Oracle® Argus Insight

Installation Guide

Release 8.2

E96559-01

August 2018

ORACLE®

Oracle Argus Insight Installation Guide, Release 8.2

E96559-01

Contents

4   Upgrade the Argus Insight Data Mart Structure

5   Configure the Argus Insight Application

6   Extract, Transform, and Load Data

7 Configure the BIP Environment

8 Configure the OBIEE Environment

9 Manage the Argus Insight Cryptography Key

10 Uninstall the Argus Insight Application

Preface

This *Oracle Argus Insight Installation Guide* describes installing — or upgrading to — Argus Insight 8.2. You perform some of these tasks once. Other tasks you repeat as your system and business requirements change.

Where to Find More Information

Oracle Help Center

The latest user documentation for Oracle Health Sciences products is available at http://docs.oracle.com/en/industries/health-sciences/.

My Oracle Support

The latest release notes, patches and white papers are on My Oracle Support (MOS) at https://support.oracle.com. For help with using MOS, see https://docs.oracle.com/cd/E74665_01/MOSHP/toc.htm.

Documentation Accessibility

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

Access to Oracle Support

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

1

Introduction

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

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

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

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

1.1 Argus Insight Product Overview

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

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

The following flowchart shows the typical workflow for generating a report.
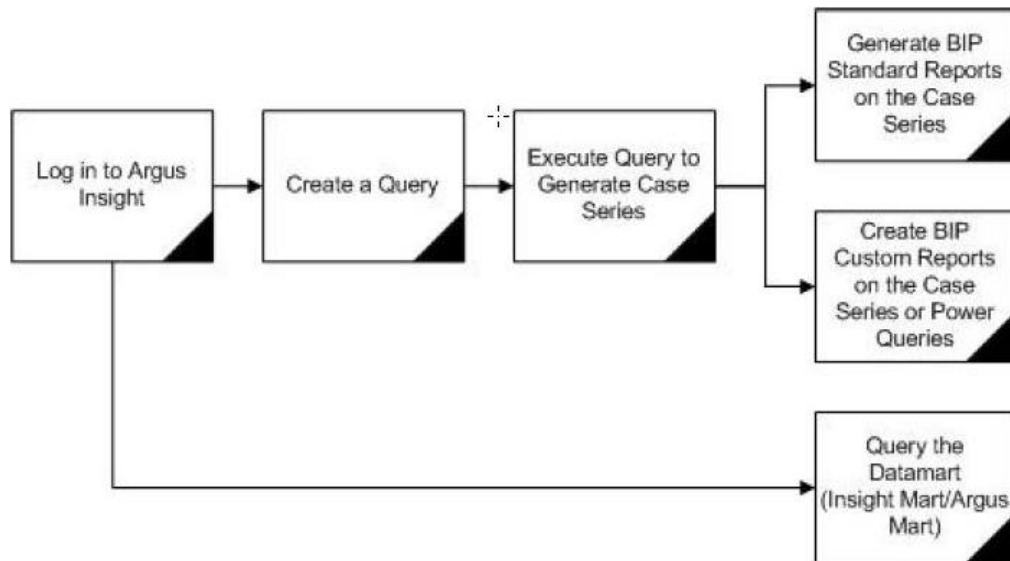
Table 1–1 describes the various features of Argus Insight:

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 (Insight Mart/Argus Mart) and applying Boolean and Set operations on them. You may use Advanced Conditions to query data on Argus Mart.
Case Series	A list of cases that match the query criteria with revisions (applicable only for Argus Mart).

1.1.1 Argus Insight Architecture
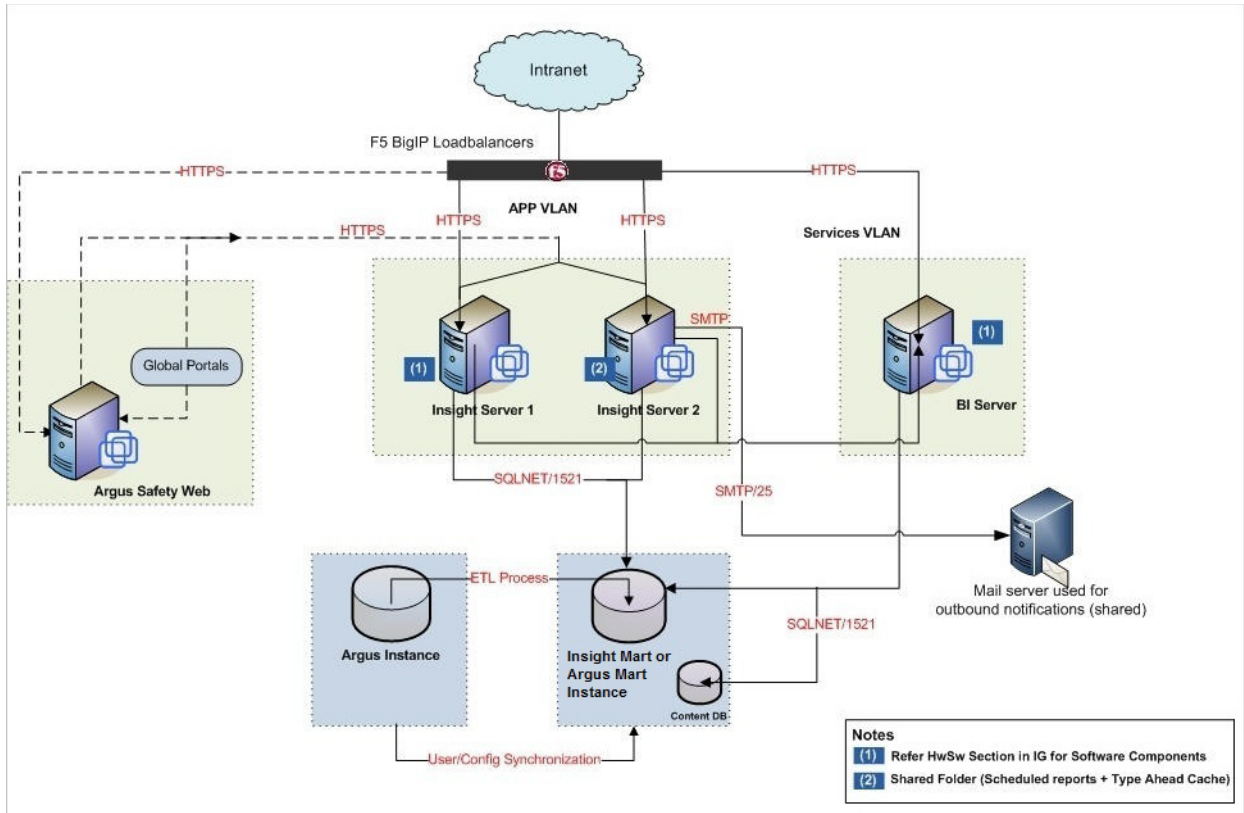
1.2 Software and Hardware Requirements

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

- Argus Insight Web Server

- Argus Insight Transaction Server

- Database Server

- OBIEE or BI Publisher (depending on which Business Intelligence tool you are using with Argus Insight)

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

- Argus Insight Client

Table 1–2   Argus Insight Software and Hardware Requirements

Component	Requirements
Argus Insight Web Server	**Supported Operating Systems:** ■ Windows 2016 ■ Windows Server 2012 R2 Standard **Note:** Make sure that you install the English versions of these operating systems. **Oracle Database Software:** ■ Oracle Client 12c Release 2 (12.2.0.1) Oracle Client 12c Release 1 (12.1.0.2) **Note:** Make sure, only one version of Oracle Client is installed on the server. Argus Insight Installer will not work in case there are multiple versions of Oracle Client are installed on the same machine. ■ Oracle Data Provider 12c Release 2 (12.2.0.1) for .Net Oracle Data Provider 12c Release 1 (12.1.0.2) for .Net **Hardware Requirements:** ■ Up to 5000 cases in the system: 2x2.6 GHz processors, 8 GB memory ■ More than 5000 cases in the system: 4x2 GHz processors, 16 GB memory **Additional Software Requirements:** ■ Dotnet Framework 3.5 Service Pack 1 ■ IIS 10 (Windows 2016) ■ IIS 8.5 (Windows 2012 R2) ■ Java Runtime Environment (JRE) version 1.8 ■ Microsoft Visual C++ 2012 (64 bit) ■ MSXML 6.0 ■ WebGate 11.1.2.3 (optional) ■ WebCenter (deprecated)—While upgrading, in the Components List, if this option appears, then uncheck it. **Note:** Argus Insight Supports SMTP and SMTPS with TLS 1.2 (Forced). SMTPS Supports both Implicit and Explicit Modes..

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

Component	Requirements
Database Server	Operating System as certified by the Oracle Database version.
	Oracle Database Software:
	■ Oracle Database Server (Enterprise Edition/Standard Edition 2 (SE2)) (12.1.0.2 or 12.2.0.1)
	(both CDB/PDB and Non-CDB formats)
	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 12c
	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 12c Release 1 (12.1.0.2 or 12.2.0.1)
	■ Exadata 12c Release 1 (12.1.0.2 or 12.2.0.1)
	Note: Oracle database Standard Edition 2 (SE2) is supported for single tenant deployment only.
	Hardware Requirements:
	■ Up to 5000 cases in the system: 2x2 GHz processors, 8 GB memory
	■ More than 5000 cases in the system: 4x2 GHz processors, 16 GB memory
Oracle Business Intelligence Enterprise Edition (OBIEE) or **BI Publisher (BIP)**	Operating System as certified by the OBIEE/BIP.
	Oracle Database Software:
	■ Same as Database Server.
	Tool Version:
	■ OBIEE or BIP 12c (12.2.1.4)
	Note: You can either install OBIEE or the stand alone BI Publisher (Dashboards are not available with standalone BI Publisher).
	Additional Software Requirements:
	■ Java Runtime Environment (JRE) version 1.8
	■ OBIEE Administrator Tool 12c (12.2.1.4) must be installed for configuring the repository file (RPD).
	Note that if you install OBIEE on a Linux machine, you need to install Oracle Business Intelligence Developer Client tools on a Windows machine. It will include the BI Administration tool.
	Refer to the *Oracle OBIEE Installation Manual* for further hardware and software requirements.
	■ WebGate 11.1.2.3 (optional)—Required for SSO configuration.

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

Component	Requirements
Argus Insight Client	**Supported Operating Systems:** ■ Windows 10 **Hardware Requirements:** ■ 2.0 GHz Minimum, 1 GB Memory **Additional Software Requirements:** ■ Adobe Acrobat Reader 11 or DC ■ Microsoft Excel: 2012 or 2016 ■ Microsoft Internet Explorer 11

> **Note:**   Argus Insight also supports:
>
> ■   Oracle Identity Manager 11.1.2.3
>
> ■   Oracle Virtual Machine Server 3.2.10 (64 bit)

1.3 Important Installation Information

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

1.3.1 Installation Requirements for the Servers

For the Argus Insight Web Server or BI Publisher:

■   **Installation Language —** You must install all software with the language setting configured to English. For example, if Oracle is installed in a language other than English, the registry entries are created with different names. Therefore, to avoid errors, install all software in English.

■   **Oracle Client —** You must install the Oracle client with the default *ORACLE_HOME* name, provided by the Oracle Universal Installer. Failure to do so will display an error message, stating that the Oracle OLE DB provider was not found during installation.

■   **Time Zone —** You must set all servers to the same time zone.

■   **Default Language Setting —** All the servers must have the default language setting enabled for US English.

To enable US English as the default language setting:

1.   Open the Microsoft System Registry Editor.

   a.   Click **Start.**

   b.   Select **Run.**

   c.   Enter **regedit**, and then click **OK.**

2.   Navigate to the following folder:

   HKEY_USERS\.DEFAULT\Control Panel\International

3.   Double-click the **sCountry** key in the right pane.

    a. In the **Value data** field, enter **United States.**

    b. Click **OK** to save changes.

4. Exit from the Registry Editor.

5. Restart the server to reflect the changes.

Additional Notes:

- **For Argus Insight Web Server:**

  - Install the Oracle client *after* you install the Dotnet Framework.

  - Ensure that either you have disabled the firewall or you have added the Argus Insight port number in the Windows Firewall Exception list. The default port number for Argus Insight is 8084.

- **For BI Publisher:**

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

1.3.2 Installation Requirements for the Argus Insight Client

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

- Add the Argus Insight URL to the trusted sites.

- Enable Cookies to the lowest possible security level.

- Enable Javascript.

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

  To enable this setting:

  1. Start Internet Explorer.

  2. Open the **Tools** menu, and select **Internet Options.**

  3. Select the **Security** tab.

  4. Click **Custom level.**

  5. Scroll to the Miscellaneous settings.

  6. Enable the **Allow script-initiated windows without size or position constraints** setting.

  7. Click **OK** to save changes.

1.3.3 General Installation Notes and Information

- All the information about LDAP, Single Sign-On Header, and SMTP configuration will be synchronized in real-time and also by ETL.

- Ensure that you have configured the Argus Safety URL in the Argus Safety Load Balancer Server.

  To do so:

  1. Navigate to **Argus Console, System Management** (Common Profile Switches), and select **Network Settings.**

2. In the Argus Safety Load Balancer Server text box, enter either the Argus Safety URL or the Argus Safety Load Balancer URL.

2

Install Argus Insight

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

2.1 Before You Install the Argus Insight Application

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

1. **Requirements—**Read Section 1.2, "Software and Hardware Requirements" and verify that your system meets the minimum requirements.

2. **Database Instance—**Verify that the Argus Insight database instance has been created and that it is running. In addition, verify that the database has been created using the character set of your Argus Safety database.

3. **Cryptographic Key—**Log in to the Argus Safety Web Server. Copy the **UserCryptoKey** from the ArgusSecureKey.ini file located at C:\Windows. You need to specify this key during the installation of Argus Insight.

4. **Security—**Log in to the Argus Insight Web Server.

   a. Ensure that the **IUSR** user or the user configured in Internet Information Services (IIS) has sufficient privileges for running the Argus Insight application. See the *Oracle Argus Insight Minimum Security Configuration Guide* for more information.

   b. Ensure that the ASP and ASP.Net extensions are enabled in IIS.

2.2 Install Argus Insight Components onto the Web Server

> **Note:** If you are upgrading Argus Insight from 8.1.1 to Argus Insight 8.2, first uninstall the application using Argus Insight application, and then run the Argus Insight 8.2 Installer.
>
> To uninstall the existing application, see Section 10, "Uninstall the Argus Insight Application".

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

1. Download the Argus Insight software from Oracle E-delivery and copy the software to the Argus Insight Web Server.

2. Log in to the Argus Insight Web Server as a user with administrator privileges.

3. Click **setup.exe.**

   The Welcome screen of the installation wizard appears.

4. Click **Next** to continue.

5. Enter your user name and company name into the appropriate fields.

6. Click **Next** to continue.

   The Select Features dialog box appears.

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

8. Click **Next** to continue.

   The Choose Destination Location dialog box appears.

9. Specify the folder where the system installs the Argus Insight application.

   ■ To install into the default folder (C:\Program Files\Oracle), click **Next.**

   ■ To install into a different folder, click **Browse,** select another folder, and then click **Next.**

   A message appears stating that the wizard is ready to install the Argus Insight files.

10. Click **Install** to start the installation.

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

11. Enter the name of the host database server where the Argus Insight data mart is located, and click **Next.**

12. Enter the instance name for the Argus Insight data mart, and click **Next.**

13. Enter the database port number you want to assign to the Argus Insight database, and click **Next.**

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

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

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

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

15. Enter the password for APR_USER.

> **Note:** The APR_USER database user provides initial database access to the application user (APR_APP) of Argus Insight. Make sure that this password is the same on all machines where any Argus Insight components are stored.
>
> You will be prompted to create or update this user during installation. 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, "Change the APR_USER Password."

16. Click **Next** to continue.

    The Confirm Password dialog box appears.

17. Re-enter the APR_USER password for verification.

18. Click **Next.**

    The Port Number dialog box appears.

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

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

20. Click **Next.**

    The Argus Insight application is installed successfully.

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

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

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

> **Note:** If you have Oracle Client 12.1.0.2 installed on your machine, go to Argus Insight software folder, copy files from bin folder and paste them into the following folders:
>
> ■ *<Argus Insight installed path>*/Bin folder
>
> ■ *<Argus Insight installed path>*/Database/DBInstaller
>
> Also, update **newVersion** to 2.121.2.0 under runtime tag in configuration files present on both Argus Insight Web Server and Argus Insight Transaction Server.

2.2.1 Change the APR_USER Password

You need to update the password on the database level and the Argus Insight Web 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:

■ Stop the Argus Insight service.

■ Stop IIS on the Argus Insight Web Server.

■ Stop the IIS.

- 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 by running the Argus Insight installer on each server.

To modify the APR_USER password:

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

   The Argus Insight Setup Maintenance dialog box appears.

2. Select **Modify**, and click **Next.**

3. Select **Change the password for APR_USER,** and click **Next.**

4. Enter the **APR_USER** password.

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

5. Click **Next.**

   A dialog box to confirm new password appears.

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

7. Click **Next.**

   The system updates the password for APR_USER.

2.3 Enable SSL Support for the Argus Insight Website

1. Log in to the Argus Insight Web Server.

2. Obtain and install the SSL certificate.

3. Go to IIS Manager.

4. Select **Argus Insight**, and select **Bindings.**

   The Site Bindings dialog box appears.

5. Click **Add.**

   The Add Site Binding dialog box appears.

6. Enter the following details in the Add Site Binding dialog box:

   a. In the **Type** field, select **https.**

   b. In the **SSL certificate** field, select your security certificate.

   c. Click **OK.**

3

Create the Argus Insight Data Mart Structure

The Argus Insight data mart structure is created while installing Argus Insight through Liquibase in silent-mode.

Besides, it also creates a link between the source Argus database and the new Argus Insight data mart. The Extract Transform and Load (ETL) process uses this link to transfer data from Argus Safety database to the Argus Insight data mart for reporting purposes.

Liquibase is a refactoring tool that enables Argus Insight to be in synchronization with the closest major release, and subsequently upgrades the product to the required minor versions of the product.

> **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 per Section 1.2, "Software and Hardware Requirements".

3.1 Before You Run the Argus Insight Installation

The **GLOBAL_NAMES** and **NLS_LENGTH_SEMANTICS** database parameters must be configured properly in order for the Argus Insight installation to run. You must check those settings *before* you run the Argus Insight Installation. If the parameters are not set properly, the installation 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_NAMES = FALSE

      Value of parameter GLOBAL_NAMES must be same in Argus Safety and Argus Insight (either TRUE for both or FALSE for both).

      If GLOBAL_NAMES is set to TRUE, the Database Name reflected in the table GLOBAL_NAME, must have the same domain for both Argus Safety and Argus Insight databases (like, us.example.com).

    - NLS_LENGTH_SEMANTICS = CHAR

    - TNS Name for Argus Safety Database must be present in the Oracle Database Client > tnsnames.ora file at the following path:

      ...\network\admin\tnsnames.ora

3. Restart the database instance to reflect the changes.

To create a DBA user:

To use a different user than SYSTEM user to execute the installation, then create a DBA user by executing the DBA User Creation script:

ArgusInsight\Database\DBInstaller\Utilities\Create_Dba_User\ai_create_dba_user.bat

For more details on creating this user, see Section 3.4.3, "Create the DBA User."

Besides creating the DBA user, this batch file also provides minimum necessary privileges required for executing the installation.

3.2 Configure dbinstaller.properties file

Open the DBInstaller\dbinstaller.properties file, and view or modify the following parameters to make sure that Liquibase runs properly.

Parameter	Description	Modify	Default or Sample Value
db_connect_string	Database instance details in the form of <host>:<port>/<SID>	Yes	db_connect_string =abc.in.oracle.com:1521/AI82DB Or, db_connect_string =abc.in.oracle.com:1521/AI82DB.IN.ORACLE.COM
dba_user	Name of the Target Database DBA user	Yes	dba_user=ai_dba_user
log_level	Log level setting related to liquibase for smooth run. Possible values: ■ DEBUG ■ INFO	Yes	log_level=info
argus_securekey_path	Complete directory path of Argus Secure Key ini file on the middle-tier.	Yes	argus_securekey_ path=c:/windows
appschema_mart_user	Argus Insight Mart schema Owner	No	appschema_mart_user=apr_ mart/pwd
.appschema_stage_user	Argus Insight Staging schema Owner	Yes	appschema_stage_user=apr_ stage/pwd
appschema_ai_link_user	Argus Insight Link User	Yes	appschema_ai_link_user=apr_ link/pwd
appschema_rls_user	Argus Insight VPD schema Owner	Yes	appschema_rls_user=rls_ user/pwd
appschema_mart_app_user	Argus Insight Application schema Owner	Yes	appschema_mart_app_user=apr_ app/pwd
appschema_mart_hist_user	Argus Insight History schema Owner	Yes	appschema_mart_hist_user=apr_ hist/pwd
appschema_ai_apr_user	Argus Insight apr User Name	No	appschema_ai_apr_user=apr_ user/pwd
appschema_ai_login_user	Argus Insight Login User Name	Yes	appschema_mart_user=apr_ mart/pwd

Parameter	Description	Modify	Default or Sample Value
ai_role	Argus Insight Mart Role	Yes	ai_role=MART_ROLE
ai_app_role	Argus Insight Mart App Role	Yes	ai_app_role=APP_ROLE
ai_link_role	Argus Insight Mart Link Role	Yes	ai_link_role=LINK_ROLE
safety_db	Argus Safety database instance name	Yes	■ safety_db=SAF82DB, or ■ safety_db=SAF82DB.US.EXAMPLE.COM
safety_ro_user	Argus Insight read only user in Safety DB	Yes	safety_ro_user=insight_ro_user
#Default Datafiles Directory	Default location of the datafiles. on the Database Server	Yes	default_datafile_destination =*<c:/app/oradata/82DB>*
#Insight Stage Normal Datafiles	Location of Argus Insight normal datafiles.	Yes	■ ai_stage_data_01_datafile=APR_STAGE_DATA_01.DBF ■ ai_stage_ind_01_datafile=APR_STAGE_INDEX_01.DBF ■ ai_stage_lob_01_datafile=APR_STAGE_LOB_01.DBF
#Insight Stage ESM Datafiles	Location of Argus Insight ESM datafiles.	Yes	■ apr_sesm_data_01_datafile=APR_SESM_DATA_01.DBF ■ apr_sesm_ind_01_datafile=APR_SESM_INDEX_01.DBF ■ apr_sesm_lob_01_datafile=APR_SESM_LOB_01.DBF
#Insight Stage WHO Datafiles	Location of Argus Insight WHO datafiles.	Yes	■ stage_who_01_datafile=APR_SWHOC_DATA_01.DBF
#Insight Mart Case/Rpt Datafiles	Location of Insight Mart case and report datafiles.	Yes	■ mart_case_rpt_data_01_datafile=APR_MCAS_DATA_01.DBF ■ mart_case_rpt_ind_01_datafile=APR_MCAS_INDEX_01.DBF ■ mart_case_rpt_lob_01_datafile=APR_MCAS_LOB_01.DBF
#Insight Mart Non-Case/Rpt Datafiles	Location of Insight Mart non-case and report datafiles.	Yes	■ mart_non_case_data_01_datafile=APR_MCFG_DATA_01.DBF ■ mart_non_case_ind_01_datafile=APR_MCFG_INDEX_01.DBF ■ mart_non_case_lob_01_datafile=APR_MCFG_LOB_01.DBF

Parameter	Description	Modify	Default or Sample Value
#Insight Mart EDM Datafiles	Location of Insight Mart EDM datafiles	Yes	■ mart_edm_data_01_datafile=APR_MEDM_DATA_01.DBF ■ mart_edm_ind_01_datafile=APR_MEDM_INDEX_01.DBF ■ mart_edm_lob_01_datafile=APR_MEDM_LOB_01.DBF
#Insight Mart WHO Datafiles	Location of Insight Mart WHO datafiles	Yes	■ mart_who_01_datafile=APR_MWHOC_DATA_01.DBF
#Insight Hist Case/Rpt Datafiles	Location of Argus Insight case or report History datafiles	Yes	■ hist_case_rpt_data_01_datafile=APR_MCAS_HIST_DATA_01.DBF ■ hist_case_rpt_ind_01_datafile=APR_MCAS_HIST_INDEX_01.DBF ■ hist_case_rpt_lob_01_datafile=APR_MCAS_HIST_LOB_01.DBF
#Insight Hist Non-Case/Rpt Datafiles	Location of Argus Insight non-case and report History datafiles.	Yes	■ hist_non_case_data_01_datafile=APR_MFACT_HIST_DATA_01.DBF ■ hist_non_case_ind_01_datafile=APR_MFACT_HIST_INDEX_01.DBF ■ hist_non_case_lob_01_datafile=APR_MFACT_HIST_LOB_01.DBF
#Insight Apr Datafiles	Location of Argus Insight APR datafiles	Yes	■ apr_user_data_01_datafile=APR_USER_DATA_01.DBF ■ apr_user_ind_01_datafile=APR_USER_INDEX_01.DBF ■ apr_user_lob_01_datafile=APR_USER_LOB_01.DBF
Default and Temporary tablespaces	Defines default and temporary tablespace name	Yes	■ default_ts=USERS ■ temp_ts=TEMP
Tablespace Encryption	Specifies the logic used for default encryption	Yes	tablespace_encryption=<blank> or <text>, where ■ blank—No encryption ■ text—like encryption using 'AES256' default storage (encrypt)
Tablespace Parameters	Specifies the details of the tablespace	Yes	■ tablespace_initial_size=10M ■ tablespace_autoextend=ON ■ tablespace_next_size=10M ■ tablespace_block_size=8K

3.3 Argus Insight Configuration Requirements

3.3.1 Database Parameters

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

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

Table 3–1   Database Parameters for Argus Insight

Database Parameter	Required Value
COMPATIBLE (for Oracle 12*c* R1)	12.1.0.2 or later
CURSOR_SHARING	EXACT
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

3.3.2 Database I/O Configuration

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)			

3.3.3 Recommended Configuration for the 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.

3.4 Create Argus Insight Database Schema

3.4.1 Prerequisites

Make sure:

- an Oracle client with Administrator option is installed on the server.
- database TNS entry should be added in the TNSNAMES.ora file.
- login machine user should have administrative privileges.

To install Java:

1. Download the jce_policy-8.zip file on your local machine from the following link:

.http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (download jce_policy-8.zip).

2. Unzip the jce_policy-8.zip.

3. Replace **local_policy.jar** and **US_export_policy.jar** files present in all the Java JRE installation security folders with the local_policy.jar and US_export_policy.jar shipped in **jce_policy-8.zip**.

   For example:

   Location of Java JRE 64-bit.

   C:\Program Files\Java\jre1.8.0_161\lib\security

4. From the command prompt verify that Java is properly installed by executing:

   java -version

   If no Java version appears, check the environment variables settings and path system variables have correct Java installation path set.

To set Java Installation Path:

1. Right-click the My Computer (or Computer) icon, and from the drop-down menu select **Properties**.

2. From the left-pane, select **Advanced system settings**.

   The System Properties dialog box with Advanced tab appears.

3. In the Startup and Recovery section, click **Environment Variables**.

4. From the System variables section, scroll-down to **Path** variable, and double-click.

   The Edit System Variable dialog box appears.

5. In the **Variable value:** field, enter the location where Java will be installed, and end it with a semi-colon (;).

6. Click **OK** to close the Edit System Variable dialog box.

7. Click **OK** to close the System Properties dialog box.

3.4.2 Create Users and Roles in the Argus Safety Database

1. To create the Safety Read-only user for Insight, execute the following script from the folder DBInstaller\Utilities\Create_Safety_Ro_User:

   - For Windows—Use the batch script ai_argus_read_only{user}.bat

   - For Linux—Use the shell script ai_argus_read_only{user}

2. When prompted, enter the following parameters:

   - Name of the Safety Database instance

   - Name of DBA User in Safety Database

   - DBA user password in Safety Database

   - Name of the Safety Read Only User to be created for Insight

   - Password of the Safety Read Only User

   - Role to be associated with Safety Read-only User

   - Default Tablespace for Safety Read-only User—For example, USERS

■ Temporary Tablespace for Safety Read-only User—For example, TEMP

The process of creating a Safety Read-only user begins.

3. Review the log file from the following path, and check for any errors, when a confirmation message appears.

C:\Program Files (x86)\Oracle\ArgusInsight\Database\DBInstaller\Utilities\Create_Safety_Ro_User\AI_AS_RO_User_MMDDYYYY_HH24MISS.log

3.4.3 Create the DBA User

> **Note:**   You must execute this script to install Argus Insight database, even if you are using the SYSTEM user. This script provides additional grants to the existing user.

To create a DBA user that has privileges same as the SYSTEM user for installation:

1. Execute the following script from the folder DBInstaller\Utilities\Create_Dba_User:

   ■ For Windows—Use the batch script ai_create_dba_user.bat

   ■ For Linux—Use the shell script ai_create_dba_user

2. When prompted, enter the following parameters:

   ■ Argus Insight Database instance name

   ■ SYS or an equivalent SYSDBA user on this database

   ■ SYSDBA user password

   ■ Name of the DBA User—For example, SYSTEM or AI_DBA_USER

   ■ DBA user password

   If you provide a non-existing user name, then the script creates this as a new user, and provides the necessary grants to this user.

   If you provide an already existing user name, then the script provides the necessary additional grants to the existing user.

   When done, a message appears as:

   Created DBA user &dba_user

3. Press **Exit**.

4. Verify the log files for status information from:

   C:\Program Files (x86)\Oracle\ArgusInsight\Database\DBInstaller\Utilities\Create_Dba_User\AI_DBA_User_ MMDDYYYY_HH24MISS.log

> **Recommendation:**   For security reasons, Oracle recommends to drop the DBA user from the database after successful installation of Argus Insight as this user will have DBA privileges.
>
> To drop this user, connect to the respective database as a privileged user, and execute the following command:
>
> ```
> DROP USER <INSTALL_USER> CASCADE;
> ```

3.4.4 Create Fresh Argus Insight Schema

1. Log in to the Argus Insight Web Server.

2. Navigate to Programs > Oracle > Argus Insight > Database > DBInstaller.

3. Open DbInstaller\dbinstaller.properties file.

4. Modify the following parameters:

   - **Insight Database**:

     – db_connect_string—connects to the Argus Insight database.

       Syntax: db_connect_string=<host>:<port>/<SID>

       For example, server.us.xx.com:1521/AI82MT

     – dba_user—specifies the name of the DBA user to run Argus Insight Liquibase Install.

       See Section 3.4.3, "Create the DBA User."

     – default_datafile_directory—default location on the database server, where datafiles will be created.

   - **Insight User** of each schema, where password is optional:

     – appschema_mart_user

     – appschema_stage_user

     – appschema_mart_app_user

     – appschema_mart_hist_user

     – appschema_ai_link_user

     – appschema_rls_user

     – appschema_ai_apr_user

     – appschema_ai_login_user

   - **Insight Roles:**

     – ai_role—specifies Mart User roles

     – ai_app_role—specifies App User roles

     – ai_link_role—specifies Link User roles

   - **Secure Key:**

     – argus_securekey_path—path of the file insight.ini in the middle-tier machine from where the DBInstaller.bat is executed.

   - **Safety Database:**

     – safety_db—Argus Safety database instance name

     – safety_ro_user—Argus Insight Read-only user created in Argus Safety

   > **Note:** For more information on these parameters, see Section 3.2, "Configure dbinstaller.properties file."
   >
   > It is recommended that you preserve the default names for tablespaces and roles.

5. From the command prompt, go to DBInstaller directory.

6. Type dbinstaller.bat, and press **Enter**.

The Liquibase install begins, and the parameters (as entered) appear on the command prompt screen with password in the hidden mode (****).

7. Keep monitoring the Liquibase progress by querying the Liquibase Log table insight_dbchangelog, created in APR_MART schema.

8. When the process is complete, a confirmation message appears with the latest version of Argus Insight.

The following is created as per the values specified in the dbinstaller.properties file:

- **Users**
  - MART_USER
  - STAGE_USER
  - MART_APP_USER
  - MART_HIST_USER
  - AI_LINK_USER
  - RLS_USER
  - AI_APR_USER
  - AI_LOGIN_USER

- **Roles**
  - AI_ROLE
  - AI_APP_ROLE
  - AI_LINK_ROLE

- **Factory Data**
  - Out of the box Factory data is loaded into tables such as ETL_PROCEDURES, CMN_PROFILE_GLOBAL, etc.

- **Database Links**, DB_LINK_ARGUS:
  - From STAGE_USER of Argus Insight to ARGUS_APP of Safety
  - From MART_USER of Argus Insight to ARGUS_APP of Safety
  - From MART_APP_USER of Insight to ARGUS_APP of Safety

- **Tablespaces**

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

STAGE Schema Tablespaces	MART Schema Tablespaces	HIST Schema Tablespaces	APR User Tablespaces
APR_STAGE_DATA_01	APR_MCAS_DATA_01	APR_MCAS_HIST_DATA_01	APR_USER_DATA_01
APR_STAGE_INDEX_01	APR_MCAS_INDEX_01	APR_MCAS_HIST_INDEX_01	APR_USER_INDEX_01

STAGE Schema Tablespaces	MART Schema Tablespaces	HIST Schema Tablespaces	APR User Tablespaces
APR_STAGE_LOB_01	APR_MCAS_LOB_01	APR_MCAS_HIST_ LOB_01	APR_USER_LOB_01
APR_SESM_DATA_01	APR_MCFG_DATA_ 01	APR_MFACT_HIST_ DATA_01	
APR_SESM_INDEX_ 01	APR_MCFG_INDEX_ 01	APR_MFACT_HIST_ INDEX_01	
APR_SESM_LOB_01	APR_MCFG_LOB_01	APR_MCFG_HIST_ LOB_01	
APR_SWHOC_ DATA_01	APR_MEDM_DATA_ 01		
	APR_MEDM_ INDEX_01		
	APR_MEDM_LOB_01		
	APR_MWHOC_ DATA_01		

9. Press **Exit**.

3.4.5 Validate the Schema

1. Navigate to Database > DBInstaller > ValidateSchema.

2. Run the batch script **validate_schema.bat**.

3. When prompted, enter the following parameters:

   ■ Enter instance name: <Argus Insight Database Instance name>

   ■ Enter DBA User Name: <DBA user of Argus Insight>

   ■ Enter Password for DBA User: <DBA User password in Argus Insight>

   ■ Enter Validation Data File Name: The validation control file name (without the .CTL extension)

      For example, VLDN_APR_AI_8.2

   ■ Enter the destination where the log file is to be placed:

      <C:\AI_82\Database\DBInstaller\ValidateSchema>

   ■ Enter the log file name for recording the schema differences:

      <VLDN_APR_AI_8.2_diff.log>

   ■ Enter Validation Output File Name: The validation output file name to record the validation progress:

      <VLDN_APR_AI_8.2.log>

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

5. When the validation process is complete, a confirmation message appears.

   The log files are created at the following location:

   C:\Program Files (x86)\Oracle\ArgusInsight\Database\DBInstaller\ValidateSchema

■ To view any schema discrepancies, such as missing objects, use the Difference Log File.

■ To view the list of errors, which occurred during schema validation, use the Output Log File.

Note:

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

– Objects are RO% views/columns

– GRANTEE is Argus Insight Read-only user

■ If Argus Insight and Argus Mart are installed on the same Database server, ignore the differences due to grants from APR_MART/RLS_USER of Insight to AM_MART_USER/AM_APP_USER of Argus Mart.

3.4.6 Create Argus Insight Read-only User

1. Open DBInstaller\Utilities\ Create_Insight_Ro_User file.

   ■ For Windows—execute the batch script ai_ ro_user.bat

   ■ For Linux—execute the shell script ai_ ro_user

2. When prompted, enter the following parameters:

   ■ Enter TNSNAME Entry to connect to the ARGUS INSIGHT Database: < ARGUS INSIGHT Database name>

   ■ Enter the name of Custom DBA user in Insight Database: < Argus Insight Install user>

   ■ Enter password for install user in Insight Database: <Install user password>

   ■ Enter Mart schema owner name in Insight Database: <Mart User of Insight>

   ■ Enter Argus Insight History schema owner name in Insight Database: <Mart Hist User of Insight>

   ■ Enter Read Only user to be created in Insight Database: <Read-only user to be created in Insight>

   ■ Enter password for Read Only user of Insight Database: <Insight Read-only user password>

3. Press **Exit**.

4. Verify the log files for status information from:

   DBInstaller\Utilities\Create_Insight_Ro_User\AI_RO_User_MMDDYYYY_ HH24MISS.log

3.5 Create Database Links

3.5.1 From Argus Safety to Argus Insight Database

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

1. Create the reverse DB Link by executing the script file from DBInstaller\Utilities\Database_Links\argus_to_mart.

   ■ For Windows—execute the batch script ai_argus_db_link_setup.bat

   ■ For Linux—execute the shell script ai_argus_db_link_setup

2. When prompted, enter the following parameters:

   ■ Enter the Argus Safety Database Tns Name: <Safety Database Instance Name>

   ■ Enter the name of Argus Safety schema owner in Safety Database Instance: <user account that owns the Argus Safety schema>

   ■ Enter the password for Argus Safety schema owner: <password of Argus Schema owner>

   ■ Enter the name of Argus Safety Role: < Argus Safety role>

   ■ Enter the name of Read only Role in Safety Database: <Insight Read-only role, created in Argus Safety>

   ■ Enter the Argus Insight Database Tns Name: <Argus Insight database>

   ■ Enter the name of link user in Insight Database.: <link user of Argus Insight>

   ■ Enter the password for user Link user: <link user password>

3. Verify that the script is successfully connected as <Safety schema owner/Safety schema password>@<Argus Safety Database Name>, and press **Enter**.

4. When the confirmation message appears, press **Enter**.

   Wait until a message *Created <Insight DB Global Name> @ARGUS_TO_MART* appears. This link name gets stored in the key DB_LINK_ARGUS_TO_MART of CMN_PROFILE_GLOBAL of the Argus Safety database.

5. Press **Exit** to close the window.

6. Verify the log files for status from:

   DBInstaller\Utilities\Database_Links\argus_to_mart\ ARGUS_TO_MART_DB_ LINK_MMDDYYYY_HH24MISS.log

3.5.2 From Argus Insight to Argus Safety (manually)

During Fresh installation, the database link from Argus Insight to Argus Safety (DB_ LINK_ARGUS) is created as a part of the installation process. However, you can manually recreate the link DB_LINK_ARGUS.

1. Navigate to DBInstaller\Utilities\Database_Links\db_link_argus.

   ■ For Windows—execute the batch script ai_create_db_link_argus.bat

   ■ For Linux—execute the shell script ai_create_db_link_argus

2. When prompted, enter the following parameters:

   ■ Enter the name of the Safety Database instance: <Safety Database Instance Name>

   ■ Enter the name of the Insight Database instance: <Insight Database Instance Name>

- Enter the name of DBA User in Insight DB: <Insight dba user>

- Enter the password for user &dba_user: <Insight dba user pwd>

- Enter the name of the Read Only User in Safety DB: <Safety Read Only user for Insight>

- Enter the password for Read Only user in Safety: <Read-only user pwd>

- Enter the name of the stage owner in Insight: <Stage user of Insight>

- Enter the password for Stage user: <Stage user password>

- Enter the name of the mart owner in Insight: <Mart user of Insight>

- Enter the password for Mart owner: <Mart user password>

- Enter the name of the mart app owner in &insight_db: <App user of Insight>

- Enter the password for app owner: <App user password>

3. Verify that the script is successfully connected as <Insight DBA user/Insight DBA user pwd>@<Argus Insight>, and press **Enter**.

   Wait until a message *Created <Safety DB Global Name> @DB_LINK_ARGUS* appears for each Stage, Mart, and App user. This link name is stored in the key DB_LINK_ ARGUS of CMN_PROFILE_GLOBAL in the Argus Insight database.

   For example, a typical DB link is:

   - SAF82DB@DB_LINK_ARGUS

   - SAF82DB.US.CORP.COM@DB_LINK_ARGUS

4. Press **Exit** to close the Insight to Argus Database Link Creation window.

5. Verify the log files for status from:

   DBInstaller\Utilities\Database_Links\db_link_argus\DB_LINK_ARGUS_ MMDDYYYY_HH24MISS.log

3.6 Run Initial ETL

1. Navigate to DBInstaller folder.

2. Double click **dbinstaller.exe**.

3. Click **Initial ETL**.

4. Enter the parameters, and click **OK**.

5. Click **Start ETL**.

6. To monitor the ETL progress, execute query on tables:

   - staging_data_insert_log

   - mart_data_insert_log

   For more details on ETL, see Chapter 6, "Extract, Transform, and Load Data."

3.7 Run Additional Grant Scripts for Single DB Instance

If Argus Insight and Argus Mart are running on the same database, provide additional grants for this database instance.

1. Navigate to DBInstaller\Utilities\ am_grants.

- For Windows—execute the batch script am_grants.bat

- For Linux—execute the shell script am_grants

2. When prompted, enter the following parameters:

   - Enter the TNS name to connect to SDM database: <Argus Insight Database Instance name>

   - Enter the name of dba user in Insight Database: <DBA user of Insight Database>

   - Enter Password for User install user: <DBA user password>

3. Press **Exit** when a status message appears as:

   Execution of grants from Insight to Mart User and Mart App User completed

4. Verify the log files for status from:

   C:\Program Files (x86)\Oracle\ArgusInsight\Database\DBInstaller\Utilities\am_grants\AM_GRANTS_ MMDDYYYY_HH24MISS.log

   ---

   Note: After execution of the utility, Argus Insight schema validation file will reflect additional privileges.

4

Upgrade the Argus Insight Data Mart Structure

Argus Insight upgrade process has been moved from Schema Creation Tool to Liquibase for silent installation.

4.1 Prepare for Database Upgrade

Before upgrading, make sure:

1. In the profile switch CMN_PROFILE_GLOBAL, the existing database version is 8.1.1.

2. Take the latest Liquibase build for 8.2.

3. Recreate the Safety RO User of Argus Insight.

4. Recreate the DB_LINK_ARGUS from Argus Insight to Argus Safety (See Section 3.5.2, "From Argus Insight to Argus Safety (manually)")

4.2 Upgrade Database

1. Log in to Argus Insight Web Server.

2. Navigate to Programs > Oracle > Argus Insight > Database > DBInstaller.

3. Open DBInstaller.properties file.

4. Modify the following parameters:

   - **Insight Database**:
     - db_connect_string—connects to the Argus Insight database.

       Syntax: db_connect_string=<host>:<port>/<SID>

       For example, db_connect_string=Dbname.us.xx.com:1521/AI82MT

       Or, db_connect_string=Dbname.us.xx.com:1521/AI82MT.us.xx.com
     - dba_user—specifies the name of the DBA user to run Argus Insight Liquibase Install.

       See Section 3.4.3, "Create the DBA User."

   - **Insight User** of each schema, where password is optional:
     - appschema_mart_user
     - appschema_stage_user

- appschema_mart_app_user

- appschema_mart_hist_user

- appschema_ai_link_user

- appschema_rls_user

- appschema_ai_apr_user

- appschema_ai_login_user

- **Insight Roles:**

- ai_role—specifies Mart User roles

- ai_app_role—specifies App User roles

- ai_link_role—specifies Link User roles

- **Secure Key:**

- argus_securekey_path—path of the file insight.ini in the middle-tier machine from where the DBInstaller.bat is executed.

- **Safety Database:**

- safety_db—Argus Safety database instance name

- safety_ro_user—Argus Insight Read-only user created in Argus Safety

---

Note: For more information on these parameters, see Section 3.2, "Configure dbinstaller.properties file."

---

5. From the command prompt, go to DBInstaller directory.

6. Type dbinstaller.bat, and press **Enter**.

   The Liquibase upgrade begins, and the parameters (as entered) appear on the command prompt screen with password in the hidden mode (****).

7. Keep monitoring the Liquibase progress by querying the Liquibase Log table insight_dbchangelog, created in APR_MART schema.

8. When the process is complete, a confirmation message appears with the latest version of Argus Insight.

9. Validate Schema using the schema validation control file VLDN_APR_AI_8.2.CTL.

   See Section 3.4.5, "Validate the Schema."

5

Configure the Argus Insight Application

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

5.1 Log In to Argus Insight for Configuration and Setup

1. Log in with rights to a workstation from where you can access the Argus Insight application.

2. Start Internet Explorer.

3. In the Address bar, enter the following URL to start the Argus Insight:

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

4. Press **Enter.**

   The Argus Insight Login screen appears.

5. Log in to the Argus Insight application:

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

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

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

   c. Click **Login.**

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

   > **Note:** In case of a multi-tenant setup, you must ensure that the entire configuration is done using the default enterprise.
   >
   > - This will help in copying the configuration to a different enterprise
   > - All the global configuration is available in the default enterprise.

5.2 Configure the Argus Insight Application Profile Switches

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

For detailed information about all the profile switches, see:

- *Oracle Argus Insight CMN Profile Enterprise Table Guide* (CMN_PROFILE_ ENTERPRISE.pdf)

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

5.2.1 Access and Modify the Profile Switches

To access and modify the Argus Insight profile switches:

1. Log in to the Argus Insight application.

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

   The Administration Tools screen appears.

3. Click the **List Maintenance** tab.

4. From the List Maintenance Items group, select **Profile Switches**.

   The Attributes group is updated with the profile switches that you may configure.

   > **Note:** When the Argus Insight Database Source profile switch is set to **Argus Mart**, then in the List Maintenance section, only **Profile Switches** and **Case Series Modification Justification** list maintenance items are available.
   >
   > For more information on this profile switch, see Section 5.2.4, "Set Up the Attributes Specific ONLY to Argus Mart".

5.2.2 Set Up the Populate Data Attributes

You may control data population based on data attributes.

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

Table 5–1   Populate Data Attribute-Value set

Attribute	Value
POPULATE AFFILIATE DATA	0 — Do not bring any affiliate data into the Insight data mart.
	1 — Bring all affiliate data into the Insight data mart.
POPULATE INTERCHANGE DATA	0 — Do not bring any interchange data into the Insight data mart.
	1— Bring all interchange data into the Insight data mart.
	2 — Bring only the SAFETYREPORT, MESSAGES, and EDI_ INFO tables data into the Insight data mart.
POPULATE CASE/CONFIGURATION DATA	0 — Populate configuration data only.
	1 — Populate all the data (both case and configuration data).

Table 5–1   (Cont.) Populate Data Attribute-Value set

Attribute	Value
LEGACY REPORTS CONFIGURATION	0 — Configuration items are not visible. 1— Configuration items are visible. **Note**: If Legacy Reports Configuration switch is set to 1, then legacy reports switches becomes available for obsolete reports, and you must configure the following switches: ■ POPULATE NARRATIVE LANGUAGES TABLE ■ COMPANY LOGO PATH ■ DAYS TO LOCK ■ UDN COLUMN FOR SUPPLIER NAME ■ FOLLOW-UP ACTION CODE ■ POPULATE DLL SLL REPORTS TABLE DATA To configure these switches, refer to Argus Insight 7.0.2 Installation Guide.

To set the data attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.

2. From the List Maintenance Items group, select **Profile Switches**.

3. From the Attributes group, select a profile switch, and click **Modify**.

    The Modify Attributes dialog box appears.

    > **Note:**   See Table 5–1, " Populate Data Attribute-Value set".

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

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

5.2.3 Set Up the Email Attributes

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

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

Table 5–2   Email Specific Attribute-Value set

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

Table 5–2   (Cont.) Email Specific Attribute-Value set

Attribute	Value
ETL EMAIL RECEIVER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry.
	If the Value field blank, then no email messages are sent.
EMAIL SENDER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry.
	If the Value field blank, then no email messages are sent.
FAILED RECIPIENTS STATUS EMAIL ADDRESS	Specify the email address of the user who will receive information about undeliverable emails.

To configure the attributes related to email messages and delivery:

1. On the Administration Tools screen, click the **List Maintenance** tab.

2. From the List Maintenance Items group, select **Profile Switches**.

3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   > **Note:** See Table 5–2, " Email Specific Attribute-Value set".

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

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

   > **Note:** Make sure you validate the network proxy settings before executing the Incremental ETL.
   >
   > Refer to *Oracle Argus Safety Installation Guide, Section 9.1.6 Verify and Update Network Proxy Settings*.

5.2.4 Set Up the Attributes Specific ONLY to Argus Mart

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

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

Table 5–3   Argus Mart Specific Attribute-Value set

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

> **Note:**   These profile switches are optional and should be configured only if you want to run Advanced Conditions on Argus Mart database.
>
> Argus Mart database TNS should be added in the Argus Insight Web Server TNS and Argus Insight Database Server TNS.
>
> Argus Insight Database Server TNS should be added in the Argus Mart Database TNS.

To set these attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.

2. From the List Maintenance Items group, select **Profile Switches**.

3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   > **Note:**   See Table 5–3, " Argus Mart Specific Attribute-Value set".

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

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

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

5.2.5 Set Up the Attributes Specific ONLY to BIP

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

■ BIP WEB URL

■ KEEP REPORT DATA

To define the attributes required for BIP:

1. On the Administration Tools page, click the **List Maintenance** tab.

2. From the List Maintenance Items group, select **Profile Switches**.

3. From the Attributes group, select **BIP WEB URL**.

   a. Click **Modify.**

   The Modify Attribute dialog box appears.

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

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

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

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

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

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

   a. Click **Modify.**

   The Modify Attribute dialog box appears.

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

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

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

5.2.6 Set Up the Attributes Specific ONLY to OBIEE

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

■ BI ANSWERS WEB URL

To define the attributes required for OBIEE:

1. On the Administration Tools screen, click the **List Maintenance** tab.

2. From the List Maintenance Items group, select **Profile Switches**.

3. From the Attributes group, select BI ANSWERS WEB URL, and click **Modify**.

   The Modify Attributes dialog box appears.

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

   For example, this path can be the OBIEE URL:

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

5. Click **OK**.

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

5.3 Configure Duration Value Bands

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

- Time to Onset from First Dose

- Time to Onset from Last Dose

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

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

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

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

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

To modify a duration value band:

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

   The Administration Tools screen appears.

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

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

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

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

For more information on this profile switch, see Section 5.2.4, "Set Up the Attributes Specific ONLY to Argus Mart".

---

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

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

   Note that:

   - The Label column represents the name of the range.

   - The Lower Range (>=) and Higher Range (<) columns contain the minimum and maximum values, respectively.

   - The highest value band includes all values that are greater than the highest range value specified.

5. Modify the values:

   - To modify an existing range, edit the values in the **Lower Range (>=)** and **Higher Range (<)** fields.

   - To add a range, scroll to the current highest range and click in the blank **Higher Range (<)** field.

     Enter a value greater than the current highest range,   and press **Tab** to add a new row.

   - To delete an existing range, click the **Delete** icon next to the row.

     Note that you cannot delete the lowest band.

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

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

5.4 Configure Derivation Functions

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

For example:

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

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

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

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

You can specify more than one attribute.

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

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

5.4.1 Open the Derivation Fields Dialog Box

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

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

   The Administration Tools screen appears.

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

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

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

   The Derivation Fields dialog box appears.
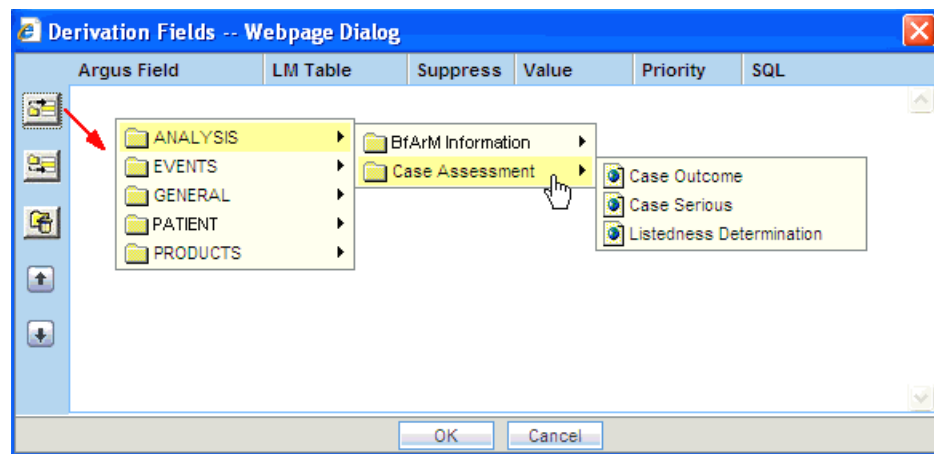
5.4.2 Icons in the Derivation Fields Dialog Box

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

Table 5–4   Icons in the Derivation Fields Dialog Box

Click…	To…
	Add a derivation field element (row) above the currently selected row
	Add a derivation field element (row) below the currently selected row
	Delete the currently selected derivation field element (row)
	Move the selected row up

Table 5–4 (Cont.) Icons in the Derivation Fields Dialog Box

Click…	To…
	Move the selected row down

5.4.3 Field Mapping Derivation Rules

Table 5–5 lists the available field mapping derivation rules for Argus Insight.

Table 5–5 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.

5.4.4 Fields and Check Boxes in the Derivation Fields Dialog Box

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

5.4.4.1 LM Table

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

5.4.4.2 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.

5.4.4.3 Value

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

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

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

Causality Rule

Parameters: VALUE, REPORTABILITY

where:

VALUE = New value for the rule

REPORTABILITY = Lower value of the group

Example: NewCausality,1

Report Type Rule

Parameters: VALUE, INC_LIT, INC_TRIAL, ABRV

where:

VALUE = New value for the rule

INC_LIT = 1 if Literature Report Type else 0

INC_TRIAL = 1 if Clinical Trial Report Type else 0

ABRV = A 3-letter abbreviation for the Report Type

Example: NewReportType,0,1,NRT

Age Group Rule

Parameters: VALUE, GROUP_LOW, GROUP_HIGH

where:

VALUE = New value for the rule

GROUP_LOW = Lowest value of the age group

GROUP_HIGH = Highest value of the age group

Example: NewAgeGroup,25,50

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

Example: Unknown,70,

Last Daily Dose Rule

Parameters: VALUE, DAILY_DOSE_SORTING_ORDER

where:

VALUE = New value for the rule

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

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

5.4.4.4 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.

5.4.4.5 SQL

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

> **Note:**   The SQL statement must follow the correct syntax.
>
> The system does not validate the length of the new values against the database. Make sure that new values being inserted into the Insight data mart do not exceed the limit defined in the database.

Guidelines for correct syntax:

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

  Correct: SELECT CASE_ID FROM RPT_CASE WHERE…

  Incorrect: SELECT RPT_CASE.CASE_ID FROM RPT_CASE WHERE…

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

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT   CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

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

  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

  Incorrect: SELECT DISTINCT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…

5.5 Configure the Argus Insight Windows Service

To configure the Argus Insight Windows service:

1. Log in to the Argus Insight Web Server.

2. Click **Start**, and select **Run.**

3. In the text box, enter **services.msc**, and click **OK.**

    The Services screen appears.

4. Right-click **Argus Insight Service**, and select **Properties.**

    The Argus Insight Service Properties dialog box appears.

5. Set the value of the **Startup type** field to **Automatic.**

6. Click **Start** to start the Argus Insight Service.

7. Click **OK** to apply the changes.

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

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

5.6 Configure the IIS File Download Limit

To configure the IIS file download limit for Windows 2012:

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

2. Double-click **ASP** in the right pane.

   The ASP dialog box appears.

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

4. From Actions in the left pane, click **Apply**.

5. Restart the IIS service.

   a. Click **Start**, and select **Run.**

   b. In the text box, enter **iisreset -start**.

   c. Click **OK.**

5.6.1 Configure the Maximum Requesting Entity Body Limit

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

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

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

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

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

2. Double-click **ASP** in the right pane.

   The ASP dialog box appears.

3. Expand **Limit Properties** and change the **Maximum Requesting Entity Body Limit** from 200000 Bytes (default) to a large value (preferably 5000000 Bytes).

4. From Actions in the left pane, click **Apply**.

5. Restart the IIS service.

   a. Click **Start**, and select **Run.**

    b. In the text box, enter **iisreset -start**.

    c. Click **OK.**

5.7 Use Export and Import to Copy Configuration Data

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

- Before importing or exporting to or from a network drive, verify that you have mapped the network drive. This tool does not support direct access to network drives.

- Before copying Argus Data, incremental ETL should be completed on Source Insight Database from Source Argus.

- It is assumed that the configuration of the instance of Argus used to run Initial and Incremental ETL on the source Argus Insight data mart will also be copied and applied on the new Argus Instance which will be associated with the new Argus Insight data mart.

- Data must be imported after loading Factory Data and before running Initial ETL on destination environment.

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

5.7.1 Export Data

1. Go to Utilities\Copy_Config and run the **Data_ExportConfigOnly.bat** file.

   The Export Utility command prompt screen appears.

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

   a. TNSNAMES entry of the Argus Insight Database

   b. DBA User

   c. DBA User Password

   d. Mart Schema Owner Name

   e. Mart Schema Owner Password

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

   Enter a directory path specific to your database environment.

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

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

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

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

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

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

    i. Name of the log file

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

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

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

- TDE is setup and Wallet is open

- TDE is not setup and Wallet is not open

The command prompt screen with Directory creation status appears.

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

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

The command prompt screen with list of parameters appears.

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

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

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

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

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

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

5.7.2 Import Data

1. Go to Utilities\Copy_Config and run the **Data_ImportConfigOnly.bat** file.

The Import Utility command prompt screen appears.

2. Press **Enter** if all prerequisites are satisfied.

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

a. TNSNAMES entry of the Argus Insight Database

b. DBA User

c. DBA User Password

d. Mart Schema Owner Name

e. Mart Schema Owner Password

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

Enter a directory path specific to your database environment.

INSIGHT.DMP created in the export process is copied here. Beside, Import_log.log is also created here.

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

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

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

> Enter a directory path specific to the machine where the Copy Configuration utility is being run.
>
> The user specified log files are generated here.
>
> Besides, make sure that the files named application_type_check.sql, insight_export_tables.par, and truncate_delete_tables.sql that were generated during export process are also copied here.

   i. Name of the log file

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

   The command prompt screen with the Encryption Wallet Verification status appears.

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

   ■ TDE is setup and Wallet is open

   ■ TDE is not setup and Wallet is not open

   The command prompt screen with Directory Creation status appears.

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

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

   The command prompt screen with list of parameters appears.

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

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

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

   A data import completed screen appears.

10. Press **Enter** to Exit.

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

5.8 Use Argus Safety to Configure Enterprises for Argus Insight (for Mutli-tenant installation only)

You must be a valid LDAP user and have access to the Argus Safety global home page.

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

To create an enterprise in Argus Insight:

1. Log in to the Global Enterprise Management portlet.

2. From the Enterprises folder, select an enterprise from the left pane.

   The Enterprises folder includes enterprises as per you access privileges.

3. To create the selected enterprise in Argus Insight, click **Copy Enterprise to Insight**.

   Note that the **Copy Enterprise to Insight** button is:

   ■ disabled if the selected enterprise already exists in Argus Insight.

   ■ enabled if you have Copy Configuration role in any of the listed enterprises.

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

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

   - The enterprise has already been created in Argus Insight.

   - You have been assigned Copy Configuration privileges for the enterprise.

5. Click **Setup.**

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

6. Click **Finish**.

5.9 Secure 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 make sure 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

6

Extract, Transform, and Load Data

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

6.1 Prerequisites, Cautions, and Warnings

Before running the Initial ETL, make sure:

- The Auto extend is set to ON for all the data files in the database that are related to staging and Insight Mart.

- The POPULATE CASE/CONFIGURATION DATA profile switch is configured to the desired value.

In addition, note that:

- Since the initial ETL requires a huge amount of temporary space, set the temporary space to 100 GB to prevent data errors. After completing the Initial ETL, reduce the temporary space to 30 GB.

- After the Initial ETL completes, the balancing log may show differences between the Argus (Stage) and Insight Mart table counts. This is because of the derivation rules applied to the Insight data mart.

- The system may display the following message:

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

  Ignore this warning for all MedDRA tables.

- **Do not** run incremental ETL for more than 50,000 cases. Run the Initial ETL again if the number of cases exceeds 50,000.

- The Argus Insight ETL will not populate the Argus Mart database.

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

6.2 Run the Initial ETL

1. Log in to the Argus Insight Web Server as a user with administrator privileges.

2. Click **Start.**

3. Navigate to **Programs > Oracle > Argus Insight,** and then select **Schema Creation Tool.**

4. Click **Initial ETL.**

The Oracle Database Connect dialog box appears.

5. To connect to the Oracle Database:

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

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

   c. Click **OK.**

   The Initial ETL Status dialog box opens.

6. Click **Start ETL**.

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

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

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

   While the ETL is in progress, you can:

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

     Closing the dialog box does not affect the execution of the ETL process.

   ■ To halt the ETL process, click **Stop ETL**.

     For more information about this option, see Section 6.2.3, "Stop the Execution of ETL."

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

6.2.1 Generate the Balance Logs

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

To generate the balance logs:

1. Wait until the dialog box that reports the initial ETL completed successfully appears.

2. Click **Balancing Logs.**

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

3. Click **OK**.

   The command prompt screen appears.

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

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

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

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

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

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

   The Balancing Reports are located at:

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

The log files are named as:

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

6.2.2 Close the Initial ETL Status Dialog Box

1. Click **Close.**

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

2. Click **OK.**

6.2.3 Stop the Execution of ETL

You may choose to stop an ETL in progress.

To halt the execution of the initial ETL process:

1. Click **Stop ETL.**

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

2. Click **OK.**

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

   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.**

6.3 Run the Initial ETL Again

To start the ETL process from the beginning:

1. Click **Run ETL.**

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

2. Click **OK.**

   The Oracle Database Connect dialog box appears.

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

   The initial ETL process starts from the beginning.

6.4 Process a Failed ETL

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

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

- To continue the failed Initial ETL process, click **Continue**.

- To ignore the failed Initial ETL process, click **Ignore**.

- For ETL Data Exclusion, click **Modify Attributes**, if PRE_REQ_CHECK_FLAG switch is set to ABORT.

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

6.4.1 Continue the Failed Initial ETL Process

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

1. Double-click on the ETL error.

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

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

3. Right-click on the ETL Error, and click **Copy** to copy the error data.
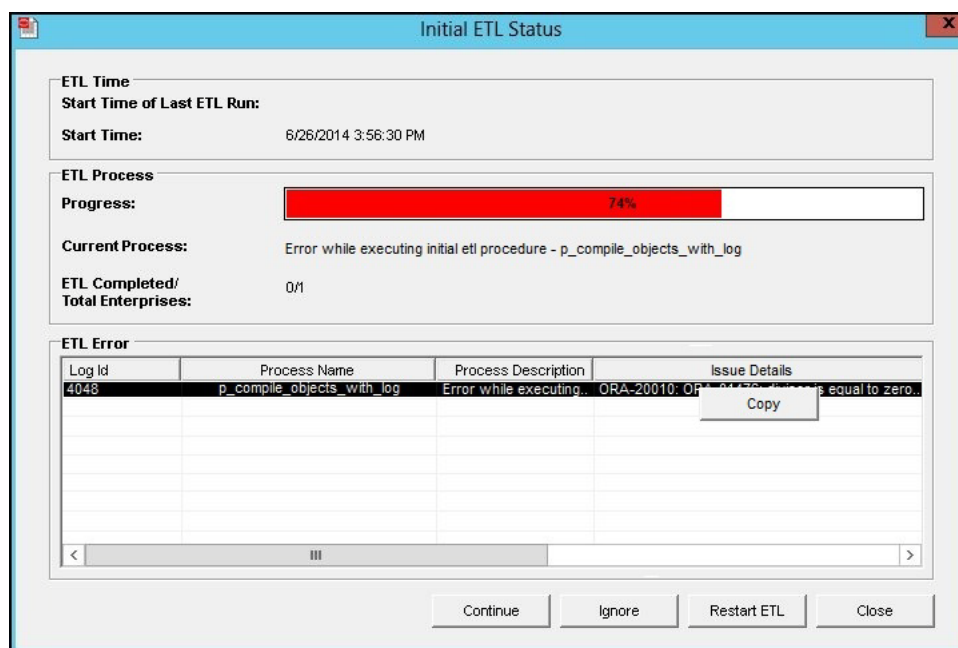
4. Click **Continue** to continue the failed ETL process.

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

5. Click **OK.**

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

6.4.2 Ignore the Failed Initial ETL Process

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

1. Click **Ignore**.

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

2. Click **OK.**

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

6.4.3 Modify the Attributes of ETL Data Exclusion

You must modify these attributes before ETL execution.

1. Log in to the Argus Insight application as a user with administrator privileges.

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

The Administration Tools screen appears.

3. Click the **List Maintenance** tab.

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

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

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

The Modify Attribute dialog box appears.

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

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

   - If you want the ETL process to abort when it encounters cases with erroneous data, enter **ABORT.**

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

6.5 Restart 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.**

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

2. Click **OK.**

The Oracle Database Connect dialog box appears.

3. Enter the APR_MART user password, the Argus Insight Database name, and click **OK**.

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

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

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

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

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

7

Configure the BIP Environment

When 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.

7.1 Create PRMART JDBC Connection

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

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

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

To connect the BIP and the database:

1. Log on to BIP using the administrator credentials.

    The BIP home page appears.

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

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

    The Data Sources screen appears.

4. Click **Add Data Source**.

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

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

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

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

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

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

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

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

    f. Click **Test Connection**.

        If successful, a confirmation message appears.

6. Click **Apply**.

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

   A connection between BIP and the database is successfully created.

7.2 Manage Users and Roles: BI Publisher Standalone Installation with BI Publisher Security

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

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

7.2.1 Create Users and Assign Roles to Users

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

1. Log on to BIP using the administrator credentials.

   The BIP home page appears.

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

   Refer to Section 6.2 > Step 2.

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

   The Users screen appears.

4. Click **Create User**.

   The Create User screen appears.

5. In the **Username** field, enter the name of the user.

6. In the **Password** field, enter the password.

7. Click **Apply**.

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

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

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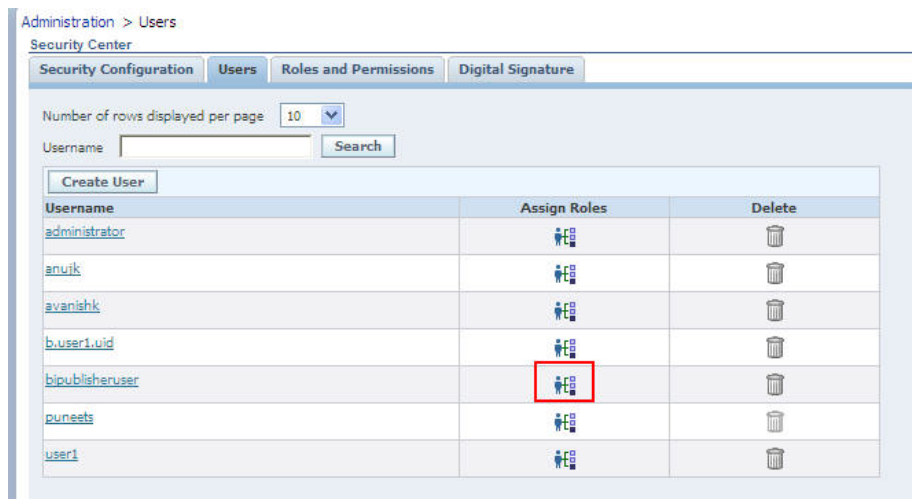
The Assign Roles screen appears.

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

See Section 7.2.2, "Create Roles, Add Data Sources, and Assign Roles" for the steps to create custom roles.

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

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

10. Click **Apply**.

The selected roles are assigned to the user.

For the list of users that you need to configure using BIP, refer to Section 7.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model".

7.2.2 Create Roles, Add Data Sources, and Assign 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.

1. Log on to BIP using the administrator credentials.

The BIP home page appears.

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

Refer to Section 6.2 > Step 2.

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

The Roles and Permissions screen appears.

4. Click **Create Role**.

The Create Role screen appears.

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

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

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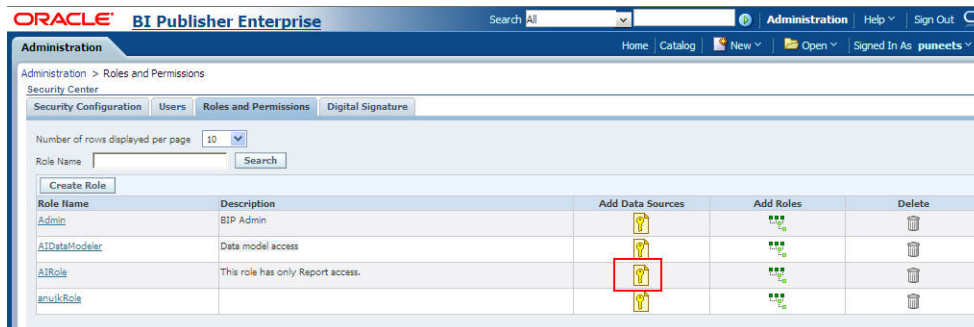
The Add Data Sources screen appears.

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

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

The Roles and Permissions screen appears.

See Section 7.1, "Create PRMART JDBC Connection" for the steps to create the JDBC connection.

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

The Add Roles screen appears.

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

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

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

For the list of roles that you need to configure using BIP, refer to Section 7.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model".

7.3 Manage Users and Roles: BI Publisher Standalone Installation with OFM Security

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

7.3.1 Create Users and Assign Roles to Users

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

For the list of users that need to be configured, refer to the Section 7.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model".

7.3.2 BI Publisher Standalone Installation in OFM Security

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

7.3.2.1 Create Users and Groups

1. Open the WebLogic Administration Console.

2. Navigate to Security Realms > myrealm > Users and Groups > Groups tab.

3. From the Groups section, and click **New**.

    The Create a New Group dialog box appears.

4. Create the following groups by entering the **Name** and **Description**, and click **OK.**

    - AIAdminGroup

    - AIAuthorGroup

    - AIConsumerGroup

To create users in the Fusion Middleware Control:

1. Open the WebLogic Administration Console.

2. Navigate to Security Realms > myrealm > Users and Groups > Users.

3. From the Users section, and click **New**.

    The Create a New User dialog box appears.

4. Enter the parameters, and click **OK**.

5. To assign a group to the user, from the Groups tab, select a Group, and click **Save**.

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

7.3.2.2 Create Roles and Policies

To create new application roles:

1. Login to Fusion Middleware Control Enterprise Manager.

2. Go to WebLogic Domain > Security > Application Roles.

    The Application Roles dialog box appears.

3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search** ▶.

    The default role available in clean slate installation appears.

4. Click **Create**.

    The Create Application Role dialog box appears.

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

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

    The Add Principal dialog box appears.

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

    A list of principals appears.

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

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

   The Add Principal dialog box appears.

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

    A list of principals appears.

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

    The Membership for **AIAdminRole** appears.

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

13. To add **AIConsumerRole**, repeat from Step 4 to Step 11.

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

To create new application policy:

1. Login to Fusion Middleware Control Enterprise Manager.

2. Go to WebLogic Domain > Security > Application Policies.

   The Application Policies screen appears.

3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.

4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.

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

6. From the list of Searched Principals, select **AIAdminRole**, and click **OK**.

7. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.

8. Select the **Resource Types** radio button.

9. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.

10. From the Search Results, select **oracle.bi.publisher.permission** (BIP Administer Server), and click **Continue**.

    The Add Permission dialog box appears.

11. For **Permission Actions**, select **All** (_all_), and click **Select**.

12. Add Resource Name as **oracle.bi.user** with **Impersonate** permission.

    The new AI Admin policy has all the permissions.

Note: Make sure all the fields are either selected or entered manually.

---

13. Repeat from Step 4 to Step 12, to add the following:

Name	Grantee	Resource Permissions
AI Author	AIAuthorRole	BIP Develop Report
		BIP Develop Data Model
AI Consumer	AIConsumerRole	BIP Access Excel Report Analyzer
		BIP Access Online Report Analyzer
		BIP Access Report Output
		BIP Schedule Report

> **Note:** For more details, refer to *Section 2.8.3.2 Creating Application Policies Using Fusion Middleware Control* from *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf.*

7.3.3 Create Roles, Adding Data Sources, and Assign Roles in WebLogic Enterprise Manager

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

1. Log on to the Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.

2. In the left pane, expand the **Business Intelligence** folder, and click **coreapplication**.

   The Coreapplication screen appears in the right pane.

3. In the Application Policies and Roles section, click **Configure and Manage Application Roles**.

   The Application Roles screen appears.

4. From the **Application Stripe** drop-down list, select the required application stripe.

5. Select any existing role (for example, BIConsumer), and click **Create Like**.
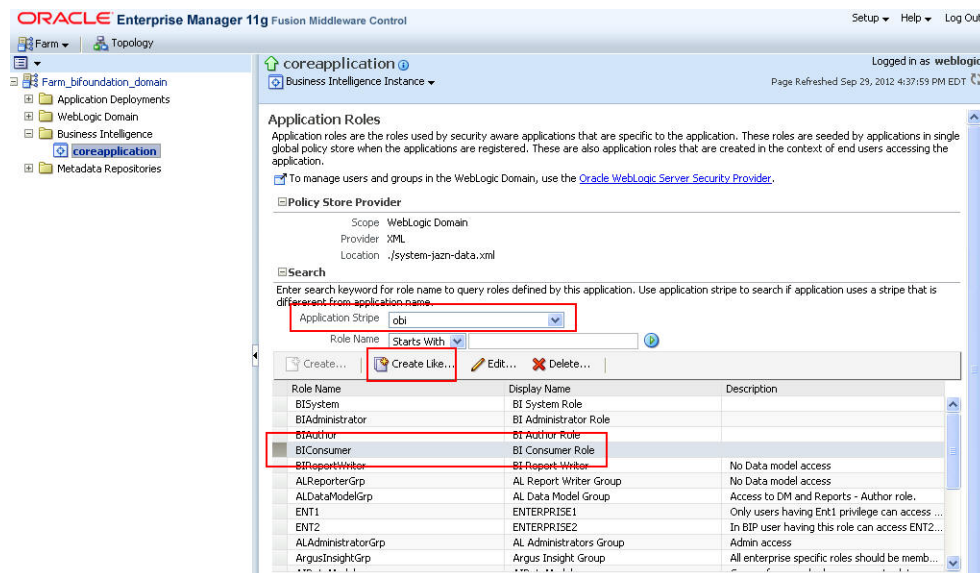
The Create Application Role screen appears.

6. In **Role Name** field, enter the name of the role.

7. Optionally, enter the **Display Name** and **Description** for the role.

8. To add any existing application role/group/user to the new role, click **Add**.
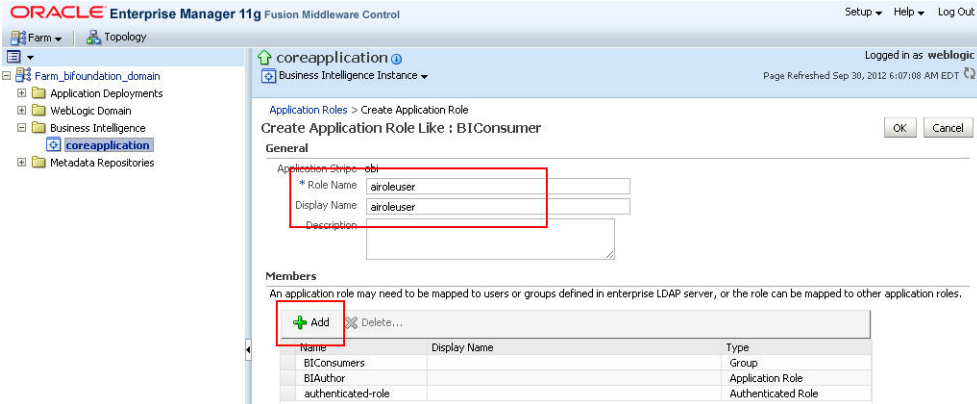
The Add Principal screen appears.

9. To display the list of all the roles, groups, and users that are created in LDAP server, click the **>** icon next to the **Display Name** field.

10. Select the name of the role, group, or user that you want to add to the new role, and click **OK**.

11. Repeat steps 8 to 10 to add more roles, users, and groups to the new role.

12. On Create Application Role screen, click **OK** to save the changes.

    When you have created the role and added the required list of users, roles, and groups to the new role, you must add the **PRMART** data source to the new role.

13. Log on to BIP using the administrator credentials.

    The BIP home page appears.

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

    Refer to Section 6.2 > Step 2.

15. In Security Center section, click **Roles and Permissions**.

    The Roles and Permission screen appears.

    You can view the name of the new role which you have just created in the list of role names.

16. Click the **Add Data Sources** icon corresponding to the name of the new role.

    The Add Data Sources screen appears.

17. From the Available Data Sources section, select **PRMART**, and click the **Move (>)** icon to move the PRMART data source to the Allowed Data Sources section.

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

    For more information, refer to the Oracle BIP Administrator's Guide > Creating Application Roles Using Fusion Middleware Control section.

    For the list of roles that need to be configured, refer to the Section 7.4, "Configure BIP Users and Roles: Oracle Fusion Middleware Security Model".

7.3.4 Create Application Policy

Once you have created the new role and assigned the required roles, users, and data sources to the role, you also need to create the application policy for the new role.

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

> **Note:** The steps mentioned in this section are valid for creating **BIReportWriter** application policy.

To create the application policy for the new role, execute the following steps:

1. Log on to the Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.

2. In the left pane, expand the **Business Intelligence** folder, and click **coreapplication**.

   The Coreapplication screen appears in the right pane.

3. In the Application Policies and Roles section, click **Configure and Manage Application Policies**.

   The Application Policies screen appears.

4. From the **Application Stripe** drop-down list, select **obi**.

5. Select the **BIAuthor** policy, and click **Create Like**.

   The Create Application Grant Like screen appears with the **Grantee** and **Permissions** sections.

6. In the Grantee section, click **Add**.

   This displays the **Add Principal** Screen.

7. To retrieve the list of all the available application roles, click the **>** icon next to the **Principal Name** field.

8. From the Searched Principals section, select the name of the role (for example, BIReportWriter), and click **OK**.

   The Create Application Grant Like screen appears.

9. From the list of Permission Classes, select the **developDataModel** resource name, and click **Delete.**

10. Click **OK** to apply the changes.

7.3.5 Upload 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.

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

   Drive:\<Argus Insight Installation Folder>\ArgusInsight\BIP\Repository

2. Log on to BIP using the BI Admin User credentials.

The BIP home page appears.

3. From the menu bar, click **Catalog**.

   The Catalog screen with the **Folders** and **Tasks** sections appears.

4. From Folders section in the left pane, click **Shared Folders**.

5. From Tasks section in the left pane, click **Upload**.

   The Upload dialog box appears.

6. Click **Browse** and navigate to the location where you have saved the **Argus Insight.xdrz** file on the local file system.

7. Click **Upload**.

   After successful upload, an **Argus Insight** folder is created in **Shared Folders**.

8. Expand the **Argus Insight** folder to verify that the **Generic Line Listing Data Model** exists in the **Data Models** sub-folder and the **Generic Line Listing Report** in **LE** and **RTF** formats exists in the **Reports** sub-folder.

7.4 Configure BIP Users and Roles: Oracle Fusion Middleware Security Model

This section lists the names of the <Admin Users> and roles that you need to configure using the steps given in Section 7.2, "Manage Users and Roles: BI Publisher Standalone Installation with BI Publisher Security" and Section 7.3, "Manage Users and Roles: BI Publisher Standalone Installation with OFM Security".

Table 7–1   Configuring BIP Users: Oracle Fusion Middleware Security Model

User	Description
BI Admin User	An Admin user refers to the user who has BI Publisher administrative rights. This user should belong to the **BIAdministration** functional role.
Data Modeler Users	An Argus Insight Data Model user refers to the user who should have access to both **Data Models** and **Reports** in the **Argus Insight** folder. This user should belong to **AIDataModeler** custom role.
	There are Enterprise specific Modeler users, who have access to **Data Models** and **Reports** in Enterprise specific folders and **Argus Insight** folder. These users should have Enterprise specific Modeler roles assigned to them. This user should belong to Enterprise specific Modeler roles.
Users	An Argus Insight Role (AIRole) user refers to the user who should have access to **Reports** only, and should have Read-only access to the Data Model which is required to create the reports. This user should belong to **AIRole**.
	There can be users who have access to reports of specific Enterprises. These users can Read/Write reports in **Enterprise specific Report** folder and **Argus Insight Report** folder. However, these users have Read-only access to the Data Models in the Enterprise specific **Data Model** and Argus Insight **Data Model** folder. This user should belong to Enterprise specific Report roles.
Global Admin Users	An AI Admin Role user should have full access to the **Argus Insight** folder (Read/Write/Delete).
	An Enterprise specific Admin user should have full access to the Enterprise specific folders (Read/Write/Delete) and **Argus Insight folder** (Read/Write/Delete).

7.4.1 Configure BIP Roles

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

Table 7–2   Configuring BIP Roles

Role	Users/Roles to be added
BIAdministration (Functional Role)	Super user who has full access to any folder and BIP Administration access
AIRole	All Argus Insight role users, **AIDataModelerRole**, and All Enterprise Report Roles (for specific enterprises)
AIDataModelerRole	All AI Data Modeler Users, All Enterprise Modeler Roles, and **AIAdminRole**
Enterprise Report Role	Users that belong to a specific Enterprise with **Reports** access and Enterprise Modeler Role
Enterprise Modeler Role	Users that belong to a particular Enterprise with both **Data Models** and **Reports** access
Enterprise Admin Role	Enterprise specific Admin users. These users should have full access to the Enterprise specific folders.
AIAdminRole	Any User with this role should have full access to the Argus Insight Folder. The Enterprise Admin Role should be added to this role.
BIAdministrator (Functional Role)	BI Admin User
BIAuthor (Functional Role)	**AIDataModelerRole**
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**

7.4.2 Folder Level Permissions

View folder level permissions for BI Publisher Standalone Installation:

You cannot see the permissions of shared folder for BIP Stand-Alone installation. Besides, the Argus Insight folder permissions appears.
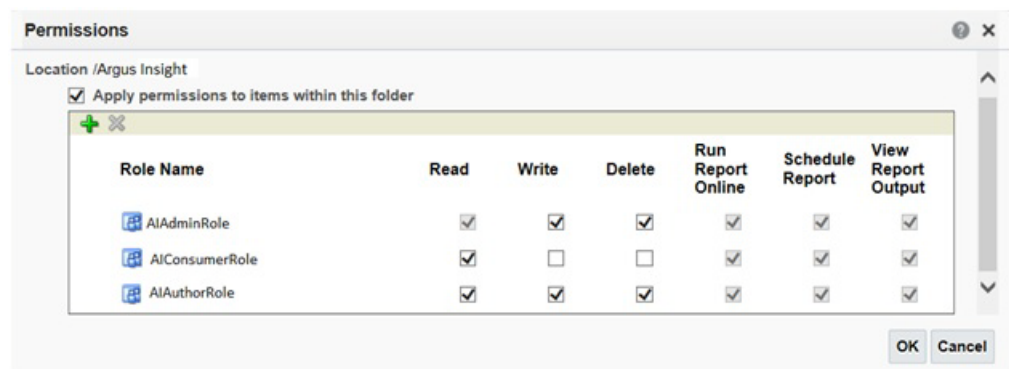
To assign folder level permissions for BIP Integrated Installation (OBIEE+BIP):

1. Login to OBIEE Analytics with the WebLogic user credentials.

2. Go to Catalog > Shared Folders > Tasks > Permissions.

   The Permissions dialog box appears.

3. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
AI Admin Role	Open (Read, and Traverse)
AI Author Role	Open (Read, and Traverse)
AI Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

4. Go to Shared Folders > Argus Insight > Permissions.

   The Permissions dialog box appears.

5. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

8

Configure the OBIEE Environment

8.1 Pre-installation Configuration

Before integrating OBIEE with Argus Insight, make sure to complete the following tasks:

1. Install JDK 1.8 on the machine where Argus Insight is installed.

2. Since the data for analysis is based on Argus Mart schema and not the Insight Mart schema, the TNS entry for the Argus Mart schema should be present in the OBIEE 12c home at the following path:

   <obiee_home>\user_projects\domains\bi\config\fmwconfig\bienv\core\

   > **Note:** In this chapter, **bi** is referred as the domain name. This domain name may differ based on your configuration.
   >
   > *<obiee_home>/user_projects/domains/bi*

3. Set up the TNS for Oracle Client Home in the PATH variable.

4. Install Argus Mart.

   When the installation is complete, the new tables, indexes, packages and all the objects required for OBIEE are created in the Argus Mart schema.

   Additionally, a read only user AM_BI_USER with read-only privileges on BI Objects is created.

   For detailed information on installing and upgrading Argus Mart schema, refer to *Oracle Argus Mart Installation and Administration Guide*.

8.2 Configure the OBIEE Repository and Web Catalog using the BAR File

Oracle Business Intelligence Application Archive (BAR) file is a compressed archive file that contains a cohesive set of BI metadata artifacts (data model, content model, and authorization model). When deploying BI application from one server to another you can use these BAR files to transfer the metadata instead of transferring the RPD, Catalog, and the Security Model separately.

A BAR file contains the following BI application module artifacts:

■ Data model metadata for the Oracle BI Server. This metadata is xml-based but functionally equivalent to an .RPD file.

- Presentation Services catalog metadata for a service instance.

- Security policy metadata containing application role and application role memberships, and permission and permission set grants for a service instance.

- A manifest file declaring the dependencies of the BAR file.

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

8.2.1 Import the BAR file in an existing OBIEE instance

Before importing the BAR File, make sure:

- OBIEE 12.2.4 is installed

- The Administrator Console is up and running

  (validate it from *http://<machinename>.<port>/console*)

- The Enterprise Manager (Fusion Middleware Control) is up and running

  (validate it from *http://<machinename>.<port>/em*)

To import the BAR file:

1. Copy the BAR file from *<AI HOME>OBIEE\BAR File\ssi.bar* to a local folder on the machine where the OBIEE is installed.

   For example, copy the file at *C:\AIOBIEE*.

2. Login to the Enterprise Manager with the WebLogic credentials.

3. Click **Target Navigation.**

   The Target Navigation drop-down menu appears.

4. Go to Business Intelligence > biinstance.

   The Business Intelligence Instance screen appears.

5. From the Availability tab, select **Processes**, and click **Stop All**.

   A confirmation dialog box appears.

6. Click **Yes**.

   All the running processes are stopped.

7. Go to the command prompt, and start the WebLogic Scripting Tool (using **wlst.cmd** on Windows, and **wlst.sh** on Unix/Linux) from the following path:

   <OracleBI Home>\Middleware\oracle_common\common\bin

8. To know the **BI Service Instance key**, type the following command, and press Enter.

> *listBIServiceInstances(domainHome)*

where, Domain Home is the directory of the BI Install domain, the default path is:

<obiee_home>/user_projects/domains/bi

The Key appears at the end of the command.

For example, **ssi** appears as the Key.

9. Exit WLST using the **exit ()** command.

10. To import the BAR file:

   a. Go to the Domain Home path:

      <obiee_home>/user_projects/domains/bi/bitools/bin

   b. Execute the following command:

      importarchive.cmd BI Service Instance key *<complete path of bar file to import>*

      For example, importarchive.cmd ssi C:\ai82\ssi.bar

11. Go to Enterprise Manager, from the Availability tab, select **Processes**, and click **Start All**.

   A confirmation dialog box appears.

12. Click **Yes**.

   The BAR file imports the RPD, Catalog and the Security model.

To check if the BAR file has imported RPD, Catalog, and the Security Model:

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

   The following roles are imported as default application roles:

   ■ AI Admin Role

   ■ AI Author Role

   ■ AI Consumer Role

   For a list of privileges assigned to these roles, refer to Section 8.6, "OBIEE Default Application Roles."

2. To modify the Connection Pool Settings:

   a. From the following path, right click the **admintool.cmd** file, and click **Run as Administrator**.

      <obiee_home>\user_projects\domains\bi\bitools\bin

      The BI Admin Tool opens.

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

> **Note:** To open the RPD in online mode, you must set the Open Database Connectivity (ODBC). Refer to the Appendix A, "Create ODBC Connection for OBIEE Administration Tool."
>
> If OBIEE is installed on the Unix or Linux machine, set up the Oracle Business Intelligence Developer Client Tool on any Windows machine to access the BI Administration Tool.

    c. Click the **Connection Pool**, and modify the **Data source name**, **User name**, and **Password**.

    Modify both the connection pools: AI80OBIEE_CP and AI80OBIEE_CP_ InitBlocks.

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

Ignore the warning messages that appear during the consistency check.

4. Create OBIEE Groups and Users. (See Section 8.4, "Create Users and Groups in OBIEE")

5. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 8.5, "OBIEE Catalog Folder-level Permissions")

6. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics with WebLogic user credentials.

Go to Administration > Security > Manage Privileges.

For a list of privileges assigned to these roles, refer to Section 8.6, "OBIEE Default Application Roles."

7. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

8. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

8.2.2 Import the BAR file to create a new OBIEE Instance

1. Copy the BAR file from *<AI HOME>OBIEE\BAR File\ssi.bar* to a local folder on the machine where the OBIEE is installed.

2. When creating an instance in OBIEE 12c, enter the BAR file path in the **Path** field of the OBIEE Initial Application wizard screen.

3. When the installation is completed successfully, and all the processes are up, open the RPD in online mode, and change the **Connection Pool Settings**. (See To check if the BAR file has imported RPD, Catalog, and the Security Model: > Step 2)

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

Ignore the warnings that appear during the consistency check

5. From the Enterprise Manager > Stop and Start the BI processes.

6. Create OBIEE Groups and Users. (See Section 8.4, "Create Users and Groups in OBIEE")

7. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See Section 8.5, "OBIEE Catalog Folder-level Permissions")

8. To view and administer privileges for the Oracle Business Intelligence components, login to OBIEE Analytics with WebLogic user credentials.

   Go to Administration > Security > Manage Privileges.

   For a list of privileges assigned to these roles, refer to Section 8.6, "OBIEE Default Application Roles."

9. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

10. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

8.3 Configure OBIEE Repository and Web Catalog Manually

1. Copy the RPD, and Catalog files from *<AI HOME>OBIEE\RPD\ and <AI HOME>OBIEE\Catalog folders* to a machine where the OBIEE is installed.

2. Open the RPD Admin tool in offline mode from the following path:

   <obiee_home>\user_projects\domains\bi\bitools\bin\ admintool.cmd

   The default Repository Password is **insight123**.

3. Change the **Connection Pool Settings**. (See To check if the BAR file has imported RPD, Catalog, and the Security Model: > Step 2)

4. Save the changes, and close the RPD.

5. From the command prompt:

   a. Navigate to the *<obiee_home>\user_projects\domains\bi\bitools\bin*

   b. Run the following command:

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

      For example, *datamodel.cmd uploadrpd -I C:\AIOBIEE\RPD\ArgusInsight.rpd -W insight123 -U weblogic -P weblogic1 -SI ssi*

6. Login to the Enterprise Manager with the WebLogic credentials.

7. Click **Target Navigation**.

   The Target Navigation drop-down menu appears.

8. Go to Business Intelligence > biinstance.

   The Business Intelligence Instance screen appears.

9. From the Availability tab, select **Processes**, and click **Stop All**.

   A confirmation dialog box appears.

10. Click **Yes**.

    All the running processes are stopped.

11. Go to *Catalog\argusinsight\root\shared* folder:

    a. Copy **argus+insight** folder, and **argus+insight.atr** file.

      b. Paste in *<obiee_home>\user_projects\domains\bi\bidata\service_*
      instances\ssi\metadata\content\catalog\root\shared folder.

12. Go to Enterprise Manager, from the Availability tab, select **Processes**, and click
Start All.

    A confirmation dialog box appears.

13. Click **Yes**.

14. Create User Groups and Users manually in Admin Console. (See Section 8.4.1,
"Create Users and Groups in WebLogic Server.").

15. Create Roles and policies manually in Enterprise Manager. (See Section 8.4.2,
"Create Roles and Policies with Fusion Middleware Control.")

16. To view and administer privileges for the Oracle Business Intelligence
components, login to OBIEE Analytics with WebLogic user credentials.

17. Go to Administration > Security > Manage Privileges.

    For a list of privileges assigned to these roles, refer to Section 8.6, "OBIEE Default
Application Roles."

18. Go to Catalog, and set the folder level permissions for the OBIEE Groups. (See
Section 8.5, "OBIEE Catalog Folder-level Permissions")

19. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files
and Metadata**.

20. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid
user credentials.

> **Note:** All the WLST commands are case sensitive.
>
> To start the WebLogic Scripting Tool on Unix or Linux, use wlst.sh
> command, rest all of the commands mentioned in the procedure
> remains same.
>
> While executing the WLST commands on Windows server, you must
> use forward slash (/) to avoid any error messages. For example:
>
> ```
> C:/AIBOEE/instance/import/ssi.bar
> ```

8.4 Create Users and Groups in OBIEE

8.4.1 Create Users and Groups in WebLogic Server

To create users and groups in OBIEE:

1. Open the WebLogic Administration Console.

2. Navigate to Security Realms > myrealm > Users and Groups > Groups tab.

3. From the Groups section, and click **New**.

    The Create a New Group dialog box appears.

4. Create the following groups by entering the **Name** and **Description**, and click **OK.**

    ■   AIAdminGroup

- AIAuthorGroup

- AIConsumerGroup

To create users in the Fusion Middleware Control:

1. Open the WebLogic Administration Console.

2. Navigate to Security Realms > myrealm > Users and Groups > Users.

3. From the Users section, and click **New**.

   The Create a New User dialog box appears.

4. Enter the parameters, and click **OK**.

5. To assign a group to the user, from the Groups tab, select a Group, and click **Save**.

8.4.2 Create Roles and Policies with Fusion Middleware Control

> **Note:** This section is applicable only when you manually upload the RPD file and Catalog. For more details, refer to Section 8.3, "Configure OBIEE Repository and Web Catalog Manually.".

To create new application roles:

1. Login to Fusion Middleware Control Enterprise Manager.

2. Go to WebLogic Domain > Security > Application Roles.

   The Application Roles dialog box appears.

3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search** ▶.

   The default role available in clean slate installation appears.

4. Click **Create**.

   The Create Application Role dialog box appears.

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

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

   The Add Principal dialog box appears.

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

   A list of principals appears.

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

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

   The Add Principal dialog box appears.

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

    A list of principals appears.

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

    The Membership for **AIAdminRole** appears.

12. Repeat from Step 4 to Step 11 to create other Roles and add Member to these roles as listed in the table below.

Role	Application Roles
AI Admin Role	AI Admin Group
	Weblogic
AI Author Role	AI Author Group
	AI Admin Group
AI Consumer Role	AI Consumer Group
	AI Author Group
	AI Admin Group

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

To create new application policy:

1. Login to Fusion Middleware Control Enterprise Manager.

2. Go to WebLogic Domain > Security > Application Policies.

   The Application Policies screen appears.

3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.

4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.

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

6. From the list of Searched Principals, select **AIAdminRole**, and click **OK**.

7. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.

8. Select the **Resource Types** radio button.

9. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.

10. From the Search Results, select **oracle.bi.publisher.permission** (BIP Administer Server), and click **Continue**.

    The Add Permission dialog box appears.

11. For **Permission Actions**, select **All** (_all_), and click **Select**.

12. Repeat from Step 4 to Step 11, to add the following:

Policy Name/Principal	Resource Type	Resource Name	Permission Actions
AI Admin Role	oracle.bi.catalog	*	manage
	oracle.bi.server.permission	oracle.bi.server.manageRepositories	_all_
	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanger.manageCatalog	_all_
	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
	oracle.bi.repository	oracle.bi.repository	manage
	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
AI Author Role	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	*
	oracle.bi.delivers.job	*	schedule
AI Consumer Role	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	READ,EXECUTE
	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_

> **Note:** For more details, refer to *Section 2.8.3.2 Creating Application Policies Using Fusion Middleware Control* from *https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf*.
>
> For a list of privileges for BIApplication Role specified above, refer to Section 8.6, "OBIEE Default Application Roles."

8.5 OBIEE Catalog Folder-level Permissions

1. Login to OBIEE Analytics with the WebLogic user credentials.

2. Go to Catalog > Shared Folders > Tasks > Permissions.

   The Permissions dialog box appears.

3. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role	Full Control
AI Author Role	Full Control
AI Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

   a. Select **Apply Permissions to sub-folders.**

   b. Select **Permissions to items within folder.**

   c. Click **OK**.

4. Go to Shared Folders > Argus Insight > Permissions.

   The Permissions dialog box appears.

5. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

   a. Select **Apply Permissions to sub-folders.**

   b. Select **Permissions to items within folder.**

   c. Click **OK**.

Setup the Permissions through the Catalog Manager

If you are unable to set the folder level permissions, refer to the OBIEE Catalog manager.

1. Open the catalog manager from the following path, right-click **runcat.cmd**, and click **Run as administrator**.

   <obiee_home >\user_projects\domains\<instance_name>\bitools\bin\runcat.cmd

2. Open the catalog in offline mode from the catalog path.

   For example:

   C:\Oracle\Middleware\Oracle_Home\user_projects\domains\bi1\bidata\service_instances\ssi\metadata\content\catalog

3. Click the **'/'** folder.

   In the right pane, the Shared folder appears.

   a. Right-click the Shared folder, and select **Permissions**.

The Permissions dialog box appears.

b. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

c. Select **Apply Permissions to sub-folders.**

d. Select **Permissions to items within folder.**

e. Click **OK**.

4. Right-click the Shared folder > **Properties**, set the owner as **BiServiceAdministrator**, and click **OK**.

5. From the tree structure (on the left side), click Shared folder.

Argus Insight folder appears on the right side.

a. Right-click Argus Insight folder, and click Permissions.

The Permissions dialog box appears.

b. Set the permissions as in Step 3 b to 3 d.

c. Click **OK**.

6. Right-click Argus Insight folder > **Properties**, set the owner as **AIAdminRole**, and click **OK**.

7. Login to OBIEE Analytics, and check the folder level permissions.

8. Go to Administration > Maintenance and Troubleshooting, and click **Reload Files and Metadata**.

8.6 OBIEE Default Application Roles

To view and administer privileges of Oracle Business Intelligence components:

1. Login to OBIEE Analytics with WebLogic user credentials.

2. Go to Administration > Security > Manage Privileges.

> **Note:** Create these privileges only when you manually upload the RPD and Catalog.
>
> You do not need to create these privileges when you import the BAR file.

Component	Privilege	Default Role Granted
Access	Access to Dashboards	AI Consumer Role, BI Service Administrator

Component	Privilege	Default Role Granted
Access	Access to Answers	AI Author Role, BI Service Administrator
Access	Access to BI Composer	AI Author Role, BI Service Administrator
Access	Access to Delivers	AI Author Role, BI Service Administrator
Access	Access to Briefing Books	AI Consumer Role, BI Service Administrator
Access	Access to Mobile	AI Consumer Role, BI Service Administrator
Access	Access to Administration	AI Admin Role, BI Service Administrator
Access	Access to Segments	AI Consumer Role, BI Service Administrator
Access	Access to Segment Trees	AI Author Role, BI Service Administrator
Access	Access to List Formats	AI Author Role, BI Service Administrator
Access	Access to Metadata Dictionary	AI Author Role, BI Service Administrator
Access	Access to Oracle BI for Microsoft Office	AI Consumer Role, BI Service Administrator
Access	Access to Oracle BI Client Installer	AI Consumer Role, BI Service Administrator
Access	Catalog Preview Pane UI	AI Consumer Role, BI Service Administrator
Access	Access to Export	AI Consumer Role, BI Service Administrator
Access	Access to KPI Builder	AI Author Role, BI Service Administrator
Access	Access to Scorecard	AI Consumer Role, BI Service Administrator
Actions	Create Navigate Actions	AI Consumer Role, BI Service Administrator
Actions	Create Invoke Actions	AI Author Role, BI Service Administrator
Actions	Save Actions containing embedded HTML	AI Admin Role, BI Service Administrator
Admin: Catalog	Change Permissions	AI Author Role, BI Service Administrator
Admin: Catalog	Toggle Maintenance Mode	AI Admin Role, BI Service Administrator
Admin: General	Manage Sessions	AI Admin Role, BI Service Administrator
Admin: General	Create Dashboards	AI Author Role, BI Service Administrator
Admin: General	See sessions IDs	AI Admin Role, BI Service Administrator
Admin: General	Change Log Configuration	AI Admin Role, BI Service Administrator
Admin: General	Issue SQL Directly	AI Admin Role, BI Service Administrator
Admin: General	View System Information	AI Admin Role, BI Service Administrator
Admin: General	Performance Monitor	AI Admin Role, BI Service Administrator
Admin: General	Manage Agent Sessions	AI Admin Role, BI Service Administrator
Admin: General	Manage Device Types	AI Admin Role, BI Service Administrator
Admin: General	Manage Map Data	AI Admin Role, BI Service Administrator
Admin: General	See privileged errors	AI Admin Role, BI Service Administrator

Component	Privilege	Default Role Granted
Admin: General	See SQL issued in errors	AI Consumer Role, BI Service Administrator
Admin: General	Manage Global Variables	AI Admin Role, BI Service Administrator
Admin: General	Diagnose BI Server Query	Denied: Authenticated User
Admin: General	Manage Marketing Jobs	AI Author Role, BI Service Administrator
Admin: General	Manage Marketing Defaults	AI Admin Role, BI Service Administrator
Admin: Security	Manage Catalog Accounts	AI Admin Role, BI Service Administrator
Admin: Security	Manage Privileges	AI Admin Role, BI Service Administrator
Admin: Security	Set Ownership of Catalog Objects	AI Admin Role, BI Service Administrator
Admin: Security	User Population - Can List Users	AI Consumer Role, BI Service Administrator, BI System
Admin: Security	User Population - Can List Catalog Groups	AI Consumer Role, BI Service Administrator, BI System
Admin: Security	User Population - Can List Application Roles	AI Consumer Role, BI Service Administrator, BI System
Admin: Security	Access to Permissions Dialog	AI Consumer Role, BI Service Administrator
Briefing Book	Add To or Edit a Briefing Book	AI Author Role, BI Service Administrator
Briefing Book	Download Briefing Book	AI Consumer Role, BI Service Administrator
Briefing Book	Add to Snapshot Briefing Book	AI Consumer Role, BI Service Administrator
Catalog	Personal Storage (My Folders and My Dashboard)	AI Consumer Role, BI Service Administrator
Catalog	Reload Metadata	AI Admin Role, BI Service Administrator
Catalog	See Hidden Items	AI Author Role, BI Service Administrator
Catalog	Create Folders	AI Author Role, BI Service Administrator
Catalog	Archive Catalog	AI Admin Role, BI Service Administrator
Catalog	Unarchive Catalog	AI Admin Role, BI Service Administrator
Catalog	Upload Files	AI Admin Role, BI Service Administrator
Catalog	Perform Global Search	AI Author Role, BI Service Administrator
Catalog	Perform Extended Search	AI Author Role, BI Service Administrator
Conditions	Create Conditions	AI Author Role, BI Service Administrator
Dashboards	Save Customizations	AI Consumer Role, BI Service Administrator
Dashboards	Assign Default Customizations	AI Author Role, BI Service Administrator
Dashboards	Create Bookmark Links	AI Consumer Role, BI Service Administrator
Dashboards	Create Prompted Links	AI Consumer Role, BI Service Administrator
Dashboards	Export Entire Dashboard To Excel	AI Consumer Role, BI Service Administrator

Component	Privilege	Default Role Granted
Dashboards	Export Single Dashboard Page To Excel	AI Consumer Role, BI Service Administrator
Formatting	Save System-Wide Column Formats	AI Admin Role, BI Service Administrator
Home and Header	Access Home Page	AI Consumer Role, BI Service Administrator
Home and Header	Access Catalog UI	AI Consumer Role, BI Service Administrator
Home and Header	Access Catalog Search UI	AI Consumer Role, BI Service Administrator
Home and Header	Access Rapid Search UI	AI Consumer Role, BI Service Administrator
Home and Header	Simple Search Field	AI Consumer Role, BI Service Administrator
Home and Header	Advanced Search Link	AI Consumer Role, BI Service Administrator
Home and Header	Open Menu	AI Consumer Role, BI Service Administrator
Home and Header	New Menu	AI Consumer Role, BI Service Administrator
Home and Header	Help Menu	AI Consumer Role, BI Service Administrator
Home and Header	Dashboards Menu	AI Consumer Role, BI Service Administrator
Home and Header	Favorites Menu	AI Consumer Role, BI Service Administrator
Home and Header	My Account Link	AI Consumer Role, BI Service Administrator
Home and Header	Custom Links	AI Consumer Role, BI Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
Home and Header	Access Data Loader	Denied: Authenticated User
My Account	Access to My Account	AI Consumer Role, BI Service Administrator
My Account	Change Preferences	AI Consumer Role, BI Service Administrator
My Account	Change Delivery Options	AI Consumer Role, BI Service Administrator
Answers	Create Views	AI Author Role, BI Service Administrator
Answers	Create Prompts	AI Author Role, BI Service Administrator
Answers	Access Advanced Tab	AI Author Role, BI Service Administrator
Answers	Edit Column Formulas	AI Author Role, BI Service Administrator
Answers	Save Content with HTML Markup	AI Admin Role, BI Service Administrator
Answers	Enter XML and Logical SQL	AI Author Role, BI Service Administrator

Component	Privilege	Default Role Granted
Answers	Edit Direct Database Analysis	AI Admin Role, BI Service Administrator
Answers	Create Analysis From Simple SQL	AI Admin Role, BI Service Administrator
Answers	Create Advanced Filters and Set Operations	AI Author Role, BI Service Administrator
Answers	Save Filters	AI Author Role, BI Service Administrator
Answers	Save Column	AI Author Role, BI Service Administrator
Answers	Add EVALUATE_PREDICATE Function	AI Author Role, BI Service Administrator
Answers	Execute Direct Database Analysis	AI Admin Role, BI Service Administrator
Answers	Upload Images	AI Author Role, BI Service Administrator
Delivers	Create Agents	AI Author Role, BI Service Administrator
Delivers	Publish Agents for Subscription	AI Author Role, BI Service Administrator
Delivers	Deliver Agents to Specific or Dynamically Determined Users	AI Admin Role, BI Service Administrator
Delivers	Chain Agents	AI Author Role, BI Service Administrator
Delivers	Modify Current Subscriptions for Agents	AI Admin Role, BI Service Administrator
Proxy	Act As Proxy	Denied: Authenticated User
RSS Feeds	Access to RSS Feeds	AI Consumer Role, BI Service Administrator
Scorecard	Create/Edit Scorecards	AI Author Role, BI Service Administrator
Scorecard	View Scorecards	AI Consumer Role, BI Service Administrator
Scorecard	Create/Edit Objectives	AI Author Role, BI Service Administrator
Scorecard	Create/Edit Initiatives	AI Author Role, BI Service Administrator
Scorecard	Create Views	AI Author Role, BI Service Administrator
Scorecard	Create/Edit Causes And Effects Linkages	AI Author Role, BI Service Administrator
Scorecard	Create/Edit Perspectives	AI Author Role, BI Service Administrator
Scorecard	Add Annotations	AI Consumer Role, BI Service Administrator
Scorecard	Override Status	AI Consumer Role, BI Service Administrator
Scorecard	Create/Edit KPIs	AI Author Role, BI Service Administrator
Scorecard	Write Back to Database for KPI	AI Consumer Role, BI Service Administrator
Scorecard	Add Scorecard Views To Dashboards	AI Consumer Role, BI Service Administrator
List Formats	Create List Formats	AI Author Role, BI Service Administrator
List Formats	Create Headers and Footers	AI Author Role, BI Service Administrator
List Formats	Access Options Tab	AI Author Role, BI Service Administrator
List Formats	Add/Remove List Format Columns	AI Admin Role, BI Service Administrator
Segmentation	Create Segments	AI Author Role, BI Service Administrator
Segmentation	Create Segment Trees	AI Author Role, BI Service Administrator

Component	Privilege	Default Role Granted
Segmentation	Create/Purge Saved Result Sets	AI Admin Role, BI Service Administrator
Segmentation	Access Segment Advanced Options Tab	AI Admin Role, BI Service Administrator
Segmentation	Access Segment Tree Advanced Options Tab	AI Admin Role, BI Service Administrator
Segmentation	Change Target Levels within Segment Designer	AI Author Role, BI Service Administrator
Mobile	Enable Local Content	AI Consumer Role, BI Service Administrator
Mobile	Enable Search	AI Consumer Role, BI Service Administrator
SOAP	Access SOAP	AI Consumer Role, BI Service Administrator, BI System
SOAP	Impersonate as system user	BI System
SOAP	Access MetadataService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access ScorecardAssessmentService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access MsgdbService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access ReportEditingService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access KPIAssessmentService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access ConditionEvaluationService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access SecurityService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access Tenant Information	BI System
SOAP	Access SchedulerService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access DashboardService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access ScorecardMetadataService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access JobManagementService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access CatalogIndexingService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access UserPersonalizationService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access AnalysisExportViewsService Service	AI Consumer Role, BI Service Administrator
SOAP	Access CatalogService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access AdministrationSOAPService Service	AI Consumer Role, BI Service Administrator, BI System

Component	Privilege	Default Role Granted
SOAP	Access HtmlViewService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access XmlGenerationService Service	AI Consumer Role, BI Service Administrator, BI System
SOAP	Access IBotService Service	AI Consumer Role, BI Service Administrator, BI System
Subject Area: "AI-Aggregate Analysis"	Access within Oracle BI Answers	AI Author Role, BI Service Administrator
View Canvas	Add/Edit Canvas View	AI Author Role, BI Service Administrator
View Column Selector	Add/Edit Column Selector View	AI Author Role, BI Service Administrator
View Compound Layout	Add/Edit Compound Layout View	AI Author Role, BI Service Administrator
View Contribution Wheel	Add/Edit Contribution Wheel View	AI Author Role, BI Service Administrator
View Graph	Add/Edit Graph View	AI Author Role, BI Service Administrator
View Funnel	Add/Edit Funnel View	AI Author Role, BI Service Administrator
View Gauge	Add/Edit Gauge View	AI Author Role, BI Service Administrator
View Micro Chart	Add/Edit Micro Chart View	AI Author Role, BI Service Administrator
View Filters	Add/Edit Filters View	AI Author Role, BI Service Administrator
View Dashboard Prompt	Add/Edit Dashboard Prompt View	AI Author Role, BI Service Administrator
View Performance Tile	Add/Edit Performance Tile View	AI Author Role, BI Service Administrator
View Heat Matrix	Add/Edit Heat Matrix View	AI Author Role, BI Service Administrator
View Static Text	Add/Edit Static Text View	AI Author Role, BI Service Administrator
View Javascript view	Edit Javascript View	AI Author Role, BI Service Administrator
View Legend	Add/Edit Legend View	AI Author Role, BI Service Administrator
View Map	Add/Edit Map View	AI Author Role, BI Service Administrator
View Narrative	Add/Edit Narrative View	AI Author Role, BI Service Administrator
View No Results	Add/Edit No Results View	AI Author Role, BI Service Administrator
View Pivot Table	Add/Edit Pivot Table View	AI Author Role, BI Service Administrator
View Generic Plugin View	Add/Edit Generic Plugin View View	AI Author Role, BI Service Administrator
View Report Prompt	Add/Edit Report Prompt View	AI Author Role, BI Service Administrator
View Create Segment	Add/Edit Create Segment View	AI Author Role, BI Service Administrator
View Selection Steps	Add/Edit Selection Steps View	AI Author Role, BI Service Administrator
View Logical SQL	Add/Edit Logical SQL View	AI Author Role, BI Service Administrator
View Table	Add/Edit Table View	AI Author Role, BI Service Administrator
View Create Target List	Add/Edit Create Target List View	AI Author Role, BI Service Administrator
View Ticker	Add/Edit Ticker View	AI Author Role, BI Service Administrator

Component	Privilege	Default Role Granted
View Title	Add/Edit Title View	AI Author Role, BI Service Administrator
View Treemap	Add/Edit Treemap View	AI Author Role, BI Service Administrator
View Trellis	Add/Edit Trellis View	AI Author Role, BI Service Administrator
View View Selector	Add/Edit View Selector View	AI Author Role, BI Service Administrator
Write Back	Manage Write Back	AI Admin Role, BI Service Administrator
Write Back	Write Back to Database	Denied: Authenticated User

9

Manage 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 Update the Cryptography Key and Re-encrypt

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 screen appears.

4. Enter the following parameters and click **Validate**.

    a. DBA user name

    b. DBA user password

    c. Argus Insight database name

    After successful authentication, the Argus Insight Key Management - Options to re-crypt and change password are enabled.

5. Select **Re-Encrypt Existing Passwords**.

6. Select **Apply New Secure Key** check box.

7. In the **Enter Current Argus Secure Key** field, enter the existing Argus Insight Secure Key.

8. In the **Enter New Argus Secure Key** field, enter the new Argus Insight Secure Key from the Argus Safety Server.

    You may copy **UserCryptoKey** from the ArgusSecureKey.ini file, which is present on all Argus Safety Servers in C:\Windows folder. Make sure you use the exact key used by the corresponding Argus Safety Server.

9. Enter justification.

10. Click **Execute** to start the password regeneration process.

When the password regeneration process completes, the status of the regeneration process (success or fail) appears.

11. Click **Reset** to enable the **Execute** button again.

9.2 Update the Cryptography Key and Change Password

To change all Argus Insight related passwords you can use Key Management Tool. You can change password with the existing cryptography key or use the new cryptography key. If the new cryptography key is used then the same key will be updated in ArgusSecureKey.ini.

To change the cryptography key and change 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.**

   Or, go to: *C\Program Files (x86)\Oracle\ArgusInsight\Bin*

   The Argus Insight Key Management screen appears.

4. Enter the following parameters and click **Validate**.

   a. DBA user name

   b. DBA user password

   c. Argus Insight database name

   After successful authentication, the Argus Insight Key Management - Options to re-crypt and change password are enabled.

5. Select **Change Passwords**.

6. To change the cryptographic key, select **Apply New Secure Key** check box.

7. In the **Enter Current Argus Secure Key** field, enter the existing Argus Insight Secure Key.

8. In the **Enter New Argus Secure Key** field, enter the new Argus Insight Secure Key from the Argus Safety Server.

   You may copy **UserCryptoKey** from the ArgusSecureKey.ini file, which is present on all Argus Safety Servers in C:\Windows folder. Make sure you use the exact key used by the corresponding Argus Safety Server.

9. Enter the Argus Insight Application User Password (deselect this options if you do not want to change password).

10. Enter APR_USER password (deselect this option if you do not want to change password in the AI.INI).

11. Enter the password for Argus Mart application users.

   If Argus Mart is not configured then this section will be disabled.

   ■ You can provide individual password for all enterprises.

   ■ To set same password for all the enterprises, select **Set same Password for all enterprise**.

   ■ Deselect the check box for which enterprise you do not want to change password.

- ■ Deselect all the check boxes if you do not want to change Argus Mart password.

12. Enter justification.

13. Click **Execute** to start the password change process.

When the password change process completes, the status of the process (success or fail) appears.

14. Click **Reset** to enable the **Execute** button again.

9.3 Copy 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 Argus Insight Web Servers

You must copy the AI.ini and Argus SecureKey.ini files to keep the cryptography key and the APR_USER password in sync on all the servers. In case these files are not copied or any other Argus Insight Web Server will not function.

9.4 Restart IIS and Run ETL

After you change the cryptography key, you must complete the following steps on the Argus Insight Web Server to reflect the changes:

1. Restart the Internet Information Services (IIS).

2. Run the incremental ETL.

10

Uninstall the Argus Insight Application

To uninstall Argus Insight 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 > Program and Features.**

3. Select **Uninstall or change a program.**

4. Right-click Argus Insight, and click **Uninstall**.

    The Argus Insight wizard is initiated and the Welcome screen appears with options to modify, verify, and remove programs.

5. Select **Remove**, and click **Next.**

6. Click **Yes**.

    The Argus Insight application is uninstalled completely and a message appears when the process is completed.

7. Click **Finish.**

    A warning message appears stating that you must restart your computer to complete uninstall process of Argus Insight.

    Be sure to save your work and close other open applications before continuing.

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

10.1 Delete the Argus Insight Folder from the Web Server

You must restart the server after the Argus Insight application is uninstalled. 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.

10.2 Reset the IIS

If you uninstall Argus Insight, be sure to reset the Internet Information Services (IIS) before you install the Argus Insight application again.

A

Create ODBC Connection for OBIEE Administration Tool

This appendix comprises the steps to create ODBC connection for OBIEE Administration tool.

1. Navigate to Control Panel > All Control Panel Items > Administrative Tools.

2. Double-click Data Sources (ODBC) (64-bit).

    The ODBC Data Source Administrator (64-bit) dialog box appears.

3. From the System DSN tab, and click **Add**.

    The Create New Data Source dialog box appears.

4. From the list of the available drivers, select **Oracle BI Server**, and click **Finish**.

    The Oracle BI Server DSN Configuration dialog box appears.

5. Enter the following fields:

    a. **Name**—AIOBIEE (or any name)

    b. **Description**—Argus Insight OBIEE (or any description)

    c. **Server**—OBIEE Server Name

6. Click **Next**.

    a. **Login ID**—weblogic

    b. **Password**—<password for weblogic>

    c. **Port**—The port must be same as mentioned in the Managed Server port list for OBIEE BI Server.

        To retrieve this port, go to Enterprise Manager > BI Instance > Availability tab.

7. Click **Next**.

    The Oracle BI Server DSN Configuration dialog box appears.

8. From the list of database, select **AI80_SRC**.

9. Click **Finish**.