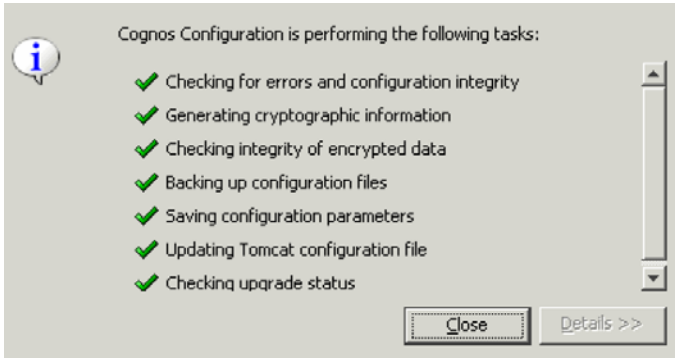


4. Set the **Namespace ID** property to **PowerReports.**
5. Set the **Java class name** property to **JDBCPowerReports.**

8.1.4.5 Saving Your Configuration and Starting the Cognos 10 Service

To save the configuration and start the Cognos 10 service:

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

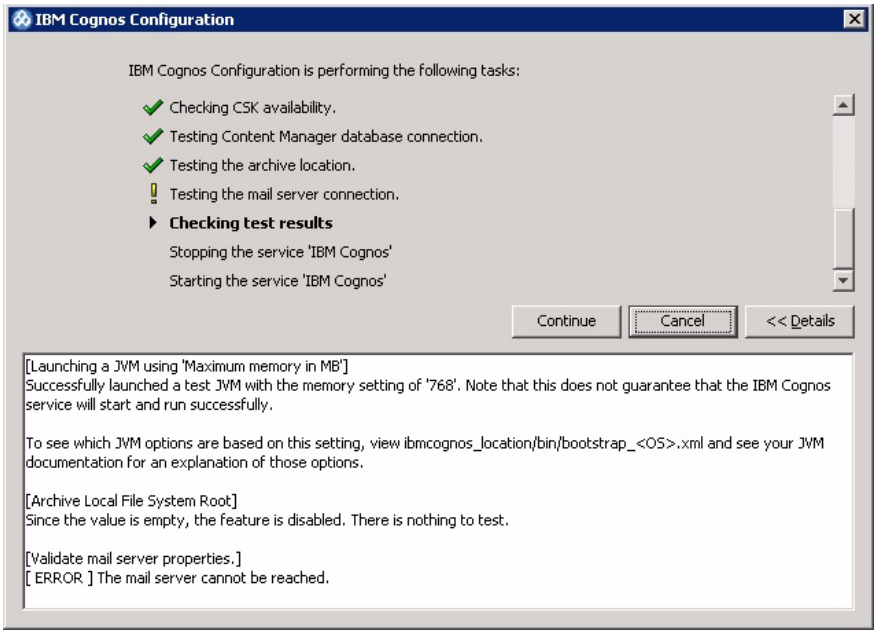


2. Click **Close** when the system completes all the configuration tasks.
3. Click the **Start** icon in the IBM Cognos Configuration window to run the Cognos 10 service.

The system begins to run the IBM Cognos 10 service.

- If there are no problems with the configuration, the system completes the test phase and starts the IBM Cognos 10 service successfully.

- If there are possible problems with the configuration, the system stops running the service and displays a warning message. When you click **OK** to acknowledge the warning message, the system opens another dialog box with more information. For example:



At this point, you can:

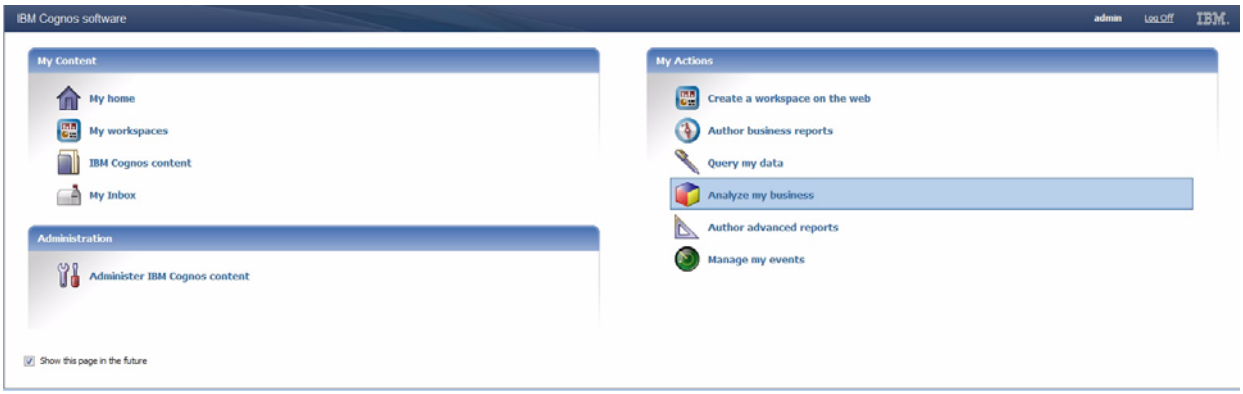
- Click **Details** for more information about the warnings and errors.
- Click **Cancel** to stop the process. If the warnings or errors are due to reasons other than mail server connection failure, cancel the process and check your configuration again.
- Click **Continue** to ignore the warnings and errors, and complete the process of starting the IBM Cognos 10 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 10 configuration.

8.1.5 Creating Cognos Data Source (PRMART)

To create Cognos Data Source (PRMART):

1. Log in to the Cognos 10.
2. The IBM Cognos 10 Home page opens.

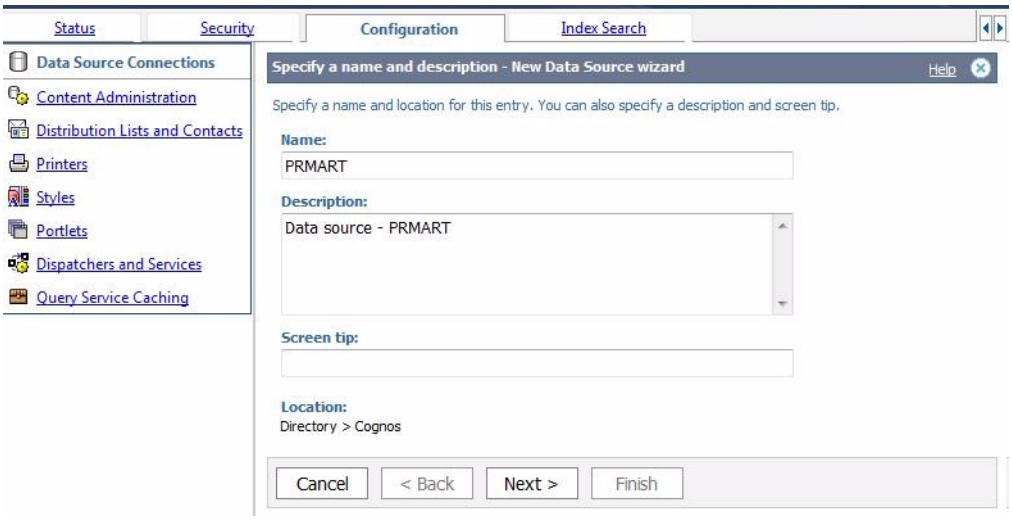


Note: If your security settings on the server do not permit you to view the Cognos connection, add the site URL (http://*Cognos_10_Server*/cognos10) to the list of local intranet sites.

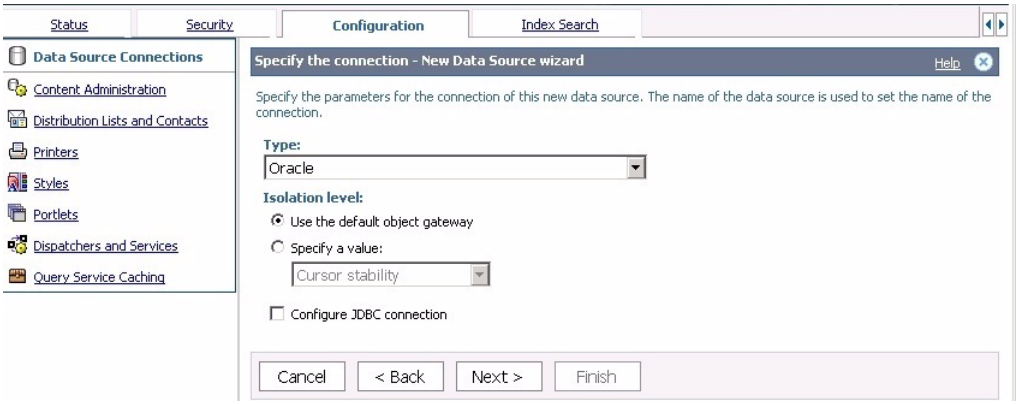
3. Click **Administer IBM Cognos content.** The IBM Cognos Administration window opens.

4. Click the **Configuration** tab.
5. Click **Data Source Connections**.
6. Click **New Data Source** icon. The Specify a name and description - New Data Source Wizard page opens.

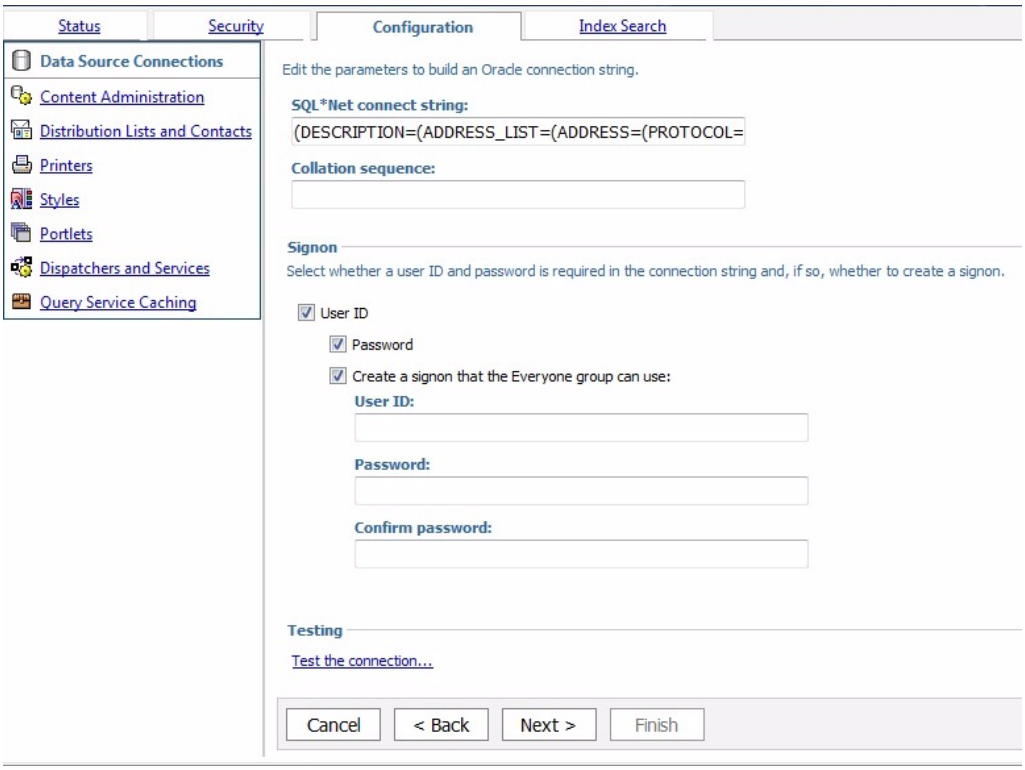
7. Enter the **Name** and **Description** of the data source, and click **Next**. The Specify the connection - New Data Source Wizard page opens.



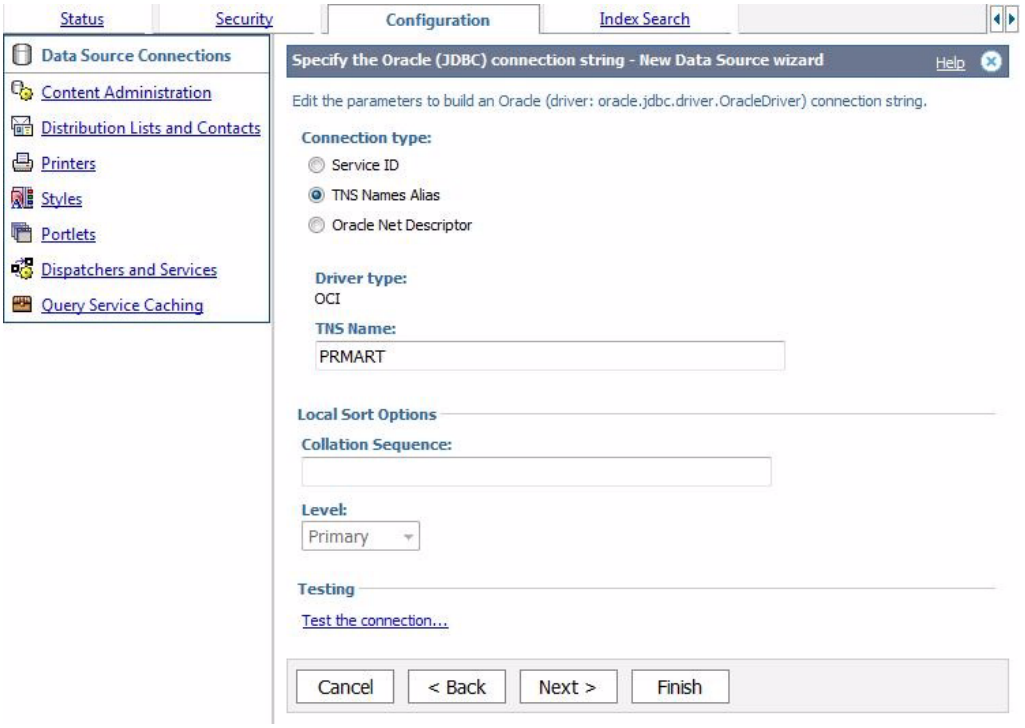
8. Specify parameters for the connection, and click **Next**.



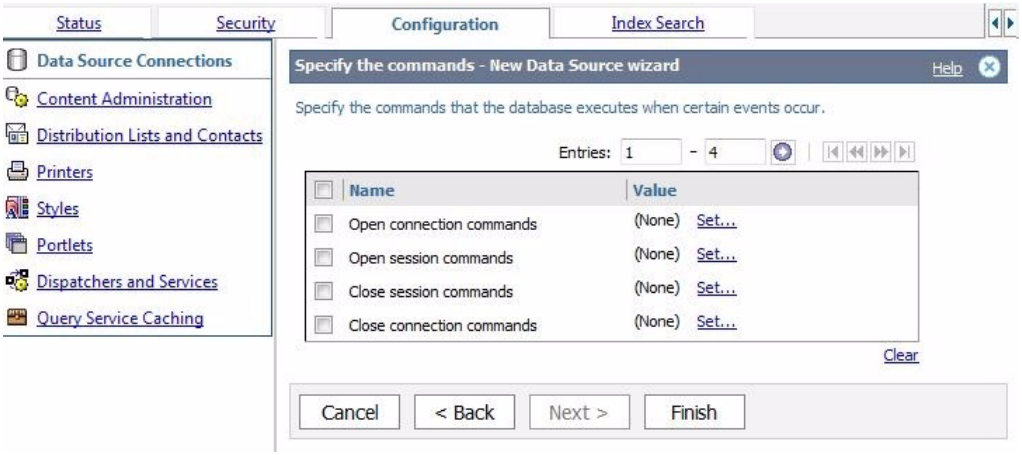
9. Enter the connection string in **SQL *Netconnect string:**, and click **Test the connection...**



10. Click **Next**. The Specify the Oracle (JDBC) connection string - New Data Source wizard page opens.
11. Specify the **Connection type**, and click **Next**. The Specify the commands - New Data Source wizard page opens.



12. Specify the commands for connection.



For more information on Cognos commands, refer to **Argus Insight Extensibility Guide > Section 4.2 Applying Argus Data Security** and **Section 4.3 Applying Enterprise Security**.

13. Click **Finish**. The PRMART data source is created.

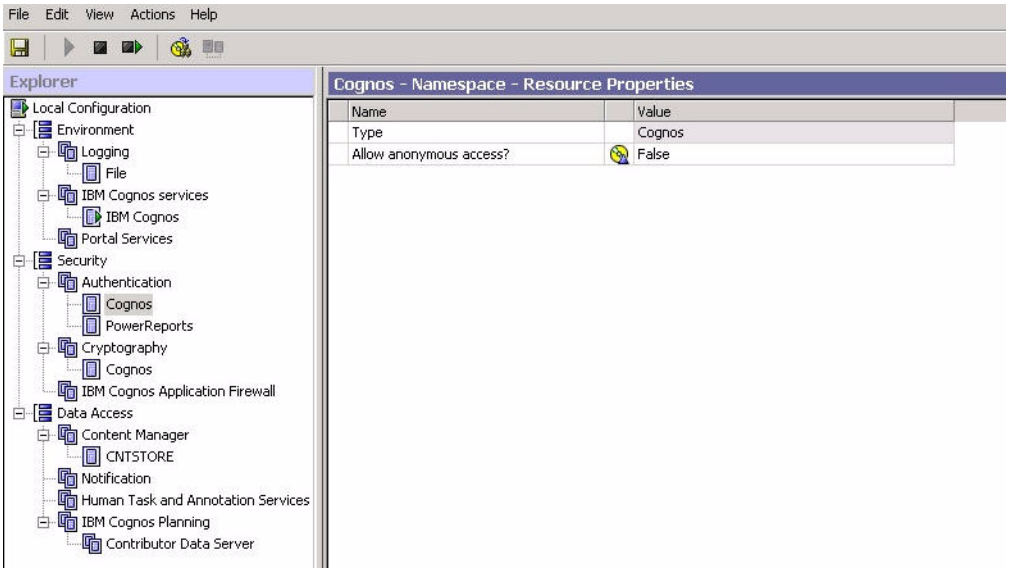
8.1.6 Configuring Cognos Security

This section includes the following topics:

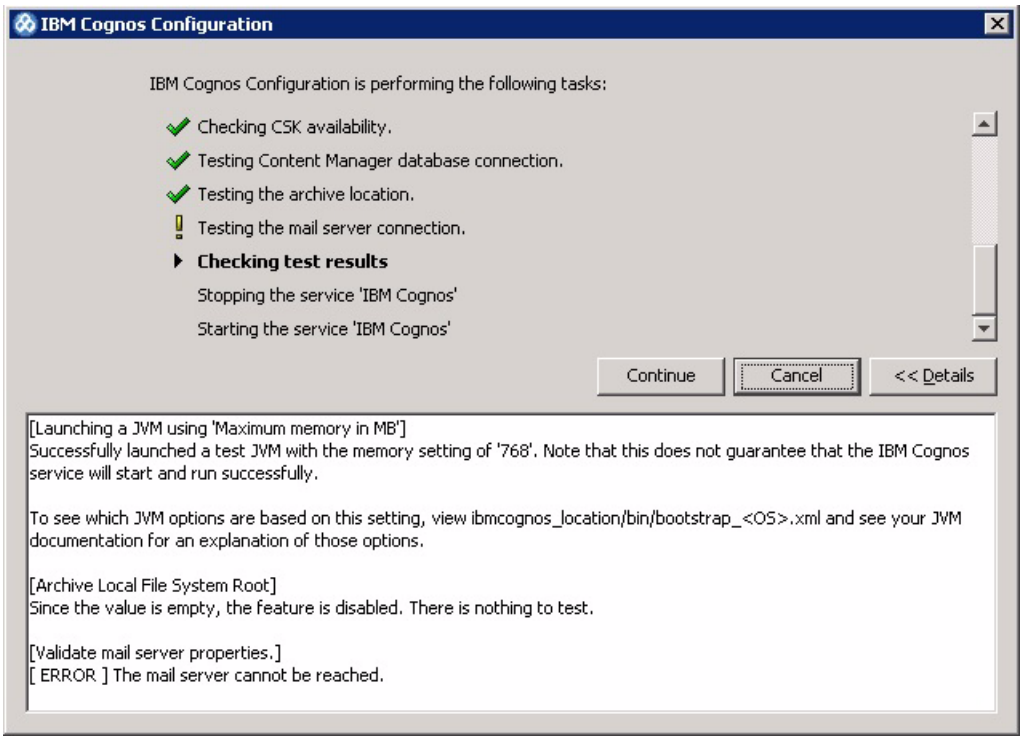
8.1.6.1 Activating the PowerReports Namespace

To activate the PowerReports namespace:

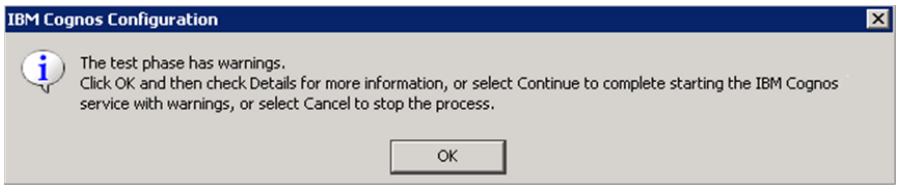
1. Open the Cognos 10 configuration.
2. Click **Start, All Programs, IBM Cognos 10,** and then select **IBM Cognos Configuration.** The IBM Cognos Configuration window opens.
3. Navigate to **Security, Authentication,** and then select **Cognos.** The system displays the Cognos - Namespace - Resource properties pane.
4. Set the **Allow Anonymous access?** property to **False.**



5. Open the **File** menu and select **Save.**
6. Open the **Actions** menu and select **Restart** to restart the Cognos 10 service. The system displays status information about each task being performed during the restart.



During the Cognos service restart, the system may display the following message if there are any warnings:

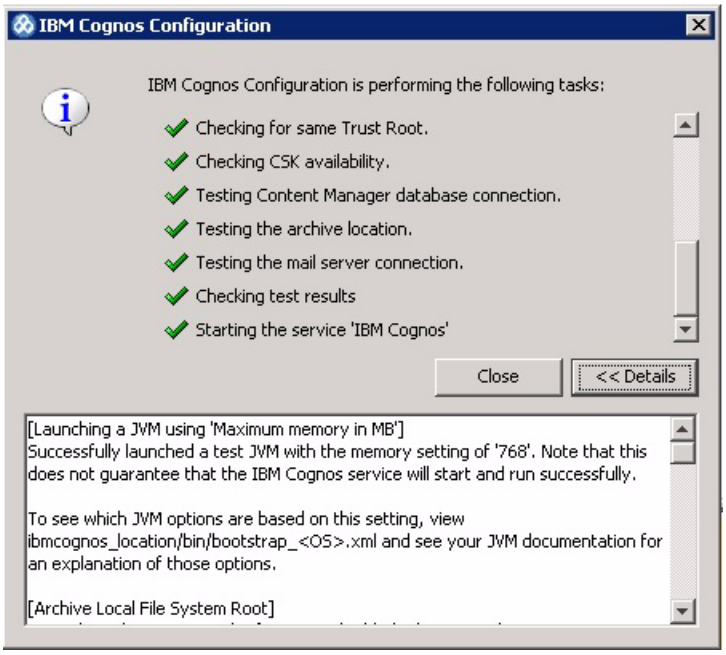


7. Process any warning message as follows:
   a. Click **OK.**
   b. Click **Details** to obtain more information about the warning.

      Depending on the type of warning, you can:

      — Click **Continue** to ignore the warning and continue with the process of restarting the IBM Cognos 10 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 10 service.
8. Wait until the system performs all the configuration tasks and displays the status for each task.



9. Click **Close** to exit the Cognos configuration.

Note: Make sure that you remove the **Everyone** user group from the **Directory Administrator** and **System Administrator** roles of Cognos. Before doing this, make sure that you have a valid user as part of the **System Administrator** role in Cognos.

If you have not added any user as part of the System Administrator role in Cognos, then you have to add Everyone user group in System Administrator roles of Cognos again.

To add the **Everyone** user group in the System Administrator role of Cognos:

1. Connect to the Content Store database as the content store user.
2. Navigate to the following folder:

   Cognos_10_Install_Path\C10\configuration\schemas\content
3. Run the **AddSysAdminMember.sql** script.
4. Commit the changes.

8.1.7 Configuring Roles and Permissions

To configure enterprise specific roles and permissions:

1. Log in to the Cognos 10 Server as an administrator user.
2. Create an Enterprise-specific role for each enterprise. For example:
   - ENT1_Role for Enterprise 1
   - ENT2_Role for Enterprise 2
3. Add all users belonging to the specific enterprises to their respective roles. For example:
   - Add ENT1_user to ENT1_Role

Note: If a user is a member of multiple enterprises, the user must be added to the roles for all the enterprises.

4. Create a folder in Public Folders for each enterprise. For example:
   - ENT1_Folder for Enterprise 1
   - ENT2_Folder for Enterprise 2
5. Select the required permissions of the Enterprise-specific role for the Enterprise-specific folder. For example,
   - Add ENT1_Role to the ENT1_Folder and provide the Read, Write, Execute, and Traverse permissions on this folder.

9

Managing the Argus Insight Cryptography Key

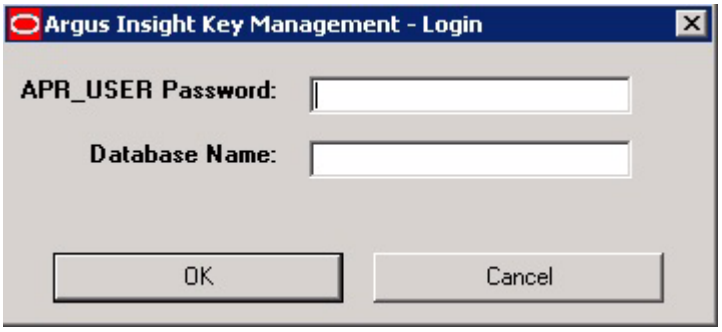
This chapter describes how to update the cryptography key in Argus Insight *after* the key has been updated in Argus Safety.

9.1 Updating the Cryptography Key

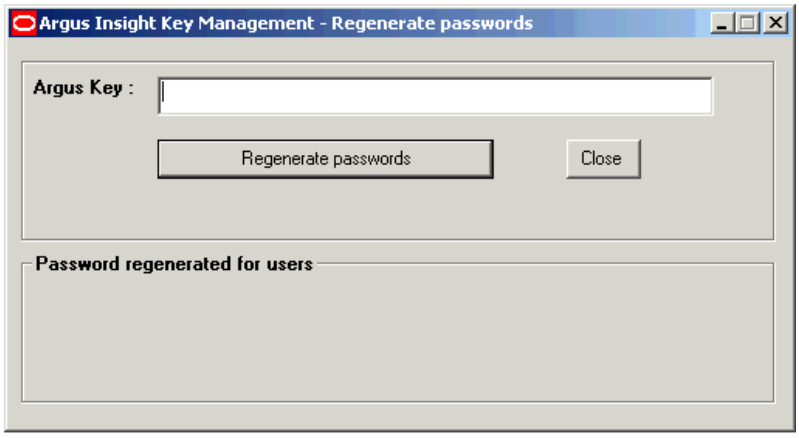
After the cryptography key has been updated in Argus Safety, you must update the cryptography key in Argus Insight. This process will update all the required passwords in Argus Insight using the new key.

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.



5. Enter the new key from the Argus Safety Server. You can copy **UserCryptoKey** from the ArgusSecureKey.ini file, which is present on all Argus Safety Servers in C:\Windows folder. Make sure you use the exact key used by the corresponding Argus Safety Server.
6. Click **Regenerate passwords** to start the password regeneration process.

   When the password regeneration process completes, the system:

   - Displays whether the regeneration process was successful (or failed)
   - Lists the passwords that changed

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

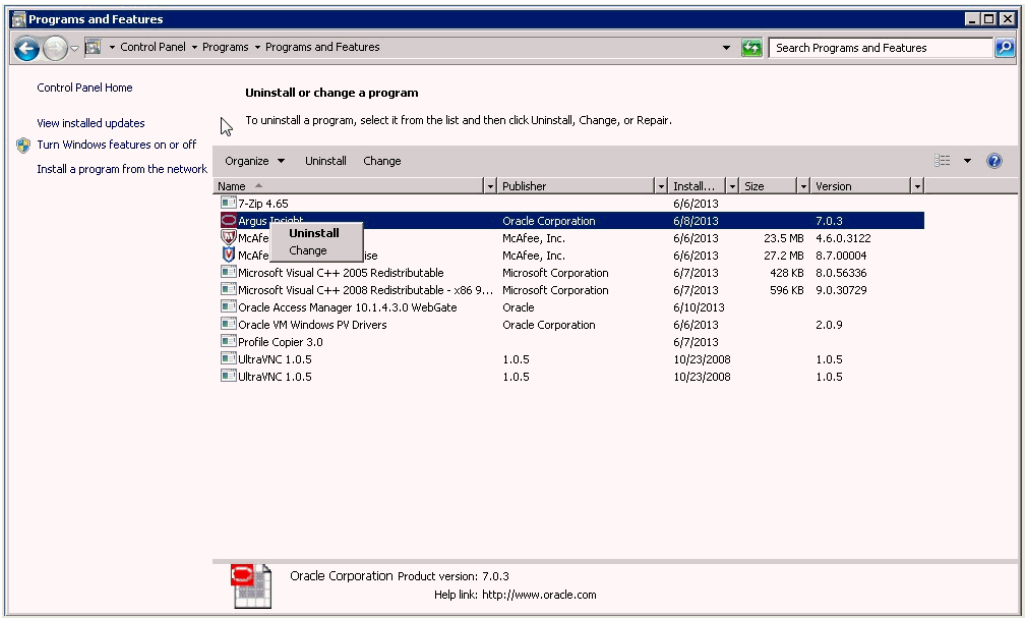
Uninstalling the Argus Insight Application

This chapter describes how to uninstall the Argus Insight application.

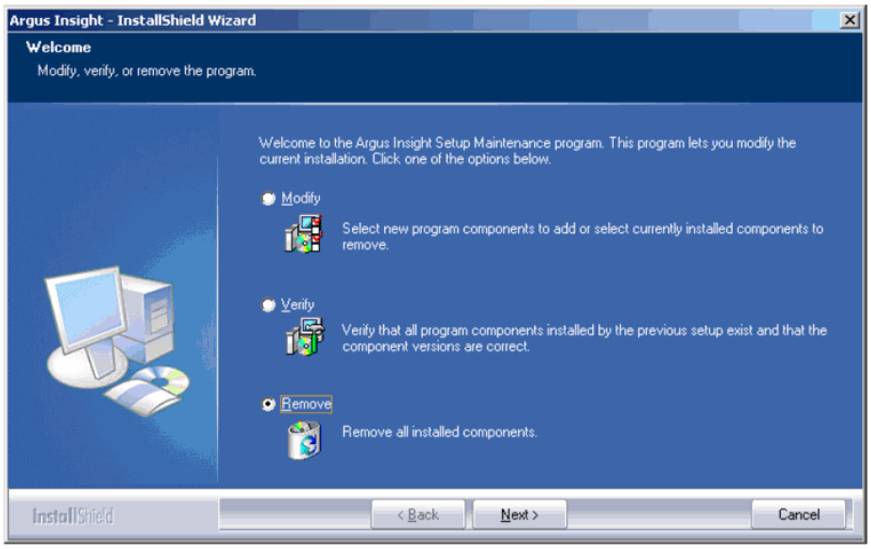
10.1 Uninstalling Argus Insight from the Web Server

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.



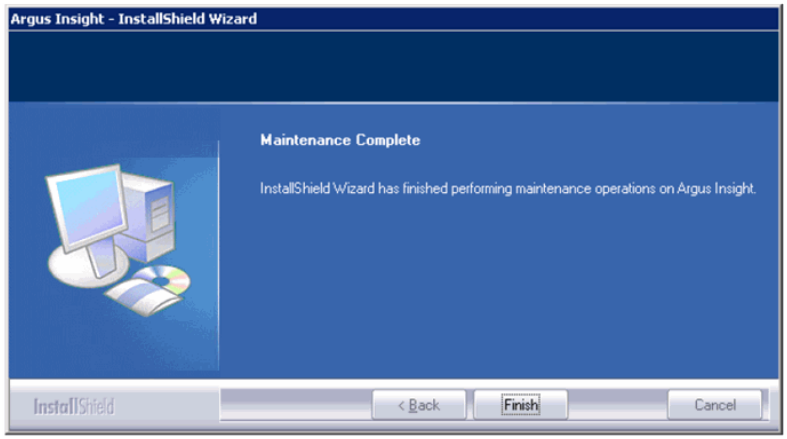
The system starts the Argus Insight wizard and opens the Welcome screen with options for modifying, verifying, and removing programs.



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.



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.